

Setting Up Desktop and Application Pools in View

VMware Horizon 7
Version 7.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001999-00

vmware[®]

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

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

Copyright © 2016 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

	Setting Up Desktop and Application Pools in View	7
1	Introduction to Desktop and Application Pools	9
	Farms, RDS Hosts, and Desktop and Application Pools	9
	Advantages of Desktop Pools	10
	Desktop Pools for Specific Types of Workers	11
	Advantages of Application Pools	14
2	Preparing Unmanaged Machines	15
	Prepare an Unmanaged Machine for Remote Desktop Deployment	15
	Install Horizon Agent on an Unmanaged Machine	16
3	Creating and Preparing a Parent Virtual Machine for Cloning	19
	Creating a Virtual Machine for Cloning	19
	Install Horizon Agent on a Virtual Machine	26
	Install Horizon Agent Silently	30
	Configure a Virtual Machine with Multiple NICs for Horizon Agent	36
	Optimize Guest Operating System Performance	37
	Disable the Windows Customer Experience Improvement Program	38
	Optimizing Windows for Instant-Clone and View Composer Linked-Clone Virtual Machines	39
	Preparing a Parent Virtual Machine	45
	Creating Virtual Machine Templates	49
	Creating Customization Specifications	50
4	Creating Automated Desktop Pools That Contain Full Virtual Machines	51
	Automated Pools That Contain Full Virtual Machines	51
	Worksheet for Creating an Automated Pool That Contains Full Virtual Machines	51
	Create an Automated Pool That Contains Full Virtual Machines	55
	Clone an Automated Desktop Pool	56
	Desktop Settings for Automated Pools That Contain Full Virtual Machines	57
5	Creating Linked-Clone Desktop Pools	59
	Linked-Clone Desktop Pools	59
	Worksheet for Creating a Linked-Clone Desktop Pool	59
	Create a Linked-Clone Desktop Pool	67
	Clone an Automated Desktop Pool	69
	Desktop Pool Settings for Linked-Clone Desktop Pools	70
	View Composer Support for Linked-Clone SIDs and Third-Party Applications	71
	Keeping Linked-Clone Machines Provisioned for Use in Remote Desktop Sessions During View Composer Operations	75
	Use Existing Active Directory Computer Accounts for Linked Clones	76

- 6 Creating Instant-Clone Desktop Pools 79**
 - Instant-Clone Desktop Pools 79
 - Add an Instant Clone Domain Administrator 81
 - Worksheet for Creating an Instant-Clone Desktop Pool 81
 - Create an Instant-Clone Desktop Pool 85
 - ClonePrep Guest Customization 86
 - Instant Clone Maintenance Utilities 87

- 7 Creating Manual Desktop Pools 89**
 - Manual Desktop Pools 89
 - Worksheet for Creating a Manual Desktop Pool 89
 - Create a Manual Desktop Pool 91
 - Create a Manual Pool That Contains One Machine 92
 - Desktop Pool Settings for Manual Pools 93

- 8 Setting Up Remote Desktop Services Hosts 95**
 - Remote Desktop Services Hosts 95
 - Install Remote Desktop Services on Windows Server 2008 R2 97
 - Install Remote Desktop Services on Windows Server 2012 or 2012 R2 97
 - Install Desktop Experience on Windows Server 2008 R2 98
 - Install Desktop Experience on Windows Server 2012 or 2012 R2 98
 - Restrict Users to a Single Session 99
 - Install Horizon Agent on a Remote Desktop Services Host 99
 - Enable Time Zone Redirection for RDS Desktop and Application Sessions 102
 - Enable Windows Basic Theme for Applications 102
 - Configure Group Policy to Start Runonce.exe 103
 - RDS Host Performance Options 103
 - Configuring 3D Graphics for RDS Hosts 104

- 9 Creating Farms 107**
 - Farms 107
 - Preparing a Parent Virtual Machine for an Automated Farm 108
 - Worksheet for Creating a Manual Farm 111
 - Worksheet for Creating an Automated Farm 112
 - Create a Manual Farm 116
 - Create an Automated Farm 117

- 10 Creating Application Pools 119**
 - Application Pools 119
 - Worksheet for Creating an Application Pool Manually 120
 - Create an Application Pool 120

- 11 Creating RDS Desktop Pools 123**
 - Understanding RDS Desktop Pools 123
 - Create an RDS Desktop Pool 124
 - Desktop Pool Settings for RDS Desktop Pools 124
 - Configure Adobe Flash Throttling with Internet Explorer for RDS Desktop Pools 125

- 12 Provisioning Desktop Pools 127**
 - User Assignment in Desktop Pools 127
 - Naming Machines Manually or Providing a Naming Pattern 128
 - Manually Customizing Machines 133
 - Desktop Pool Settings for All Desktop Pool Types 135
 - Adobe Flash Quality and Throttling 139
 - Setting Power Policies for Desktop Pools 140
 - Configuring 3D Rendering for Desktops 145
 - Prevent Access to View Desktops Through RDP 156
 - Deploying Large Desktop Pools 157

- 13 Entitling Users and Groups 159**
 - Add Entitlements to a Desktop or Application Pool 159
 - Remove Entitlements from a Desktop or Application Pool 160
 - Review Desktop or Application Pool Entitlements 160
 - Restricting Remote Desktop Access 160

- 14 Configuring Remote Desktop Features 165**
 - Configuring Unity Touch 165
 - Configuring Flash URL Redirection for Multicast or Unicast Streaming 168
 - Configuring Flash Redirection 172
 - Configuring URL Content Redirection 177
 - Configuring Real-Time Audio-Video 183
 - Configuring Scanner Redirection 197
 - Configuring Serial Port Redirection 202
 - Managing Access to Windows Media Multimedia Redirection (MMR) 209
 - Managing Access to Client Drive Redirection 211

- 15 Using USB Devices with Remote Desktops and Applications 213**
 - Limitations Regarding USB Device Types 214
 - Overview of Setting Up USB Redirection 215
 - Network Traffic and USB Redirection 216
 - Automatic Connections to USB Devices 216
 - Deploying USB Devices in a Secure View Environment 217
 - Using Log Files for Troubleshooting and to Determine USB Device IDs 219
 - Using Policies to Control USB Redirection 220
 - Troubleshooting USB Redirection Problems 230

- 16 Reducing and Managing Storage Requirements 233**
 - Managing Storage with vSphere 233
 - Reducing Storage Requirements with Instant Clones 239
 - Reducing Storage Requirements with View Composer 240
 - Storage Sizing for Instant-Clone and View Composer Linked-Clone Desktop Pools 241
 - Storage Overcommit for View Composer Linked-Clone Virtual Machines 245
 - View Composer Linked-Clone Data Disks 247
 - Storing View Composer Linked Clones on Local Datastores 248

- Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones 249
- Configure View Storage Accelerator for View Composer Linked Clones 250
- Reclaim Disk Space on View Composer Linked Clones 251
- Using VAAI Storage for View Composer Linked Clones 253
- Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones 254

- 17 Configuring Policies for Desktop and Application Pools 255**
 - Setting Policies in View Administrator 255
 - Using Smart Policies 257
 - Using Active Directory Group Policies 263
 - Using View Group Policy Administrative Template Files 264
 - View ADM and ADMX Template Files 264
 - Horizon Agent Configuration ADM Template Settings 266
 - PCoIP Policy Settings 271
 - VMware Blast Policy Settings 282
 - Using Remote Desktop Services Group Policies 283
 - Setting Up Location-Based Printing 292
 - Active Directory Group Policy Example 297

- 18 Configuring User Profiles with View Persona Management 301**
 - Providing User Personas in View 301
 - Using View Persona Management with Standalone Systems 302
 - Migrating User Profiles with View Persona Management 303
 - Persona Management and Windows Roaming Profiles 306
 - Configuring a View Persona Management Deployment 306
 - Best Practices for Configuring a View Persona Management Deployment 315
 - View Persona Management Group Policy Settings 318

- 19 Troubleshooting Machines and Desktop Pools 327**
 - Display Problem Machines 327
 - Send Messages to Desktop Users 328
 - Problems Provisioning or Recreating a Desktop Pool 328
 - Troubleshooting Network Connection Problems 339
 - Troubleshooting USB Redirection Problems 342
 - Manage Machines and Policies for Unentitled Users 344
 - Resolving Database Inconsistencies with the ViewDbChk Command 344
 - Further Troubleshooting Information 347

- Index 349**

Setting Up Desktop and Application Pools in View

Setting Up Desktop and Application Pools in View describes how to create and provision pools of machines and create pools of remote applications that run on Microsoft Remote Desktop Services (RDS) hosts. It includes information about preparing machines, configuring policies, entitling users and groups, configuring remote desktop features, 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 Desktop and Application Pools

1

With Horizon 7, you can create desktop pools that include thousands of virtual desktops. You can deploy desktops that run on virtual machines (VMs), physical machines, and Windows Remote Desktop Services (RDS) hosts. Create one VM as a base image, and Horizon 7 can generate a pool of virtual desktops from that image. You can also create application pools that give users remote access to applications.

This chapter includes the following topics:

- [“Farms, RDS Hosts, and Desktop and Application Pools,”](#) on page 9
- [“Advantages of Desktop Pools,”](#) on page 10
- [“Desktop Pools for Specific Types of Workers,”](#) on page 11
- [“Advantages of Application Pools,”](#) on page 14

Farms, RDS Hosts, and Desktop and Application Pools

You can create desktop and application pools to give users remote access to virtual machine-based desktops, session-based desktops, physical computers, and applications. You can also choose Microsoft Remote Desktop Services (RDS), VMware PC-over-IP (PCoIP), or VMware Blast to provide remote access to users.

RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. These servers host applications and desktop sessions that users can access remotely. To access RDS desktop pools or applications, Horizon Client 3.0 or later is required.

Desktop Pools

There are three main types of desktop pools: automated, manual, and RDS. 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. RDS desktop pools are not a collection of machines, but instead, provide users with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously.

Application Pools

Application pools let you deliver applications to many users. The applications in application pools run on a farm of RDS hosts.

Farms

Farms are collections of RDS hosts and facilitate the management of those hosts. Farms can have a variable number of RDS hosts and provide a common set of applications or RDS desktops to users. When you create an RDS desktop pool or an application pool, you must specify a farm. The RDS hosts in the farm provide desktop and application sessions to users.

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 or an RDS host
- 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 248. Instant clone pools are not supported on local data stores.

NOTE For information about other types of storage options, see [Chapter 16, “Reducing and Managing Storage Requirements,”](#) on page 233.

- 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 `vmadmin` 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 248. Instant clone pools are not supported on local data stores.

NOTE For information about other types of storage options, see [Chapter 16, “Reducing and Managing Storage Requirements,”](#) on page 233.

- 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 [Chapter 17, “Configuring Policies for Desktop and Application Pools,”](#) on page 255.
- 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.

Advantages of Application Pools

With application pools, you give users access to applications that run on servers in a data center instead of on their personal computers or devices.

Application pools offer several important benefits:

- **Accessibility**
Users can access applications from anywhere on the network. You can also configure secure network access.
- **Device independence**
With application pools, you can support a range of client devices, such as smart phones, tablets, laptops, thin clients, and personal computers. The client devices can run various operating systems, such as Windows, iOS, Mac OS, or Android.
- **Access control**
You can easily and quickly grant or remove access to applications for one user or a group of users.
- **Accelerated deployment**
With application pools, deploying applications can be accelerated because you only deploy applications on servers in a data center and each server can support multiple users.
- **Manageability**
Managing software that is deployed on client computers and devices typically requires significant resources. Management tasks include deployment, configuration, maintenance, support, and upgrades. With application pools, you can simplify software management in an enterprise because the software runs on servers in a data center, which requires fewer installed copies.
- **Security and regulatory compliance**
With application pools, you can improve security because applications and their associated data are centrally located in a data center. Centralized data can address security concerns and regulatory compliance issues.
- **Reduced cost**
Depending on software license agreements, hosting applications in a data center can be more cost-effective. Other factors, including accelerated deployment and improved manageability, can also reduce the cost of software in an enterprise.

Preparing Unmanaged Machines

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 [Chapter 8, “Setting Up Remote Desktop Services Hosts,”](#) on page 95.

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 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 89.

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 2-1. Horizon Agent Custom Setup Options for Unmanaged Machines in an IPv4 Environment (Optional)

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

Table 2-1. 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 2-2. 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

3

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 [Chapter 8, “Setting Up Remote Desktop Services Hosts,”](#) on page 95.

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,”](#) on page 19
- [“Install Horizon Agent on a Virtual Machine,”](#) on page 26
- [“Install Horizon Agent Silently,”](#) on page 30
- [“Configure a Virtual Machine with Multiple NICs for Horizon Agent,”](#) on page 36
- [“Optimize Guest Operating System Performance,”](#) on page 37
- [“Disable the Windows Customer Experience Improvement Program,”](#) on page 38
- [“Optimizing Windows for Instant-Clone and View Composer Linked-Clone Virtual Machines,”](#) on page 39
- [“Preparing a Parent Virtual Machine,”](#) on page 45
- [“Creating Virtual Machine Templates,”](#) on page 49
- [“Creating Customization Specifications,”](#) on page 50

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 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.
- 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 3-1. 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: <ul style="list-style-type: none"> ■ For Windows 7 SP1: 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.

Table 3-1. 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 View Desktops Through RDP,”](#) on page 156.
- 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 Use the VMware Tools time synchronization function to ensure that the virtual machine is synchronized to ESXi.

ESXi must synchronize to an external NTP source, for example, the same time source as Active Directory.

Disable other time synchronization mechanisms such as Windows Time Service.

The VMware Tools online help provides information on configuring time synchronization between guest and host.

- 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 25
- 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 any other Horizon software component, including security server, Connection Server, View Composer, or 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 3-2. 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.
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 <i>View Security</i> 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.

Table 3-2. Horizon Agent Custom Setup Options in an IPv4 Environment (Continued)

Option	Description
Virtual Printing	<p>Lets users print to any printer available on their client computers. Users do not have to install additional drivers on their desktops.</p> <p>In Horizon 6.0.1 and later, virtual printing is supported on the following remote desktops and applications:</p> <ul style="list-style-type: none"> ■ 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 ■ Hosted Apps ■ Hosted Apps that are launched from Horizon Client inside remote desktops <p>In Horizon 6.0 and earlier, virtual printing is supported on desktops that are deployed on single-user, Windows Desktop machines.</p> <p>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.</p>
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	<p>Lets users authenticate with smart cards when they use the PCoIP or Blast Extreme display protocol. This option is not selected by default.</p> <p>Smartcard Redirection is supported on remote desktops that are deployed on single-user machines.</p>
VMware Audio	Provides a virtual audio driver on the remote desktop.
Flash Redirection (experimental)	<p>Redirects Flash multimedia content in an Internet Explorer 9, 10, or 11 browser to the client, for performance optimization. This is a Tech Preview feature.</p> <p>This option is not selected by default. You must select the option to install it.</p> <p>Flash Redirection is available in Horizon 7.0 and later releases.</p>

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

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

Feature	Description
PCoIP Agent	<p>Lets users connect to the View desktop using the PCoIP display protocol.</p> <p>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.</p>
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.

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

Feature	Description
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 3-5](#).

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 in a virtual machine that is managed by vCenter Server. In addition, the installer installs the VMware Blast, PCoIP, 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,BlastProtocol,PCoIP,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 VMware Blast, PCoIP, 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,BlastProtocol,PCoIP,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 3-4. Command-Line Options for a View Component's Bootstrap Program

Option	Description
/s	<p>Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs.</p> <p>For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code></p> <p>The /s option is required to run a silent installation.</p>
/v" MSI_command_line_options"	<p>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.</p> <p>For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"</code></p> <p>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.</p> <p>For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""</code></p> <p>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.</p> <p>The /v"command_line_options" option is required to run a silent installation.</p>

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 3-5. MSI Command-Line Options and MSI Properties

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

Table 3-5. MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
ADDLOCAL	<p>Determines the component-specific options to install.</p> <p>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.</p> <p>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.</p> <p>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 SVI Agent are mutually exclusive. To install NGVC, you must specify it explicitly.</p> <p>The following example installs Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, and all features that are supported on the guest operating system: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></p> <p>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.</p> <p>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: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</code></p> <p>To specify individual setup options, type a comma-separated list of setup option names. Do not use spaces between names. Use the format <code>ADDLOCAL=value,value,value...</code></p> <p>You must include <code>Core</code> when you use the <code>ADDLOCAL=value,value,value...</code> property.</p> <p>The following example installs Horizon Agent with the Core, BlastProtocol, PCoIP, UnityTouch, Instant Clone Agent, and Virtual Printing features:</p> <pre>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,BlastProtocol,PCoIP,UnityTouch,NGVC,ThinPrint"</pre> <p>The preceding example does not install other components, even those that are installed by default interactively.</p> <p>The ADDLOCAL MSI property is optional.</p>
REBOOT	<p>You can use the <code>REBOOT=ReallySuppress</code> option to allow system configuration tasks to complete before the system reboots.</p> <p>This MSI property is optional.</p>
<code>/l*v log_file</code>	<p>Writes logging information into the specified log file with verbose output.</p> <p>For example: <code>/l*v ""%TEMP%\vmmsi.log"</code></p> <p>This example generates a detailed log file that is similar to the log generated during an interactive installation.</p> <p>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.</p> <p>The <code>/l*v</code> option is optional.</p>

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 3-6 shows the Horizon Agent silent installation properties that you can use at the command-line.

Table 3-6. MSI Properties for Silently Installing Horizon Agent

MSI Property	Description	Default Value
INSTALLDIR	<p>The path and folder in which the Horizon Agent software is installed.</p> <p>For example: <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path.</p> <p>This MSI property is optional.</p>	%ProgramFiles %VMware\VMware View\Agent
RDP_CHOICE	<p>Determines whether to enable Remote Desktop Protocol (RDP) on the desktop.</p> <p>A value of 1 enables RDP. A value of 0 leaves the RDP setting disabled.</p> <p>This MSI property is optional.</p>	1
UNITY_DEFAULT_APPS	<p>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.</p> <p>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,” on page 166.</p> <p>This MSI property is optional.</p>	
URL_FILTERING_ENABLED	<p>Specifies whether the URL Content Redirection feature is installed.</p> <p>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,” on page 177.</p> <p>This MSI property is optional.</p>	0
VDM_VC_MANAGED_AGENT	<p>Determines whether vCenter Server manages the virtual machine on which Horizon Agent is installed.</p> <p>A value of 1 configures the desktop as a vCenter Server-managed virtual machine.</p> <p>A value of 0 configures the desktop as unmanaged by vCenter Server.</p> <p>This MSI property is required.</p>	None
VDM_SERVER_NAME	<p>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.</p> <p>For example: <code>VDM_SERVER_NAME=10.123.01.01</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.</p>	None
VDM_SERVER_USERNAME	<p>The user name of the administrator on the View Connection Server computer. This MSI property applies to unmanaged desktops only.</p> <p>For example: <code>VDM_SERVER_USERNAME=domain\username</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.</p>	None
VDM_SERVER_PASSWORD	<p>The View Connection Server administrator user password.</p> <p>For example: <code>VDM_SERVER_PASSWORD=secret</code></p> <p>This MSI property is required for unmanaged desktops.</p> <p>Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.</p>	None
VDM_IP_PROTOCOL_USAGE	<p>Specifies the IP version that Horizon Agent uses. The possible values are IPv4 and IPv6.</p>	IPv4

Table 3-6. MSI Properties for Silently Installing Horizon Agent (Continued)

MSI Property	Description	Default Value
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 3-7](#) 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 3-7. 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 <code>VDM_FLASH_URL_REDIRECTION=1</code> 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 3-7. 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 specify the following features explicitly. You must always specify Core.

Silent Installation Feature	Description
Core	The core Horizon Agent functions.
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,BlastProtocol,PCoIP,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 as \$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 3-8](#), verify that you took the optimization steps in “[Optimize Guest Operating System Performance](#),” on page 37.

Table 3-8. 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, <code>hiberfil.sys</code> , 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 <code>hiberfil.sys</code> 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 3-8. 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 not 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 Windows prefetch 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 26.

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](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.
 - On the parent virtual machine, open a command prompt.
 - Type the `ipconfig /releas` 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 59.

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

4

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,”](#) on page 51
- [“Worksheet for Creating an Automated Pool That Contains Full Virtual Machines,”](#) on page 51
- [“Create an Automated Pool That Contains Full Virtual Machines,”](#) on page 55
- [“Clone an Automated Desktop Pool,”](#) on page 56
- [“Desktop Settings for Automated Pools That Contain Full Virtual Machines,”](#) on page 57

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 4-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Option	Description	Fill In Your Value Here
User assignment	<p>Choose the type of user assignment:</p> <ul style="list-style-type: none"> ■ 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. <p>For details, see “User Assignment in Desktop Pools,” on page 127.</p>	
Enable automatic assignment	<p>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.</p> <p>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.</p>	
vCenter Server	<p>Select the vCenter Server that manages the virtual machines in the pool.</p>	
Desktop Pool ID	<p>The unique name that identifies the pool in View Administrator.</p> <p>If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.</p> <p>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.</p>	
Display name	<p>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.</p>	
Access group	<p>Select an access group in which to place the pool or leave the pool in the default root access group.</p> <p>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 <i>View Administration</i> document.</p> <p>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.</p>	
Delete machine after logoff	<p>If you select floating user assignment, choose whether to delete machines after users log off.</p> <p>NOTE You set this option on the Desktop Pool Settings page.</p>	

Table 4-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	<p>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 135.</p> <p>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.</p> <p>For more information about power policies and automated pools, see “Setting Power Policies for Desktop Pools,” on page 140.</p>	
Stop provisioning on error	<p>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.</p>	
Virtual Machine Naming	<p>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.</p> <p>For details, see “Naming Machines Manually or Providing a Naming Pattern,” on page 128.</p>	
Specify names manually	<p>If you specify names manually, prepare a list of machine names and, optionally, the associated user names.</p>	
Naming Pattern	<p>If you use this naming method, provide the pattern.</p> <p>The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine.</p> <p>For details, see “Using a Naming Pattern for Automated Desktop Pools,” on page 130.</p>	
Maximum number of machines	<p>If you use a naming pattern, specify the total number of machines in the pool.</p> <p>You can also specify a minimum number of machines to provision when you first create the pool.</p>	
Number of spare (powered on) machines	<p>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 128.</p> <p>When you specify names manually, this option is called # Unassigned machines kept powered on.</p>	

Table 4-1. 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	<p>If you use a naming pattern and provision machines on demand, specify a minimum number of machines in the pool.</p> <p>The minimum number of machines is created when you create the pool.</p> <p>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.</p>	
Use vSphere Virtual SAN	<p>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 235.</p>	
Template	<p>Select the virtual machine template to use for creating the pool.</p>	
vCenter Server folder	<p>Select the folder in vCenter Server in which the desktop pool resides.</p>	
Host or cluster	<p>Select the ESXi host or cluster on which the virtual machines run.</p> <p>In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts.</p>	
Resource pool	<p>Select the vCenter Server resource pool in which the desktop pool resides.</p>	
Datastores	<p>Select one or more datastores on which to store the desktop pool.</p> <p>For clusters, you can use shared or local datastores.</p> <p>NOTE If you use Virtual SAN, select only one datastore.</p>	
Use View Storage Accelerator	<p>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.</p> <p>This feature is supported on vSphere 5.0 and later.</p> <p>This feature is enabled by default.</p> <p>For details, see “Configure View Storage Accelerator for View Composer Linked Clones,” on page 250.</p>	

Table 4-1. 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	<p>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.</p> <p>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 View on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <p>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.</p>	
Guest customization	<p>Select a customization specification (SYSPREP) from the list to configure licensing, domain attachment, DHCP settings, and other properties on the machines.</p> <p>Alternatively, you can customize the machines manually after they are created.</p>	

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 3, “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 135.

- 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 159.

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-clone pool, see [“Create a Linked-Clone Desktop Pool,”](#) on page 67.

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 159.

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 4-2](#) 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 135.

Table 4-2. 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 their machines	Yes	Yes
Allow user to initiate separate sessions from different client devices		Yes
Delete machine after logoff		Yes
Default display protocol	Yes	Yes

Table 4-2. Settings for Automated Pools That Contain Full Virtual Machines (Continued)

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
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

Creating Linked-Clone Desktop Pools

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,”](#) on page 59
- [“Worksheet for Creating a Linked-Clone Desktop Pool,”](#) on page 59
- [“Create a Linked-Clone Desktop Pool,”](#) on page 67
- [“Clone an Automated Desktop Pool,”](#) on page 69
- [“Desktop Pool Settings for Linked-Clone Desktop Pools,”](#) on page 70
- [“View Composer Support for Linked-Clone SIDs and Third-Party Applications,”](#) on page 71
- [“Keeping Linked-Clone Machines Provisioned for Use in Remote Desktop Sessions During View Composer Operations,”](#) on page 75
- [“Use Existing Active Directory Computer Accounts for Linked Clones,”](#) on page 76

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 5-1. 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: <ul style="list-style-type: none"> ■ 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 127.	
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 <i>View Administration</i> 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 135. For a list of the settings that apply to linked-clone pools, see “Desktop Pool Settings for Linked-Clone Desktop Pools,” on page 70. For more information about power policies and automated pools, see “Setting Power Policies for Desktop Pools,” on page 140.	

Table 5-1. 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 128.	
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 130.	
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 128. 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 75.	

Table 5-1. 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	<p>If you use a naming pattern, choose whether to provision all machines when the pool is created or provision machines as they are needed.</p> <ul style="list-style-type: none"> ■ 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	<p>If you use a naming pattern and provision desktops on demand, specify a minimum number of machines in the pool.</p> <p>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.</p>	
Redirect Windows profile to a persistent disk	<p>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.</p> <p>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.</p> <p>If you store the Windows profile in the OS disk, user data and settings are removed during refresh, recompose, and rebalance operations.</p>	
Disk size and drive letter for persistent disk	<p>If you store user profile data on a separate View Composer persistent disk, provide the disk size in megabytes and the drive letter.</p> <p>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.</p>	
Disposable File Redirection	<p>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.</p> <p>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.</p>	

Table 5-1. 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	<p>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.</p> <p>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.</p> <p>You can select a drive letter for the disposable file disk. The default value, Auto, directs View to assign the drive letter.</p> <p>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.</p>	
Use vSphere Virtual SAN	<p>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 235.</p>	
Select separate datastores for persistent and OS disks	<p>(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.</p>	
Select separate datastores for replica and OS disks	<p>(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.</p> <p>For details, see “Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones,” on page 249.</p> <p>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.</p>	
Parent VM	<p>Select the parent virtual machine for the pool.</p>	
Snapshot (default image)	<p>Select the snapshot of the parent virtual machine to use as the base image for the pool.</p> <p>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.</p>	
VM folder location	<p>Select the folder in vCenter Server in which the desktop pool resides.</p>	

Table 5-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Host or cluster	<p>Select the ESXi host or cluster on which the desktop virtual machines run.</p> <p>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.</p> <p>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.</p> <p>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 157.</p>	
Resource pool	<p>Select the vCenter Server resource pool in which the desktop pool resides.</p>	
Datastores	<p>Select one or more datastores on which to store the desktop pool.</p> <p>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 241.</p> <p>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 248.</p> <p>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.</p> <p>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 157.</p> <p>For more information about the disks that are created for linked clones, see “View Composer Linked-Clone Data Disks,” on page 247.</p> <p>NOTE If you use Virtual SAN, select only one datastore.</p>	

Table 5-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Storage Overcommit	<p>Determine the storage-overcommit level at which linked-clones are created on each datastore.</p> <p>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 246.</p> <p>NOTE This setting has no effect if you use Virtual SAN.</p>	
Use View Storage Accelerator	<p>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.</p> <p>This feature is supported on vSphere 5.0 and later.</p> <p>This feature is enabled by default.</p> <p>For details, see “Configure View Storage Accelerator for View Composer Linked Clones,” on page 250.</p>	
Use native NFS snapshots (VAAI)	<p>(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.</p> <p>You can use this feature only if you select datastores that reside on NAS devices that support native cloning operations through VAAI.</p> <p>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.</p> <p>This feature is supported on vSphere 5.0 and later.</p> <p>For details, see “Using VAAI Storage for View Composer Linked Clones,” on page 253.</p>	
Reclaim VM disk space	<p>(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.</p> <p>This feature is supported on vSphere 5.1 and later. The linked-clone virtual machines must be virtual hardware version 9 or later.</p> <p>For details, see “Reclaim Disk Space on View Composer Linked Clones,” on page 251.</p>	

Table 5-1. 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:	<p>(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.</p> <p>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.</p> <p>For example: 2 GB.</p> <p>The default value is 1 GB.</p>	
Blackout Times	<p>Configure days and times during which View Storage Accelerator regeneration and the reclamation of virtual machine disk space do not take place.</p> <p>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.</p> <p>For details, see “Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones,” on page 254.</p>	
Transparent Page Sharing Scope	<p>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.</p> <p>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 View on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <p>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.</p>	
Domain	<p>Select the Active Directory domain and user name.</p> <p>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.</p> <p>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.</p> <p>For information about configuring View Composer, see the <i>View Administration</i> document.</p>	

Table 5-1. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
AD container	<p>Provide the Active Directory container relative distinguished name.</p> <p>For example: CN=Computers</p> <p>When you run the Add Desktop Pool wizard, you can browse your Active Directory tree for the container.</p>	
Allow reuse of pre-existing computer accounts	<p>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.</p> <p>The existing computer accounts must be located in the Active Directory container that you specify with the Active Directory container setting.</p> <p>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.</p> <p>For details, see “Use Existing Active Directory Computer Accounts for Linked Clones,” on page 76.</p>	
Use QuickPrep or a customization specification (Sysprep)	<p>Choose whether to use QuickPrep or select a customization specification (Sysprep) to configure licensing, domain attachment, DHCP settings, and other properties on the machines.</p> <p>Sysprep is supported for linked clones only on vSphere 4.1 or later software.</p> <p>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.</p> <p>For details, see “Choosing QuickPrep or Sysprep to Customize Linked-Clone Machines,” on page 72.</p>	
Power-off script	<p>QuickPrep can run a customization script on linked-clone machines before they are powered off.</p> <p>Provide the path to the script on the parent virtual machine and the script parameters.</p>	
Post-synchronization script	<p>QuickPrep can run a customization script on linked-clone machines after they are created, recomposed, and refreshed.</p> <p>Provide the path to the script on the parent virtual machine and the script parameters.</p>	

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 3, “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 59.
- 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 135.
- 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 159.

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-clone pool, see [“Create a Linked-Clone Desktop Pool,”](#) on page 67.

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 159.

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 5-2](#) 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 135.

Table 5-2. 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 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 5-2. 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 72.

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 75.

[Table 5-3](#) shows the effect of View Composer operations on linked-clone SIDs and third-party application GUIDs.

Table 5-3. 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 5-4](#) compares QuickPrep with customization specifications that are created with Microsoft Sysprep.

Table 5-4. 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 73.	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 5-4. 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 75.
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 73.

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

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

This chapter includes the following topics:

- [“Instant-Clone Desktop Pools,”](#) on page 79
- [“Add an Instant Clone Domain Administrator,”](#) on page 81
- [“Worksheet for Creating an Instant-Clone Desktop Pool,”](#) on page 81
- [“Create an Instant-Clone Desktop Pool,”](#) on page 85
- [“ClonePrep Guest Customization,”](#) on page 86
- [“Instant Clone Maintenance Utilities,”](#) on page 87

Instant-Clone Desktop Pools

An instant-clone desktop pool is an automated desktop pool. vCenter Server creates the desktop virtual machines 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 virtual machine and therefore consume less storage than full virtual machines. In addition, instant clones also share the memory of a parent virtual machine. Instant clones are created using the vmFork technology. An instant-clone desktop pool has the following key properties:

- 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 user to log in. Guest customization and AD domain join are completed as part of the initial power-on workflow.
- When a user logs off, the desktop virtual machine 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 recreate the pool from any snapshot of any parent virtual machine. You can use push image to roll out OS and application patches.
- Clones are automatically rebalanced over available datastores when clones are created.
- View storage accelerator is automatically enabled.
- Transparent page sharing is automatically enabled.

Because View can create instant clones very quickly, you typically do not need to provision a large number of desktops up front or to have a large number of ready desktops. For this reason, when compared with View Composer linked clones, instant clones can make the task of managing a large number of desktops 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 version 11 or later.

It is recommended that you configure distributed virtual switches in the vSphere environment.

In Horizon 7.0, instant clones have certain restrictions:

- Single-user desktops only. RDS hosts are not supported.
- Floating user assignment only. 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 pre-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 machines 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 off, so that reclaiming unused disk space in a VM no longer has a significant impact on storage consumption.

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

- 1 View publishes the image that you selected. In vCenter Server, four folders (ClonePrepInternalTemplateFolder, ClonePrepParentVmFolder, ClonePrepReplicaVmFolder, and ClonePrepResyncVmFolder) are created if they do not exist, and a number of internal VMs that are required for cloning are created. In View Administrator, you can see the progress of this operation on the summary page of the desktop pool. During publishing, the Pending Image pane shows the image and its state.

NOTE Do not tamper with the four folders or the internal VMs that are in them. Otherwise, errors might occur. The internal VMs are automatically 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 very fast. Typically, a clone can be created in less than two seconds. During this process, the Current Image pane shows the image and its state.

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. Again, 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 must be created, for example, when a user logs off or when you increase the size of the pool. 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 will be created on the remaining datastores.
- If you add a datastore, manually remove some desktops from the original datastores so that the new desktops will be 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 desktops are recreated, they will be evenly distributed across the datastores.

For details about all the settings that are available to an instant-clone pool, see [“Worksheet for Creating an Instant-Clone Desktop Pool,”](#) on page 81.

Add an Instant Clone Domain Administrator

Before you can 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 administrator's login name and password

Worksheet for Creating an Instant-Clone Desktop Pool

When you create an instant-clone desktop pool, the Horizon Administrator's Add Desktop Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

Before you create a instant-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. Horizon 7 uses the snapshot as the base image to create the clones.

NOTE You cannot create a instant-clone pool from a virtual machine template.

Table 6-1. 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 virtual machines in the pool.	
Desktop Pool ID	The unique name that identifies the pool in Horizon Administrator. If multiple Connection Server configurations are running in your environment, make sure that another Connection Server configuration is not using the same pool ID. A Connection Server configuration can be a standalone View Connection Server instance or a pod of replicated instances.	
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.	

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

Option	Description	Fill In Your Value Here
Access group	<p>Select an access group in which to place the pool or leave the pool in the default root access group.</p> <p>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 <i>View Administration</i> document.</p> <p>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.</p>	
State	<p>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 will stop.</p>	
Connection Server restrictions	<p>You can restrict access to the pool to certain Connection Servers by clicking the Browse button and selecting one or more Connection Servers.</p> <p>If you intend to provide access to the 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.</p>	
Automatically logoff after disconnect	<ul style="list-style-type: none"> ■ 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. <p>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.</p>	
Allow user to initiate separate sessions from different client devices	<p>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.</p>	
Default display protocol	<p>Select the default display protocol. The choices are Microsoft RDP, PCoIP, and VMware Blast.</p>	
Allow users to choose protocol	<p>Specify whether users can choose display protocols other than the default.</p>	

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

Option	Description	Fill In Your Value Here
HTML Access	<p>Select Enabled to allow users to connect to remote desktops from within their Web browsers.</p> <p>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.</p> <p>To use HTML Access, you must install HTML Access in your View deployment. For more information, see <i>Using HTML Access</i>, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.</p> <p>To use HTML Access with VMware Identity Manager, you must pair View Connection Server with a SAML Authentication server, as described in the <i>View Administration</i> document. VMware Identity Manager must be installed and configured for use with View Connection Server.</p>	
Adobe Flash quality	<p>Determines the quality of Adobe Flash content that is displayed on Web pages.</p> <ul style="list-style-type: none"> ■ 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. <p>For more information, see “Adobe Flash Quality and Throttling,” on page 139.</p>	
Adobe Flash throttling	<p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>For more information, see “Adobe Flash Quality and Throttling,” on page 139.</p>	
Stop provisioning on error	<p>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.</p>	
Naming pattern	<p>The pattern you specify is used as a prefix in all the machine names, followed by a unique number to identify each machine.</p> <p>For details, see “Using a Naming Pattern for Automated Desktop Pools,” on page 130.</p>	
Max number of machines	<p>Specify the total number of machines in the pool.</p>	

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

Option	Description	Fill In Your Value Here
Number of spare (powered on) machines	Specify the number of machines to keep available for users. For details, see “Naming Machines Manually or Providing a Naming Pattern,” on page 128.	
Provision machines on demand Min number of machines Provision all machines up front	Specify whether to provision all machines when the pool is created or provision machines as they are needed. <ul style="list-style-type: none"> ■ 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 based on the Min number of machines value or the Number of spare (powered on) machines value, whichever is higher. Additional machines are created to maintain this minimum number of available machines as users connect to desktops. 	
Select separate datastores for replica and OS disks	You can store the replica (master) virtual machine disk on a high performance datastore and the instant clones on separate datastores. For details, see “Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones,” on page 249.	
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 as long as the pool exists.	
VM folder location	Select the folder in vCenter Server in which the desktop pool resides.	
Cluster	Select the vCenter Server cluster on which the desktop virtual machines run. You can not specify an ESXi host.	
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 Instant 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 clones. The Storage Overcommit parameter is always set to Unbounded and is not configurable.	
Domain	Select a Active Directory domain. The drop-down list shows the domains that are added when you configure instant clone domain administrators. See “Add an Instant Clone Domain Administrator,” on page 81	
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.	

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

Option	Description	Fill In Your Value Here
Power-off script	Specify a script to run on the machines before they are powered off. Provide the path to the script on the parent virtual machine and the script parameters.	
Post-synchronization script	Specify a script to run on the machines after they are created. Provide the path to the script on the parent virtual machine and the script parameters.	

Create an Instant-Clone Desktop Pool

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

Prerequisites

- 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 3, “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. Horizon 7 uses the snapshot as the base image to create the clones.
- Gather the configuration information for the pool. See [“Worksheet for Creating an Instant-Clone Desktop Pool,”](#) on page 81.
- Verify that you added an instant clone domain administrator in View Administrator.

Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Click **Add**.
- 3 Select **Automated Desktop Pool**.
- 4 On the vCenter Server page, choose **Instant 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.

In Horizon Administrator, you can view the machines 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 vCenter Server's inventory as long as the pool exists because various pool operations need this VM to be present. If you remove the VM from vCenter Server's inventory by mistake, you must add it back and then do a push image using the same image that the pool currently has.

What to do next

Entitle users to access the pool. See [“Add Entitlements to a Desktop or Application Pool,”](#) on page 159.

ClonePrep Guest Customization

ClonePrep customizes instant clones when they are created and works similarly as QuickPrep.

ClonePrep joins all instant clones to the Active Directory domain. The clones have the same computer security identifiers (SIDs) as their 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 Executes Scripts

ClonePrep 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.

Specifically, ClonePrep 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 call to `CreateProcess` is `CreateProcess(NULL, c:\myscript.cmd, ...)`.

Providing Paths to ClonePrep Scripts

You can specify the scripts to run when you create or edit the desktop pool. 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 executable. For example, instead of specifying `C:\script\myvb.vbs`, you need to specify `C:\windows\system32\cscript.exe c:\script\myvb.vbs`.

IMPORTANT Protect ClonePrep customization scripts from access by ordinary users. Place the scripts in a secure folder.

ClonePrep Script Timeout Limit

By default, ClonePrep terminates the scripts if their execution 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.

ClonePrep Script Account

ClonePrep runs the scripts using the account under which the VMware Horizon Instant Clone Agent service is configured to run. By default, this account is `Local System`.

Do not change this log on 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. Therefore, the scripts cannot perform actions that require those privileges.

The following privileges are removed from the process that runs ClonePrep scripts:

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

ClonePrep Script Logs

The ClonePrep script 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
```

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 and optionally puts a host in maintenance mode. After performing maintenance, you can run this command to take a host out of 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 or not to enter maintenance mode after the parent VMs are deleted. If the host is already in maintenance mode, setting this parameter to OFF takes the host out of maintenance mode.

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*

Specifying 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

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,”](#) on page 89
- [“Worksheet for Creating a Manual Desktop Pool,”](#) on page 89
- [“Create a Manual Desktop Pool,”](#) on page 91
- [“Create a Manual Pool That Contains One Machine,”](#) on page 92
- [“Desktop Pool Settings for Manual Pools,”](#) on page 93

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 7-1. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	<p>Choose the type of user assignment:</p> <ul style="list-style-type: none"> ■ 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. <p>For details, see “User Assignment in Desktop Pools,” on page 127.</p>	
vCenter Server	<p>The vCenter Server that manages the machines. This option appears only if the machines are virtual machines that are managed by vCenter Server.</p>	
Machine Source	<p>The virtual machines or physical computers that you want to include in the desktop pool.</p> <ol style="list-style-type: none"> 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. <p>To use PCoIP with machines that are unmanaged virtual machines or physical computers, you must use Teradici hardware.</p> <p>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.</p> <p>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.</p>	
Desktop Pool ID	<p>The pool name that users see when they log in and that identifies the pool in View Administrator.</p> <p>If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.</p>	

Table 7-1. Worksheet: Configuration Options for Creating a Manual Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Desktop Pool Settings	<p>Settings that determine the machine state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on.</p> <p>For details, see “Desktop Pool Settings for All Desktop Pool Types,” on page 135.</p> <p>For a list of the settings that apply to manual pools, see “Desktop Pool Settings for Manual Pools,” on page 93.</p>	
Transparent Page Sharing Scope	<p>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.</p> <p>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 View on the same ESXi host can share memory pages, regardless of which pool the machines reside in.</p> <p>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.</p>	

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 3, “Creating and Preparing a Parent Virtual Machine for Cloning,”](#) on page 19.

To prepare unmanaged virtual machines and physical computers, see [Chapter 2, “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 89.
- 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 135.

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 159.

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 3, “Creating and Preparing a Parent Virtual Machine for Cloning,”](#) on page 19.

To prepare an unmanaged virtual machine or physical computer, see [Chapter 2, “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 89.
- 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 135.

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 159.

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 7-2](#) 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 135.

Table 7-2. 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 their machines	Yes	Yes		

Table 7-2. 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

Setting Up Remote Desktop Services Hosts

8

Microsoft Remote Desktop Services (RDS) hosts provide desktop sessions and applications that users can access from client devices. If you plan to create RDS desktop pools or application pools, you must first set up RDS hosts.

This chapter includes the following topics:

- [“Remote Desktop Services Hosts,”](#) on page 95
- [“Install Remote Desktop Services on Windows Server 2008 R2,”](#) on page 97
- [“Install Remote Desktop Services on Windows Server 2012 or 2012 R2,”](#) on page 97
- [“Install Desktop Experience on Windows Server 2008 R2,”](#) on page 98
- [“Install Desktop Experience on Windows Server 2012 or 2012 R2,”](#) on page 98
- [“Restrict Users to a Single Session,”](#) on page 99
- [“Install Horizon Agent on a Remote Desktop Services Host,”](#) on page 99
- [“Enable Time Zone Redirection for RDS Desktop and Application Sessions,”](#) on page 102
- [“Enable Windows Basic Theme for Applications,”](#) on page 102
- [“Configure Group Policy to Start Runonce.exe,”](#) on page 103
- [“RDS Host Performance Options,”](#) on page 103
- [“Configuring 3D Graphics for RDS Hosts,”](#) on page 104

Remote Desktop Services Hosts

An RDS host is a server computer that hosts applications and desktop sessions for remote access. An RDS host can be a virtual machine or a physical server.

An RDS host has the Microsoft Remote Desktop Services role, the Microsoft Remote Desktop Session Host service, and Horizon Agent installed. Remote Desktop Services was previously known as Terminal Services. The Remote Desktop Session Host service allows a server to host applications and remote desktop sessions. With Horizon Agent installed on an RDS host, users can connect to applications and desktop sessions by using the display protocol PCoIP or Blast Extreme. Both protocols provide an optimized user experience for the delivery of remote content, including images, audio and video.

The performance of an RDS host depends on many factors. For information on how to tune the performance of different versions of Windows Server, see <http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx>.

Horizon 7 supports at most one desktop session and one application session per user on an RDS host.

When users submit print jobs concurrently from RDS desktops or applications that are hosted on the same RDS host, the ThinPrint server on the RDS host processes the print requests serially rather than in parallel. This can cause a delay for some users. Note that the print server does not wait for a print job to complete before processing the next one. Print jobs that are sent to different printers will print in parallel.

If a user launches an application and also an RDS desktop, and both are hosted on the same RDS host, they share the same user profile. If the user launches an application from the desktop, conflicts may result if both applications try to access or modify the same parts of the user profile, and one of the applications may fail to run properly.

The process of setting up applications or RDS desktops for remote access involves the following tasks:

- 1 Set up RDS hosts.
- 2 Create a farm. See [Chapter 9, “Creating Farms,”](#) on page 107.
- 3 Create an application pool or an RDS desktop pool. See [Chapter 10, “Creating Application Pools,”](#) on page 119 or [Chapter 11, “Creating RDS Desktop Pools,”](#) on page 123.
- 4 Entitle users and groups. See [Chapter 13, “Entitling Users and Groups,”](#) on page 159.
- 5 (Optional) Enable time zone redirection for RDS desktop and application sessions. See [“Enable Time Zone Redirection for RDS Desktop and Application Sessions,”](#) on page 102.

NOTE If smart card authentication is enabled, make sure that the Smart Card service is disabled on RDS hosts. Otherwise, authentication might fail. By default, this service is disabled.



CAUTION When a user launches an application, for example, a Web browser, it is possible for a user to gain access to the local drives on the RDS host that is hosting the application. This can happen if the application provides functions that cause Windows Explorer to run. To prevent this type of access to the RDS host, follow the procedure that is described in <http://support.microsoft.com/kb/179221> to prevent an application from running Windows Explorer.

Because the procedure described in <http://support.microsoft.com/kb/179221> affects both desktop and application sessions, it is recommended that you do not create RDS desktop pools and application pools on the same farm if you plan to follow the procedure in the Microsoft KB article, so that desktop sessions are not affected.

Installing Applications

If you plan to create application pools, you must install the applications on the RDS hosts. If you want Horizon 7 to automatically display the list of installed applications, you must install the applications so that they are available to all users from the **Start** menu. You can install an application at any time before you create the application pool. If you plan to manually specify an application, you can install the application at any time, either before or after creating an application pool.

IMPORTANT When you install an application, you must install it on all the RDS hosts in a farm and in the same location on each RDS host. If you do not, a health warning will appear on the View Administrator dashboard. In such a situation, if you create an application pool, users might encounter an error when they try to run the application.

When you create an application pool, Horizon 7 automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all of the RDS hosts in a farm. You can choose any applications from that list. In addition, you can manually specify an application that is not available to all users from the **Start** menu. There is no limit on the number of applications that you can install on an RDS host.

Install Remote Desktop Services on Windows Server 2008 R2

Remote Desktop Services (RDS) is one of the roles that a Windows Server can have. You must install this role to set up an RDS host that runs Windows Server 2008 R2.

Prerequisites

- Verify that the RDS host is running Windows Server 2008 R2 Service Pack 1 (SP1).
- Verify that the RDS host is part of the Active Directory domain for the Horizon 7 deployment.
- Install the Microsoft hotfix rollup that is documented in <http://support.microsoft.com/kb/2775511>.
- Install the Microsoft update <https://support.microsoft.com/en-us/kb/2973201>.

Procedure

- 1 Log in to the RDS host as an administrator.
- 2 Start Server Manager.
- 3 Select **Roles** in the navigation tree.
- 4 Click **Add Roles** to start the Add Role wizard.
- 5 Select the role **Remote Desktop Services**.
- 6 On the Select Role Services page, select **Remote Desktop Session Host**.
- 7 On the Specify Authentication Method page, select either **Require Network Level Authentication** or **Do not require Network Level Authentication**, whichever is appropriate.
- 8 On the Configure Client Experience page, select the functionality that you want to provide to users.
- 9 Follow the prompts and finish the installation.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature. The steps for installing Desktop Experience differ on Windows Server 2008 R2 and Windows Server 2012 or 2012 R2.

Restrict users to a single desktop session. See [“Restrict Users to a Single Session,”](#) on page 99.

Install Remote Desktop Services on Windows Server 2012 or 2012 R2

Remote Desktop Services is one of the roles that a Windows Server 2012 or 2012 R2 can have. You must install this role to set up an RDS host.

Prerequisites

- Verify that the RDS host is running Windows Server 2012 or Windows Server 2012 R2.
- Verify that the RDS host is part of the Active Directory domain for the Horizon 7 deployment.

Procedure

- 1 Log in to the RDS host 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, select **Remote Desktop Services**.

- 7 On the Select Features page, accept the defaults.
- 8 On the Select Role Services page, select **Remote Desktop Session Host**.
- 9 Follow the prompts and finish the installation.

What to do next

If you plan to use HTML Access or scanner redirection, install the Desktop Experience feature. The steps for installing Desktop Experience differ on Windows Server 2008 R2 and Windows Server 2012 or 2012 R2.

Restrict users to a single desktop session. See [“Restrict Users to a Single Session,”](#) on page 99.

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.

Restrict Users to a Single Session

Horizon 7 supports at most one desktop session and one application session per user on an RDS host. You must configure the RDS host to restrict users to a single session. For Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, you can restrict users to a single session by enabling the group policy setting

Restrict Remote Desktop Services users to a single Remote Desktop Services session. This setting is located in the folder Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections. For Windows Server 2008 R2, you can also use the following procedure to restrict users to a single session.

Prerequisites

- Install the Remote Desktop Services role as described in “[Install Remote Desktop Services on Windows Server 2008 R2](#),” on page 97.

Procedure

- 1 Click **Start > Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration**.
- 2 On the Edit Settings pane, under General, double-click **Restrict each user to a single session**.
- 3 In the Properties dialog box, on the General tab, select **Restrict each user to a single session** and click **OK**.

What to do next

Install Horizon Agent on the RDS host. See “[Install Horizon Agent on a Remote Desktop Services Host](#),” on page 99.

Install Horizon Agent on a Remote Desktop Services Host

Horizon Agent communicates with Connection Server and supports the display protocols PCoIP and Blast Extreme. You must install Horizon Agent on an RDS Host.

Prerequisites

- Install the Remote Desktop Services role as described in “[Install Remote Desktop Services on Windows Server 2008 R2](#),” on page 97 or “[Install Remote Desktop Services on Windows Server 2012 or 2012 R2](#),” on page 97.
- Restrict users to a single desktop session. See “[Restrict Users to a Single Session](#),” on page 99.
- Familiarize yourself with the Horizon Agent custom setup options. See “[Horizon Agent Custom Setup Options for an RDS Host](#),” on page 100.
- 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 Log in as an administrator.
- 2 To start the Horizon Agent installation program, double-click the installer file.

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

- 3 Select the Internet Protocol (IP) version, **IPv4** or **IPv6**.
You must install all View components with the same IP version.
- 4 Select your custom setup options.
Do not select the View Composer Agent option if you are installing Horizon Agent on an RDS host that will be in a manual farm.
- 5 In the **Server** text box, type the host name or IP address of a Connection Server host.
During installation, the installer registers the RDS host with this Connection Server instance. After registration, the specified Connection Server instance, and any additional instances in the same Connection Server group, can communicate with the RDS host.
- 6 Select an authentication method to register the RDS host with the Connection Server instance.

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

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.

- 7 Follow the prompts and finish the installation.

What to do next

Create a farm. See [Chapter 9, “Creating Farms,”](#) on page 107.

Horizon Agent Custom Setup Options for an RDS Host

When you install Horizon Agent on an RDS host, you can select 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 8-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 Environment

Option	Description
USB Redirection	Gives users access to locally connected USB storage devices. Specifically, redirection of USB flash drives and hard disks is supported in RDS desktops and applications. Redirection of other types of USB devices, and other types of USB storage devices such as security storage drives and USB CD-ROM, is not supported in RDS desktops and applications. This setup option is not selected by default. You must select the option to install it. This option is available on RDS hosts that run Windows Server 2012 or 2012 R2 but not Windows Server 2008 R2. For guidance on using USB redirection securely, see the <i>View Security</i> guide. For example, you can use group policy settings to disable USB redirection for specific users.
HTML Access	Allows users to connect to RDS desktops and applications by using HTML Access. The HTML Access Agent is installed when this setup option is selected. This agent must be installed on RDS hosts to allow users to make connections with HTML Access
3D RDSH	Provides 3D graphics support to applications that run on this RDS host.

Table 8-1. Horizon Agent Custom Setup Options for an RDS Host in an IPv4 Environment (Continued)

Option	Description
View Composer Agent	Select this option if this machine is a parent virtual machine for the creation of an automated farm. Do not select this option if this machine is an RDS host in a manual farm.
Client Drive Redirection	Allows Horizon Client users to share local drives with their RDS desktops and applications. After this setup option is installed, no further configuration is required on the RDS host. Client Drive Redirection is also supported on VDI desktops that run on single-user virtual machines and 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. In Horizon 6.0.1 and later, virtual printing is supported on the following remote desktops and applications: <ul style="list-style-type: none"> ■ 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 ■ Hosted Apps ■ Hosted Apps that are launched from Horizon Client inside remote desktops In Horizon 6.0 and earlier, virtual printing is supported on desktops that are deployed on single-user, Windows Desktop machines. 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	Lets vRealize Operations Manager work with vRealize Operations Manager for Horizon.
Scanner Redirection	Redirects scanning devices that are connected to the client system so that they can be used on the RDS desktop or application. You must install the Desktop Experience feature in the Windows Server operating system on the RDS hosts to make this option available in the Horizon Agent installer. This setup option is not installed by default on Windows Server guest operating systems. You must select the option to install it. Scanner redirection is available in Horizon 6.0.2 and later releases.

In an IPv6 environment, there are no optional features.

Table 8-2. Horizon Agent Features That Are Installed Automatically on an RDS Host

Option	Description
PCoIP Agent	Allows users to connect to applications and RDS desktops using the PCoIP display protocol. You must install this component if you plan to create application pools because users can only connect to applications using PCoIP.
Windows Media Multimedia Redirection (MMR)	Provides multimedia redirection for RDS desktops. 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 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 without using the Start menu or Taskbar.
PSG Agent	Installs the PCoIP Secure Gateway on RDS hosts to implement the PCoIP display protocol for desktop and application sessions that run on RDS hosts.
VMwareRDS	Provides the VMware implementation of Remote Desktop Services functionality.

In an IPv6 environment, the automatically installed features are PCoIP Agent, PSG Agent, and VMwareRDS.

For additional features that are supported on RDS hosts, see "Feature Support Matrix for Horizon Agent" in the *View Architecture Planning* document.

Enable Time Zone Redirection for RDS Desktop and Application Sessions

If an RDS host is in one time zone and a user is in another time zone, by default, when the user connects to an RDS desktop, the desktop displays time that is in the time zone of the RDS host. You can enable the Time Zone Redirection group policy setting to make the RDS desktop display time in the local time zone. This policy setting applies to application sessions as well.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.
The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See [“Create GPOs for View Group Policies,”](#) on page 298.
- Verify that the Horizon 7 RDS ADMX files are added to Active Directory. See [“Add the Remote Desktop Services ADMX Files to Active Directory,”](#) on page 284.
- Familiarize yourself with the group policy settings. See [“RDS Device and Resource Redirection Settings,”](#) on page 286.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Horizon View RDSH Services > Remote Desktop Session Host > Device and Resource Redirection**.
- 5 Enable the setting **Allow time zone redirection**.

Enable Windows Basic Theme for Applications

If a user has never connected to a desktop on an RDS host, and the user launches an application that is hosted on the RDS host, the Windows basic theme is not applied to the application even if a GPO setting is configured to load the Aero-styled theme. Horizon 7 does not support the Aero-styled theme but supports the Windows basic theme. To make the Windows basic theme apply to the application, you must configure another GPO setting.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.
The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See [“Create GPOs for View Group Policies,”](#) on page 298.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Administrative Templates > Control Panel > Personalization**.

- 5 Enable the setting **Force a specific visual style file or force Windows classic** and set the Path to Visual Style as `%windir%\resources\Themes\Aero\Aero.msstyles`.

Configure Group Policy to Start Runonce.exe

By default, some applications that rely on the Explorer.exe file may not run in an application session. To avoid this issue, you must configure a GPO setting to start runonce.exe.

Prerequisites

- Verify that the Group Policy Management feature is available on your Active Directory server.

The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See [“Create GPOs for View Group Policies,”](#) on page 298.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain and **Group Policy Objects**.
- 3 Right-click the GPO that you created for the group policy settings and select **Edit**.
- 4 In the Group Policy Management Editor, navigate to **User Configuration > Policies > Windows Settings > Scripts (Logon/Logoff)**.
- 5 Double-click **Logon** and click **Add**.
- 6 In the Script Name box, type **runonce.exe**.
- 7 In the Script Parameters box, type **/AlternateShellStartup**.

RDS Host Performance Options

You can optimize Windows for either foreground programs or background services by setting performance options. By default, Horizon 7 disables certain performance options for RDS hosts for all supported versions of Windows Server.

The following table shows the performance options that are disabled by Horizon 7.

Table 8-3. Performance Options Disabled by Horizon 7

Performance Options Disabled by Horizon 7
Animate windows when minimizing and maximizing
Show shadows under mouse pointer
Show shadows under windows
Use drop shadow for icon labels on the desktop
Show windows contents while dragging

The five performance options that are disabled by Horizon 7 correspond to four Horizon 7 settings in the registry. The following table shows the Horizon 7 settings and their default registry values. The registry values are all located in the registry subkey `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. You can re-enable the performance options by setting one or more of the Horizon 7 registry values to **false**.

Table 8-4. Horizon 7 Settings Related to Windows Performance Options

Horizon 7 Setting	Registry Value
Disable cursor shadow	DisableMouseShadows
Disable full window drag	DisableFullWindowDrag
Disable ListView shadow	DisableListViewShadow
Disable Window Animation	DisableWindowAnimation

Configuring 3D Graphics for RDS Hosts

With 3D graphics configured for RDS hosts, both applications in application pools and applications running on RDS desktops can display 3D graphics.

The following 3D graphics options are available:

NVIDIA GRID vGPU (shared GPU hardware acceleration) A physical GPU on an ESXi host is shared among multiple virtual machines. Requires ESXi 6.0 or later.

AMD Multiuser GPU using vDGA A physical GPU on an ESXi host is shared among multiple virtual machines. Requires ESXi 6.0 or later.

Virtual Dedicated Graphics Acceleration (vDGA) A physical GPU on an ESXi host is dedicated to a single virtual machine. Requires ESXi 5.5 or later.

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.

With vDGA, you allocate an entire GPU to a single machine for maximum performance. The RDS host must be in a manual farm.

With AMD Multiuser GPU using vDGA, you can share an AMD GPU between multiple RDS hosts by making it appear as multiple PCI passthrough devices. The RDS host must be in a manual farm.

With NVIDIA GRID vGPU, each graphics card can support multiple RDS hosts and the RDS hosts must be in a manual farm. If an ESXi host has multiple physical GPUs, you can also configure the way the ESXi host assigns virtual machines to the GPUs. By default, the ESXi host assigns virtual machines to the physical GPU with the fewest virtual machines already assigned. This is called performance mode. You can also choose consolidation mode, where 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. To configure consolidation mode, edit the `/etc/vmware/config` file on the ESXi host and add the following entry:

```
vGPU.consolidation = "true"
```

3D graphics is only supported when you use the PCoIP or VMware Blast protocol. Therefore, the farm must use PCoIP or VMware Blast as the default protocol and users must not be allowed to choose the protocol.

Overview of Steps for Configuring 3D Graphics

This overview describes tasks that you must perform in vSphere and Horizon 7 to configure 3D graphics. For more information about setting up NVIDIA GRID vGPU, see the document [NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#). For more information about setting up vDGA, see the document [Graphics Acceleration in View Virtual Desktops](#). For more information about setting up AMD Multiuser GPU using vDGA, see [“Preparing to Use the Capabilities of AMD Multiuser GPU Using vDGA,”](#) on page 154.

- 1 Set up an RDS host virtual machine. For more information, see [Chapter 8, “Setting Up Remote Desktop Services Hosts,”](#) on page 95.
- 2 Add the graphics PCI device to the virtual machine. See "Other Virtual Machine Device Configuration" in the chapter "Configuring Virtual machine Hardware" in the *vSphere Virtual Machine Administration* document. Be sure to click **Reserve all memory** when adding the device.
- 3 On the virtual machine, install the device driver for the graphics card.
- 4 Add the RDS host to a manual farm, create an RDS desktop pool, connect to the desktop using PCoIP, and activate the display adapter.

You do not need to configure 3D graphics for RDS hosts in View Administrator. Selecting the option **3D RDSH** when you install Horizon Agent is sufficient. By default, this option is not selected and 3D graphics is disabled.

Creating Farms

A farm is a group of RDS hosts that provides a common set of applications or RDS desktops to users.

This chapter includes the following topics:

- [“Farms,”](#) on page 107
- [“Preparing a Parent Virtual Machine for an Automated Farm,”](#) on page 108
- [“Worksheet for Creating a Manual Farm,”](#) on page 111
- [“Worksheet for Creating an Automated Farm,”](#) on page 112
- [“Create a Manual Farm,”](#) on page 116
- [“Create an Automated Farm,”](#) on page 117

Farms

Farms simplify the task of managing RDS hosts, RDS desktops, and applications in an enterprise. You can create manual or automated farms to serve groups of users that vary in size or have different desktop or application requirements.

A manual farm consists of RDS hosts that already exist. The RDS hosts can be physical or virtual machines. You manually add the RDS hosts when you create the farm.

An automated farm consists of RDS host that are linked-clone virtual machines in vCenter Server. View Composer creates the virtual machines based on the parameters that you specify when you create the farm. The virtual machines are cloned from a single parent virtual machine and are linked to the parent in a mechanism that reduces the amount of storage that the virtual machines require.

When you create an application pool or an RDS desktop pool, you must specify one and only one farm. The RDS hosts in a farm can host RDS desktops, applications, or both. A farm can support at most one RDS desktop pool, but it can support multiple application pools. A farm can support both types of pools simultaneously.

Farms provide the following conveniences:

- **Load balancing**

By default, Horizon 7 balances the load of the RDS desktop sessions and the application sessions across all the RDS hosts in the farm. You can control the placement of new application sessions by writing and configuring load balancing scripts. For more information, see “Configuring Load Balancing for RDS Hosts” in the *View Administration* document.
- **Redundancy**

If one RDS host in a farm is offline, the other RDS hosts in the farm continue to provide applications and desktops to users.

- Scalability

A farm can have a variable number of RDS hosts. You can create farms with different numbers of RDS hosts to serve user groups of different sizes.

Farms have the following properties:

- A Horizon 7 pod can have a maximum of 200 farms.
- A farm can have a maximum of 200 RDS hosts.
- The RDS hosts in a farm can run any supported version of Windows Server. See "System Requirements for Guest Operating Systems" in the *View Installation* document.
- Automated farms support the View Composer recompose operation but do not support the refresh or rebalance operation. You can recompose an automated farm but not a subset of the RDS hosts in the farm.

IMPORTANT Microsoft recommends that you configure roaming profiles for users separately for each farm. The profiles should not be shared between farms or users' physical desktops since profile corruption and data loss may occur if a user is simultaneously logged in to two machines that load the same profile.

Preparing a Parent Virtual Machine for an Automated Farm

To create an automated farm, you must first prepare a parent virtual machine. View Composer uses this parent virtual machine to create linked-clone virtual machines, which are the RDS hosts in the farm.

- [Prepare an RDS Host Parent Virtual Machine](#) on page 108
The View Composer service requires a parent virtual machine from which you generate a base image for creating linked clones.
- [Activating Windows on Linked-Clone RDS Hosts](#) on page 110
To make sure that View Composer properly activates Windows Server operating systems on linked-clone RDS hosts, 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 110
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.

Prepare an RDS Host Parent Virtual Machine

The View Composer service requires a parent virtual machine from which you generate a base image for creating linked clones.

Prerequisites

- Verify that an RDS host virtual machine is set up. See [Chapter 8, "Setting Up Remote Desktop Services Hosts,"](#) on page 95. To set up the RDS host, be sure not to use a virtual machine that was previously registered to View Connection Server.

A parent virtual machine that you use for View Composer must either belong to the same Active Directory domain as the domain that the linked-clone machines will join or be a member of the local WORKGROUP.

- Verify that the virtual machine was not converted from a View Composer linked clone. A virtual machine that is converted from a linked clone has the clone's internal disk and state information. A parent virtual machine cannot have state information.

IMPORTANT Linked clones and virtual machines that were converted from linked clones are not supported as parent virtual machines.

- When you install Horizon Agent on the parent virtual machine, select the **View Composer Agent** option. See “[Install Horizon Agent on a Remote Desktop Services Host](#),” on page 99.

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 recompose operation to update Horizon Agent.

NOTE 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 do 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.
- 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](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx).
- To implement the RDS host load balancing feature, modify the RDS host parent virtual machine as described in "Configuring Load Balancing for RDS Hosts" in the *View Administration* document.

Procedure

- Remove the DHCP lease on the parent virtual machine to avoid copying a leased IP address to the linked clones in the farm.
 - 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. The View Composer service does not support multiple disk partitions. Multiple virtual disks are supported.
- 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. Linked clones that are created or recomposed from the virtual machine will not contain the independent disk.
- Disable the hibernation option to reduce the size of linked-clone OS disks that are created from the parent virtual machine.
- 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 of linked-clone machines. As each linked clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in repeated searches and customization delays.
- In vSphere Client, disable the vApp Options setting on the parent virtual machine.

- On 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"`

If left enabled, 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>.

- On Windows Server 2012 machines, apply the Microsoft hotfix available at <https://support.microsoft.com/en-us/kb/3020396>.

This hotfix allows Sysprep to customize a Windows Server 2012 virtual machine that has the RDS role enabled. Without the hotfix, Sysprep customization will fail on the Windows Server 2012 linked-clone machines that are deployed in an automated farm.

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 used as the baseline configuration for the first set of linked-clone machines that are anchored to the parent virtual machine.

IMPORTANT Before you take a snapshot, completely shut down the parent virtual machine by using the **Shut Down** command in the guest operating system.

Activating Windows on Linked-Clone RDS Hosts

To make sure that View Composer properly activates Windows Server operating systems on linked-clone RDS hosts, 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 View Composer does not support Multiple Activation Key (MAK) licensing.

Before you create linked-clone machines with View Composer, you must use volume activation to activate the operating system on the parent virtual machine.

When a linked-clone machine is created, and each time the linked clone is recomposed, the View Composer agent uses the parent virtual machine's KMS server to activate the operating system on the linked clone.

For KMS licensing, View Composer uses the KMS server that is configured to activate the parent virtual machine. The KMS server treats an activated linked 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.

Worksheet for Creating a Manual Farm

When you create a manual farm, the Add Farm wizard prompts you to configure certain settings.

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

Table 9-1. Worksheet: Configuration Settings for Creating a Manual Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in View Administrator.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the <i>View Administration</i> document.	
Default display protocol	Select VMware Blast , PCoIP or RDP . RDP applies to desktop pools only. The display protocol for application pools is always VMware Blast or PCoIP . If you select RDP and you plan to use this farm to host application pools, you must set Allow users to choose protocol to Yes . The default is PCoIP .	
Allow users to choose protocol	Select Yes or No . This setting applies to RDS desktop pools only. If you select Yes , users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is Yes .	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select Never or set the number of minutes as the timeout value. The default is After 1 minute .	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect .	

Table 9-1. Worksheet: Configuration Settings for Creating a Manual Farm (Continued)

Setting	Description	Fill in Your Value Here
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select Never , Immediate , or After ... minutes . Use caution when you select Immediate or After ... minutes . When a disconnected session is logged off, the session is lost. The default is Never .	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the Enabled box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	

NOTE Unlike an automated farm, a manual farm does not have the setting **Max sessions per RDS server**, because a manual farm can have RDS hosts that are not identical. For RDS hosts in a manual farm, you can edit individual RDS hosts and change the equivalent setting **Number of connections**.

Worksheet for Creating an Automated Farm

When you create an automated farm, the Add Farm wizard prompts you to configure certain settings.

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

Table 9-2. Worksheet: Configuration Settings for Creating an Automated Farm

Setting	Description	Fill in Your Value Here
ID	Unique name that identifies the farm in View Administrator.	
Description	Description of this farm.	
Access group	Access group in which to place all the pools in this farm. For more information about access groups, see the role-based delegated administration chapter in the <i>View Administration</i> document.	
Default display protocol	Select VMware Blast , PCoIP or RDP . RDP applies to desktop pools only. The display protocol for application pools is always VMware Blast or PCoIP . If you select RDP and you plan to use this farm to host application pools, you must set Allow users to choose protocol to Yes . The default is PCoIP .	
Allow users to choose protocol	Select Yes or No . This setting applies to RDS desktop pools only. If you select Yes , users can choose the display protocol when they connect to an RDS desktop from Horizon Client. The default is Yes .	
Empty session timeout (applications only)	Determines the amount of time that an empty application session is kept open. An application session is empty when all the applications that run in the session are closed. While the session is open, users can open applications faster. You can save system resources if you disconnect or log off empty application sessions. Select Never or set the number of minutes as the timeout value. The default is After 1 minute .	
When timeout occurs	Determines whether an empty application session is disconnected or logged off after the Empty session timeout limit is reached. Select Disconnect or Log off . A session that is logged off frees up resources, but opening an application takes longer. The default is Disconnect .	

Table 9-2. Worksheet: Configuration Settings for Creating an Automated Farm (Continued)

Setting	Description	Fill in Your Value Here
Log off disconnected session	Determines when a disconnected session is logged off. This setting applies to both desktop and application sessions. Select Never , Immediate , or After ... minutes . Use caution when you select Immediate or After ... minutes . When a disconnected session is logged off, the session is lost. The default is Never .	
Allow HTML Access to desktops and applications on this farm	Determines whether HTML Access to RDS desktops and applications is allowed. Check the Enabled box to allow HTML Access to RDS desktops and applications. When you edit this setting after a farm is created, the new value applies to existing desktops and applications as well as new ones.	
Max sessions per RDS server	Determines the maximum number of sessions that an RDS host can support. Select Unlimited or No More Than The default is Unlimited .	
Enable provisioning	Select this checkbox to enable provisioning after you finish this wizard. This box is checked by default.	
Stop provisioning on error	Select this checkbox to stop provisioning when a provisioning error occurs. This box is checked by default.	
Naming pattern	Specify a prefix or a name format. View will append or insert an automatically generated number starting with 1 to form the machine name. If you want the number at the end, simply specify a prefix. Otherwise, specify {n} anywhere in a character string and {n} will be replaced by the number. You can also specify {n:fixed=<number of digits>} , where fixed=<number of digits> indicates the number of digits to be used for the number. For example, specify vm-{n:fixed=3}-sales and the machine names will be vm-001-sales, vm-002-sales, and so on. NOTE Each machine name, including the automatically generated number, has a 15-character limit.	
Max number of machines	The number of machines to be provisioned.	
Minimum number of ready (provisioned) machines during View Composer maintenance operations	This setting lets you keep the specified number of machines available to accept connection requests while View Composer recomposes the machines in the farm.	
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 235	
Select separate datastores for replica and OS disks	(Available only if you do not use Virtual SAN) You can place replica and OS disks on different datastores for performance or other reasons.	
Parent VM	Select a parent virtual machine from the list. Be aware that the list includes virtual machines that do not have View Composer Agent installed. You must not select any of those machines because View Composer Agent is required. A good practice is to use a naming convention that indicates whether a virtual machine has View Composer Agent installed.	

Table 9-2. Worksheet: Configuration Settings for Creating an Automated Farm (Continued)

Setting	Description	Fill in Your Value Here
Snapshot	<p>Select the snapshot of the parent virtual machine to use as the base image for the farm.</p> <p>Do not delete the snapshot and parent virtual machine from vCenter Server, unless no linked clones in the farm 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 farm, according to farm policies. The parent virtual machine and snapshot are also required for View Composer maintenance operations.</p>	
VM folder location	Select the folder in vCenter Server in which the farm resides.	
Host or cluster	<p>Select the ESXi host or cluster on which the desktop virtual machines run.</p> <p>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.</p> <p>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.</p> <p>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.</p>	
Resource pool	Select the vCenter Server resource pool in which the farm resides.	
Datastores	<p>Select one or more datastores on which to store the farm.</p> <p>A table on the Select Linked Clone Datastores page of the Add Farm wizard provides high-level guidelines for estimating the farm'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 241.</p> <p>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 248.</p> <p>NOTE If you use Virtual SAN, select only one datastore.</p>	
Storage Overcommit	<p>Determine the storage-overcommit level at which linked-clones are created on each datastore.</p> <p>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 "Storage Overcommit for View Composer Linked-Clone Virtual Machines," on page 245.</p> <p>NOTE This setting has no effect if you use Virtual SAN.</p>	

Table 9-2. Worksheet: Configuration Settings for Creating an Automated Farm (Continued)

Setting	Description	Fill in Your Value Here
Use native NFS snapshots (VAAI)	<p>(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.</p> <p>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.</p> <p>This feature is supported on vSphere 5.0 and later.</p> <p>For details, see “Using VAAI Storage for View Composer Linked Clones,” on page 253.</p>	
Reclaim VM disk space	<p>(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.</p> <p>This feature is supported on vSphere 5.1 and later. The linked-clone virtual machines must be virtual hardware version 9 or later.</p> <p>For details, see “Reclaim Disk Space on View Composer Linked Clones,” on page 251.</p>	
Initiate reclamation when unused space on VM exceeds:	<p>(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.</p> <p>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.</p> <p>For example: 2 GB.</p> <p>The default value is 1 GB.</p>	
Blackout Times	<p>Configure days and times during which the reclamation of virtual machine disk space do not take place.</p> <p>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.</p> <p>For details, see “Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones,” on page 254.</p>	
Transparent Page Sharing Scope	<p>Select the level at which to allow transparent page sharing (TPS). The choices are Virtual Machine (the default), Farm, Pod, or Global. If you turn on TPS for all the machines in the farm, 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.</p> <p>Page sharing happens on the ESXi host. For example, if you enable TPS at the farm level but the farm is spread across multiple ESXi hosts, only virtual machines on the same host and within the same farm will share pages. At the global level, all machines managed by View on the same ESXi host can share memory pages, regardless of which farm the machines reside in.</p> <p>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.</p>	

Table 9-2. Worksheet: Configuration Settings for Creating an Automated Farm (Continued)

Setting	Description	Fill in Your Value Here
Domain	<p>Select the Active Directory domain and user name.</p> <p>View Composer requires certain user privileges to farm. The domain and user account are used by Sysprep to customize the linked-clone machines.</p> <p>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 Farm wizard to create a farm, you must select one domain and user from the list.</p> <p>For information about configuring View Composer, see the <i>View Administration</i> document.</p>	
AD container	<p>Provide the Active Directory container relative distinguished name.</p> <p>For example: CN=Computers</p> <p>When you run the Add Farm wizard, you can browse your Active Directory tree for the container.</p>	
Allow reuse of pre-existing computer accounts	<p>Select this setting to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This setting lets you control the computer accounts that are created in Active Directory.</p> <p>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.</p> <p>The existing computer accounts must be located in the Active Directory container that you specify with the Active Directory container setting.</p> <p>When this setting is disabled, a new AD computer account is created when View Composer provisions a linked clone. This setting is disabled by default.</p> <p>For details, see “Use Existing Active Directory Computer Accounts for Linked Clones,” on page 76.</p>	
Use a customization specification (Sysprep)	<p>Provide a Sysprep customization specification to customize the virtual machines.</p>	

Create a Manual Farm

You create a manual farm as part of the process to give users access to applications or RDS desktops.

Prerequisites

- Set up the RDS hosts that belong to the farm. See [Chapter 8, “Setting Up Remote Desktop Services Hosts,”](#) on page 95.
- Verify that all the RDS hosts have the Available status. In View Administrator, select **View Configuration > Registered Machines** and check the status of each RDS host on the RDS Hosts tab.
- Gather the configuration information you must provide to create the farm. See [“Worksheet for Creating a Manual Farm,”](#) on page 111.

Procedure

- 1 In View Administrator, click **Resources > Farms**.
- 2 Click **Add** to enter the configuration information that you gathered in the worksheet.
- 3 Select **Manual Farm**.

- 4 Follow the prompts in the wizard to create the farm.

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.

- 5 Select the RDS hosts to add to the farm and click **Next**.
- 6 Click **Finish**.

In View Administrator, you can now view the farm by clicking **Resources > Farms**.

What to do next

Create an application pool or an RDS desktop pool. See [Chapter 10, “Creating Application Pools,”](#) on page 119 or [Chapter 11, “Creating RDS Desktop Pools,”](#) on page 123.

Create an Automated Farm

You create an automated farm as part of the process to give users access to applications or RDS desktops.

Prerequisites

- Verify that the View Composer service is installed. 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. Both Horizon Agent and View Composer Agent must be installed on the parent virtual machine. See [“Preparing a Parent Virtual Machine for an Automated Farm,”](#) on page 108.
- 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 farm. See [“Worksheet for Creating an Automated Farm,”](#) on page 112.

Procedure

- 1 In View Administrator, click **Resources > Farms**.
- 2 Click **Add** to enter the configuration information that you gathered in the worksheet.
- 3 Select **Automated Farm**.
- 4 Follow the prompts in the wizard to create the farm.

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 now view the farm by clicking **Resources > Farms**.

What to do next

Create an application pool or an RDS desktop pool. See [Chapter 10, “Creating Application Pools,”](#) on page 119 or [Chapter 11, “Creating RDS Desktop Pools,”](#) on page 123.

Creating Application Pools

One of the tasks that you perform to give users remote access to an application is to create an application pool. Users who are entitled to an application pool can access the application remotely from a variety of client devices.

This chapter includes the following topics:

- [“Application Pools,”](#) on page 119
- [“Worksheet for Creating an Application Pool Manually,”](#) on page 120
- [“Create an Application Pool,”](#) on page 120

Application Pools

With application pools, you can deliver a single application to many users. The application runs on a farm of RDS hosts.

When you create an application pool, you deploy an application in the data center that users can access from anywhere on the network. For an introduction to application pools, see [“Farms, RDS Hosts, and Desktop and Application Pools,”](#) on page 9.

An application pool has a single application and is associated with a single farm. To avoid errors, you must install the application on all of the RDS hosts in the farm.

When you create an application pool, View automatically displays the applications that are available to all users rather than individual users from the **Start** menu on all the RDS hosts in the farm. You can select one or more applications from the list. If you select multiple applications from the list, a separate application pool is created for each application. You can also manually specify an application that is not on the list. If an application that you want to manually specify is not already installed, View displays a warning message.

When you create an application pool, you cannot specify the access group in which to place the pool. For application pools and RDS desktop pools, you specify the access group when you create a farm.

An application supports the PCoIP and VMware Blast display protocols. To enable HTML Access, see “Prepare Desktops, Pools, and Farms for HTML Access,” in the “Setup and Installation” chapter in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Worksheet for Creating an Application Pool Manually

When you create an application pool and manually specify an application, the Add Application Pools wizard prompts you for information about the application. It is not a requirement that the application is already installed on any RDS host.

You can print this worksheet and write down the properties of an application when you specify the application manually.

Table 10-1. Worksheet: Application Properties for Creating an Application Pool Manually

Property	Description	Fill in Your Value Here
ID	Unique name that identifies the pool in View Administrator. This field is required.	
Display Name	Pool name that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as ID .	
Version	Version of the application.	
Publisher	Publisher of the application.	
Path	Full pathname of the application. For example, C:\Program Files\app1.exe. This field is required.	
Start Folder	Full pathname of the starting directory for the application.	
Parameters	Parameters to pass to the application when it starts. For example, you can specify <code>-username user1 -loglevel 3</code> .	
Description	Description of this application pool.	

Create an Application Pool

You create an application pool as part of the process to give users access to an application that runs on RDS hosts.

Prerequisites

- Set up RDS hosts. See [Chapter 8, “Setting Up Remote Desktop Services Hosts,”](#) on page 95.
- Create a farm that contains the RDS hosts. See [Chapter 9, “Creating Farms,”](#) on page 107.
- If you plan to add the application pool manually, gather information about the application. See [“Worksheet for Creating an Application Pool Manually,”](#) on page 120.

Procedure

- 1 In View Administrator, click **Catalog > Application Pools**.
- 2 Click **Add**.
- 3 Follow the prompts in the wizard to create the pool.

If you choose to add an application pool manually, use the configuration information you gathered in the worksheet. If you select applications from the list that View Administrator displays, you can select multiple applications. A separate pool is created for each application.

In View Administrator, you can now view the application pool by clicking **Catalog > Application Pools**.

What to do next

Entitle users to access the pool. See [Chapter 13, "Entitling Users and Groups,"](#) on page 159.

Make sure that your end users have access to Horizon Client 3.0 or later software, which is required to support RDS applications.

If you need to ensure that View Connection Server launches the application only on RDS hosts that have sufficient resources to run the application, configure an anti-affinity rule for the application pool. For more information, see "Configure an Anti-Affinity Rule for an Application Pool" in the *View Administration* document.

Creating RDS Desktop Pools

One of the tasks that you perform to give users remote access to session-based desktops is to create a Remote Desktop Services (RDS) desktop pool. An RDS desktop pool has properties that can satisfy some specific needs of a remote desktop deployment.

This chapter includes the following topics:

- [“Understanding RDS Desktop Pools,”](#) on page 123
- [“Create an RDS Desktop Pool,”](#) on page 124
- [“Desktop Pool Settings for RDS Desktop Pools,”](#) on page 124
- [“Configure Adobe Flash Throttling with Internet Explorer for RDS Desktop Pools,”](#) on page 125

Understanding RDS Desktop Pools

An RDS desktop pool is one of three types of desktop pools that you can create. This type of pool was known as a Microsoft Terminal Services pool in previous View releases.

An RDS desktop pool and an RDS desktop have the following characteristics:

- An RDS desktop pool is associated with a farm, which is a group of RDS hosts. Each RDS host is a Windows server that can host multiple RDS desktops.
- An RDS desktop is based on a session to an RDS host. In contrast, a desktop in an automated desktop pool is based on a virtual machine, and a desktop in a manual desktop pool is based on a virtual or physical machine.
- An RDS desktop supports the RDP, PCoIP, and VMware Blast display protocols. To enable HTML Access, see “Prepare Desktops, Pools, and Farms for HTML Access,” in the “Setup and Installation” chapter in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- An RDS desktop pool is only supported on Windows Server operating systems that support the RDS role and are supported by View. See “System Requirements for Guest Operating Systems” in the *View Installation* document.
- View provides load balancing of the RDS hosts in a farm by directing connection requests to the RDS host that has the least number of active sessions.
- Because an RDS desktop pool provides session-based desktops, it does not support operations that are specific to a linked-clone desktop pool, such as refresh, recompose, and rebalance.
- If an RDS host is a virtual machine that is managed by vCenter Server, you can use snapshots as base images. You can use vCenter Server to manage the snapshots. The use of snapshots on RDS host virtual machines is transparent to View.

- RDS desktops do not support View Persona Management.
- The copy and paste feature is disabled by default for HTML Access. To enable the feature, see "HTML Access Group Policy Settings" in the chapter "Configuring HTML Access for End Users" in the *Using HTML Access* document, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Create an RDS Desktop Pool

You create an RDS desktop pool as part of the process to give users access to RDS desktops.

Prerequisites

- Set up RDS hosts. See [Chapter 8, "Setting Up Remote Desktop Services Hosts,"](#) on page 95.
- Create a farm that contains the RDS hosts. See [Chapter 9, "Creating Farms,"](#) on page 107.
- Decide how to configure the pool settings. See ["Desktop Pool Settings for RDS Desktop Pools,"](#) on page 124.

Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Click **Add**.
- 3 Select **RDS Desktop Pool**.
- 4 Provide a pool ID, display name, and description.

The pool ID is the unique name that identifies the pool in View Administrator. The display name is the name of the RDS desktop pool that users see when they log in to Horizon Client. If you do not specify a display name, it will be the same as the pool ID.

- 5 Select pool settings.
- 6 Select or create a farm for this pool.

In View Administrator, you can now view the RDS desktop 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 159.

Make sure that your end users have access to Horizon Client 3.0 or later software, which is required to support RDS desktop pools.

Desktop Pool Settings for RDS Desktop Pools

You can specify certain pool settings when you create an RDS desktop pool. Not all pool settings apply to all types of desktop pools.

For descriptions of all pool settings, see ["Desktop Pool Settings for All Desktop Pool Types,"](#) on page 135. The following pool settings apply to an RDS desktop pool.

Table 11-1. Settings for an RDS Desktop Pool

Setting	Default Value
State	Enabled
Connection Server restrictions	None
Adobe Flash quality	Do not control
Adobe Flash throttling	Disabled

Configure Adobe Flash Throttling with Internet Explorer for RDS Desktop Pools

To ensure that Adobe Flash throttling works with Internet Explorer in RDS desktops, users must enable third-party browser extensions.

Procedure

- 1 Start Horizon Client and log in to a user's desktop.
- 2 In Internet Explorer, click **Tools > Internet Options**.
- 3 Click the **Advanced** tab, select **Enable third-party browser extensions**, and click **OK**.
- 4 Restart Internet Explorer.

Provisioning Desktop Pools

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,”](#) on page 127
- [“Naming Machines Manually or Providing a Naming Pattern,”](#) on page 128
- [“Manually Customizing Machines,”](#) on page 133
- [“Desktop Pool Settings for All Desktop Pool Types,”](#) on page 135
- [“Adobe Flash Quality and Throttling,”](#) on page 139
- [“Setting Power Policies for Desktop Pools,”](#) on page 140
- [“Configuring 3D Rendering for Desktops,”](#) on page 145
- [“Prevent Access to View Desktops Through RDP,”](#) on page 156
- [“Deploying Large Desktop Pools,”](#) on page 157

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 12-1](#) compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 12-1. 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 130.	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 129.
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 132.
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 133.

Table 12-1. Naming machines Manually or Providing a machine-Naming Pattern (Continued)

Feature	Using a Machine-Naming Pattern	Naming Machines Manually
Dynamic or fixed pool size	<p>Dynamic.</p> <p>If you remove a user assignment from a machine in a dedicated-assignment pool, the machine is returned to the pool of available machines.</p> <p>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.</p> <p>NOTE Instant-clone pools can only be floating-assignment pools. The machines are always deleted on logoff.</p>	<p>Fixed.</p> <p>The pool contains the number of machines you provide in the list of machine names.</p> <p>You cannot select the Delete machine on logoff setting if you name machines manually.</p>
Spare machines	<p>You can specify a number of spare machines that View keeps powered on for new users.</p> <p>View creates new machines to maintain the specified number. View stops creating spare machines when it reaches the maximum pool size.</p> <p>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.</p> <p>NOTE Instant-clone pools do not have a power policy.</p>	<p>You can specify a number of spare machines that View keeps powered on for new users.</p> <p>View does not create new spare machines to maintain the specified number.</p> <p>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.</p>
User assignment	<p>You can use a naming pattern for dedicated-assignment and floating-assignment pools.</p> <p>NOTE Instant-clone pools can only be floating-assignment pools.</p>	<p>You can specify machine names for dedicated-assignment and floating-assignment pools.</p> <p>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.</p>

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 12-2. 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 131.

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 12-3. 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 129.

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 132.

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 130.

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 12-4. Desktop Pool Setting Descriptions

Setting	Options
State	<ul style="list-style-type: none"> ■ 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. <p>When this state is in effect, remote desktops are unavailable for use.</p>
Connection Server restrictions	<ul style="list-style-type: none"> ■ 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. <p>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.</p>
Remote machine power policy	<p>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 140.</p> <p>For more information about how power policies affect automated pools, see “Setting Power Policies for Desktop Pools,” on page 140.</p> <p>Not applicable to instant-clone desktop pools. Instant clones are always powered on.</p>
Automatically logoff after disconnect	<ul style="list-style-type: none"> ■ 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. <p>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.</p>
Allow users to reset their machines	<p>Allow users to reset their own desktops.</p> <p>Not applicable to instant-clone desktop pools.</p>
Allow user to initiate separate sessions from different client devices	<p>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.</p>
Delete machine after logoff	<p>Select whether to delete floating-assignment, full virtual machines.</p> <ul style="list-style-type: none"> ■ 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. <p>For instant-clone desktops, the machine is always deleted and recreated after logoff.</p>

Table 12-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options						
Delete or refresh machine on logoff	<p>Select whether to delete, refresh, or leave alone floating-assignment, linked-clone virtual machines.</p> <ul style="list-style-type: none"> ■ 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 <code>Deleting</code> 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. <p>For instant-clone desktops, the machine is always deleted and recreated after logoff.</p>						
Refresh OS disk after logoff	<p>Select whether and when to refresh the OS disks for dedicated-assignment, linked-clone virtual machines.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>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.</p> <p>When you refresh the OS disks in a linked-clone pool with dedicated assignment, the View Composer persistent disks are not affected.</p> <p>For instant-clone desktops, the machine is always deleted and recreated after logoff.</p>						
Default display protocol	<p>Select the display protocol that you want Connection Server to use to communicate with clients.</p> <table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top; width: 20%;">VMware Blast</td> <td>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.</td> </tr> <tr> <td style="vertical-align: top;">PCoIP</td> <td>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.</td> </tr> <tr> <td style="vertical-align: top;">Microsoft RDP</td> <td>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.</td> </tr> </table>	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.
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	<p>Allow users to override the default display protocol for their desktops by using Horizon Client.</p>						

Table 12-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
3D Renderer	<p>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.</p> <p>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).</p> <p>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 145.</p> <p>If your View deployment does not run on vSphere 5.0 or later, this setting is not available and is inactive in View Administrator.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>For more information, see “Configuring 3D Rendering for Desktops,” on page 145, “3D Renderer Options,” on page 148, and “Best Practices for Configuring 3D Rendering,” on page 150.</p> <p>Not available to instant-clone desktop pools.</p>
Max number of monitors	<p>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.</p> <p>You can select up to four monitors.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Not available to instant-clone desktop pools. In Horizon 7.0 the maximum number of monitors for instant clones is 2.</p>

Table 12-4. Desktop Pool Setting Descriptions (Continued)

Setting	Options
Max resolution of any one monitor	<p>If you select PCoIP or VMware Blast as the display protocol, you should specify the Maximum resolution of any one monitor.</p> <p>The Maximum resolution of any one monitor is set to 1920 x 1200 pixels by default, but you can configure this value.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Not available to instant-clone desktop pools. In Horizon 7.0, the maximum resolution of any monitor is 2560 x 1600.</p>
HTML Access	<p>Select Enabled to allow users to connect to remote desktops from within their Web browsers.</p> <p>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.</p> <p>To use HTML Access, you must install HTML Access in your View deployment. For more information, see <i>Using HTML Access</i>, available from https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.</p> <p>To use HTML Access with VMware Identity Manager, you must pair Connection Server with a SAML Authentication server, as described in the <i>View Administration</i> document. VMware Identity Manager must be installed and configured for use with Connection Server.</p>
Adobe Flash quality	<p>Determines the quality of Adobe Flash content that is displayed on Web pages.</p> <ul style="list-style-type: none"> ■ 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. <p>For more information, see “Adobe Flash Quality and Throttling,” on page 139.</p>
Adobe Flash throttling	<p>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.</p> <ul style="list-style-type: none"> ■ 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. <p>For more information, see “Adobe Flash Quality and Throttling,” on page 139.</p>

Table 12-4. 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 <i>server-name</i> 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 12-5](#) shows the available Adobe Flash render-quality settings.

Table 12-5. 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 12-6](#) shows the available Adobe Flash throttling settings.

Table 12-6. 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. Instant clones are always powered on.

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 View Administrator.

NOTE You cannot configure power policies for desktop pools that have unmanaged machines.

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 12-7](#) describes the available power policies.

Table 12-7. Power Policies

Power Policy	Description
Take no power action	<p>View does not enforce any power policy after a user logs off. This setting has two consequences.</p> <ul style="list-style-type: none"> View does not change the power state of the virtual machine after a user logs off. <p>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.</p> <ul style="list-style-type: none"> View does not enforce any power state after an administrative task is completed. <p>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.</p>
Ensure machines are always powered on	<p>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.</p> <p>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.</p>

Table 12-7. Power Policies (Continued)

Power Policy	Description
Suspend	<p>The virtual machine enters a suspended state when a user logs off, but not when a user disconnects.</p> <p>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 142.</p> <p>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.</p>
Power off	<p>The virtual machine shuts down when a user logs off, but not when a user disconnects.</p>

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 12-8](#) describes when View applies the configured power policy.

Table 12-8. 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)	<p>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.</p> <p>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.</p>
Automated pool with dedicated assignment	<p>To unassigned machines only.</p> <p>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.</p> <p>NOTE The Ensure machines are always powered on policy applies to assigned and unassigned machines.</p>
Automated pool with floating assignment	<p>When a machine is not in use and after a user logs off.</p> <p>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.</p>

Table 12-8. 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 142 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 12-9](#) describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 12-9. 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 12-10](#) describes the floating-assignment, automated pool in this example. The pool uses a machine-naming pattern to provision and name the machines.

Table 12-10. 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 12-11 describes the dedicated-assignment, automated pool in this example.

Table 12-11. 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 passthrough 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 must use PCoIP or VMware Blast Extreme as the default display protocol.
- Users must not be allowed to choose their own 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 View Administrator to **NVIDIA GRID vGPU**.

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 154.

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 148.

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 148.

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 148.

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 154.

Table 12-12. 3D Renderer Options for Pools Running on vSphere 5.1 or Later

Option	Description
Manage using vSphere Client	<p>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.</p> <p>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.</p> <p>Use this setting when configuring vDGA and AMD Multiuser GPU Using vDGA. This setting is also an option for vSGA.</p> <p>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.</p>
Automatic	<p>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.</p> <p>This setting is an option when configuring vSGA.</p> <p>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.</p>
Software	<p>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.</p> <p>Use this setting to configure Soft 3D.</p> <p>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.</p>
Hardware	<p>3D rendering is enabled. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on.</p> <p>This setting is an option when configuring vSGA.</p> <p>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.</p> <p>IMPORTANT If you configure the Hardware option, consider these potential constraints:</p> <ul style="list-style-type: none"> ■ 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. <p>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 156.</p>

Table 12-12. 3D Renderer Options for Pools Running on vSphere 5.1 or Later (Continued)

Option	Description
NVIDIA GRID vGPU	<p>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.</p> <p>Use this setting when configuring NVIDIA GRID vGPU.</p> <p>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.</p> <p>IMPORTANT If you configure the NVIDIA GRID vGPU option, consider these potential constraints:</p> <ul style="list-style-type: none"> ■ 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 12-13. 3D Renderer Options for Pools Running on vSphere 5.0

Option	Description
Enabled	<p>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.</p>
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 153.

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 154.

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 153.

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 155.

- 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 12-14. Flags for Configuring AMD SR-IOV

Flag	Description
<i>bus#</i>	Bus number in decimal format.
<i>device#</i>	<p>PCIe device ID for the supported AMD card, in decimal format. To see a list, use the command <code>lspci grep -i display</code>.</p> <p>For example, for a system that has two AMD GPU cards, you might see the following output when you run this command:</p> <pre>[root@host:~] lspci grep -i display 0000:04:00.0 Display controller: 0000:82:00.0 Display controller:</pre> <p>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 <code>vicfg-module</code> command.</p> <p>AMD S7150 cards support only a single GPU per card, and so the device ID and function ID are 0 for these cards.</p>
<i>function#</i>	Function number in decimal format.
<i>number_of_VFs</i>	Number of VFs (virtual functions), from 2 to 15. This number represents the number users who will share the GPU.
<i>FB_size</i>	<p>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;</p> <ul style="list-style-type: none"> ■ For 2 VFs, use 4096. ■ For 4 VFs, use 2048. ■ For 8 VFs, use 1024. ■ For 15 VFs, use 544.
<i>time_slice</i>	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.
<i>mode</i>	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" amdgpv
```

- 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" amdgpv
```

- 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" amdgpv
```

- 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, `gpvmm`, 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 `gpvmm` 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:

```
~ # gpvmm
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 View Desktops Through RDP

In certain View environments, it is a priority to prohibit access to View desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access View desktops by configuring pool settings and a group policy setting.

By default, while a user is logged in to a View desktop session, you can use RDP to connect to the virtual machine from outside of View. The RDP connection terminates the View desktop session, and the View user's unsaved data and settings might be lost. The View 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 View session-management operations.

Prerequisites

Verify that the Horizon Agent Configuration Administrative Template (ADM) file is installed in Active Directory. See [“Using View Group Policy Administrative Template Files,”](#) on page 264.

Procedure

- 1 Select PCoIP as the display protocol that you want View Connection Server to use to communicate with Horizon Client devices.

Option	Description
Create a desktop pool	<ol style="list-style-type: none"> a In View 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	<ol style="list-style-type: none"> a In View 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 View 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

You configure entitlements to control which remote desktops and applications your users can access. You can also 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.

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,”](#) on page 159
- [“Remove Entitlements from a Desktop or Application Pool,”](#) on page 160
- [“Review Desktop or Application Pool Entitlements,”](#) on page 160
- [“Restricting Remote Desktop Access,”](#) on page 160

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 View Connection Server instance that users connect to when they select desktops.

With restricted entitlements, you assign one or more tags to a View Connection Server instance. Then, when configuring a desktop pool, you select the tags of the View Connection Server instances that you want to be able to access the desktop pool.

When users log in through a tagged View Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

NOTE You cannot configure the restricted entitlements feature to restrict access to remote applications.

- [Restricted Entitlement Example](#) on page 161
This example shows a View deployment that includes two View 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 162
The restricted entitlements feature uses tag matching to determine whether a View Connection Server instance can access a particular desktop pool.
- [Considerations and Limitations for Restricted Entitlements](#) on page 163
Before implementing restricted entitlements, you must be aware of certain considerations and limitations.
- [Assign a Tag to a View Connection Server Instance](#) on page 163
When you assign a tag to a View Connection Server instance, users who connect to that View Connection Server can access only those desktop pools that have a matching tag or no tags.
- [Assign a Tag to a Desktop Pool](#) on page 163
When you assign a tag to a desktop pool, only users who connect to a View Connection Server instance that has a matching tag can access the desktops in that pool.

Restricted Entitlement Example

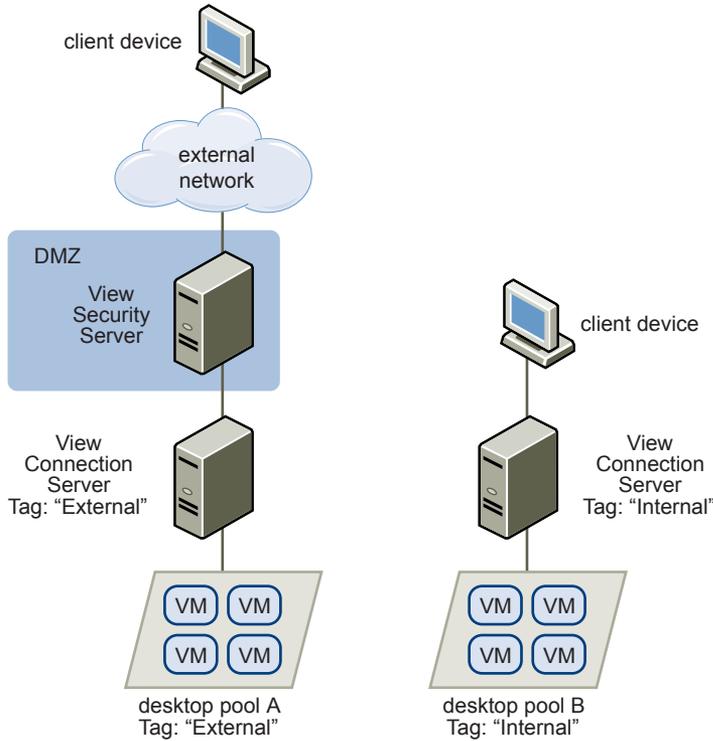
This example shows a View deployment that includes two View Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

- Assign the tag "Internal" to the View Connection Server instance that supports your internal users.
- Assign the tag "External" to the View 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 View Connection Server tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the View Connection Server tagged as Internal. [Figure 13-1](#) illustrates this configuration.

Figure 13-1. Restricted Entitlement Configuration



You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular View 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 View Connection Server instance can access a particular desktop pool.

At the most basic level, tag matching determines that a View Connection Server instance with a specific tag can access a desktop pool that has the same tag.

The absence of tag assignments can also affect whether a View Connection Server instance can access a desktop pool. For example, View Connection Server instances that do not have any tags can only access desktop pools that also do not have any tags.

Table 13-1 shows how the restricted entitlement feature determines when a View Connection Server can access a desktop pool.

Table 13-1. 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 View Connection Server instance.

Considerations and Limitations for Restricted Entitlements

Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- A single View Connection Server instance or desktop pool can have multiple tags.
- Multiple View Connection Server instances and desktop pools can have the same tag.
- Desktop pools that do not have any tags can be accessed by any View Connection Server instance.
- View Connection Server instances that do not have any tags can only access desktop pools that also do not have any tags.
- If you use a security server, you must configure restricted entitlements on the View Connection Server instance the security server is paired with. You cannot configure restricted entitlements on a security server.
- You cannot modify or remove a tag from a View Connection Server instance if that tag is still assigned to a desktop pool and no other View 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 will not be able to access that machine if the desktop pool's tag does not match the tag assigned to the View Connection Server instance that the user connected to.
- If you intend to provide access to your desktops through VMware Identity Manager and you configure View 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 launch if the desktop pool's tag does not match the tag assigned to the View Connection Server instance to which the user is connected.

Assign a Tag to a View Connection Server Instance

When you assign a tag to a View Connection Server instance, users who connect to that View Connection Server can access only those desktop pools that have a matching tag or no tags.

Procedure

- 1 In View Administrator, select **View Configuration > Servers**.
- 2 Click the **Connection Servers** tab, select the View 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.

Assign a Tag to a Desktop Pool

When you assign a tag to a desktop pool, only users who connect to a View 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 View Connection Server instances.

Procedure

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

2 Select the pool that you want to assign a tag to.

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 View Connection Server instances that can access the desktop pool.

Option	Action
Make the pool accessible to any View Connection Server instance	Select No Restrictions .
Make the pool accessible only to View 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.

Configuring Remote Desktop Features

14

Certain remote desktop features that are installed with Horizon Agent can be updated in Feature Pack Update releases as well as in core View releases. You can configure these features to enhance the remote desktop experience of your end users.

These features include HTML Access, Unity Touch, Flash URL Redirection, Real-Time Audio-Video, Windows Media Multimedia Redirection (MMR), USB Redirection, Scanner Redirection, and Serial Port Redirection.

For information about HTML Access, see the *Using HTML Access* document, located on the VMware Horizon Client Documentation Web page.

For information about USB Redirection, see [Chapter 15, “Using USB Devices with Remote Desktops and Applications,”](#) on page 213.

This chapter includes the following topics:

- [“Configuring Unity Touch,”](#) on page 165
- [“Configuring Flash URL Redirection for Multicast or Unicast Streaming,”](#) on page 168
- [“Configuring Flash Redirection,”](#) on page 172
- [“Configuring URL Content Redirection,”](#) on page 177
- [“Configuring Real-Time Audio-Video,”](#) on page 183
- [“Configuring Scanner Redirection,”](#) on page 197
- [“Configuring Serial Port Redirection,”](#) on page 202
- [“Managing Access to Windows Media Multimedia Redirection \(MMR\),”](#) on page 209
- [“Managing Access to Client Drive Redirection,”](#) on page 211

Configuring Unity Touch

With Unity Touch, tablet and smart phone users can easily 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. You can configure a default list of favorite applications that appear in the Unity Touch sidebar.

You can disable or enable the Unity Touch feature after it is installed by configuring the **Enable Unity Touch** group policy setting. See [“Horizon Agent Configuration ADM Template Settings,”](#) on page 266.

The VMware Horizon Client documents for iOS and Android devices provide more information about end user features provided by Unity Touch.

System Requirements for Unity Touch

Horizon Client software and the mobile devices on which you install Horizon Client must meet certain version requirements to support Unity Touch.

View desktop	To support Unity Touch, the following software must be installed in the virtual machine that the end user will access: <ul style="list-style-type: none"> ■ You install the Unity Touch feature by installing View Agent 6.0 or later. See “Install Horizon Agent on a Virtual Machine,” on page 26. ■ Operating systems: Windows 7 (32-bit or 64-bit), Windows 8 (32-bit or 64-bit), Windows 8.1 (32-bit or 64-bit), Windows Server 2008 R2, or Windows Server 2012 R2, Windows 10 (32-bit or 64-bit)
Horizon Client software	Unity Touch is supported on the following Horizon Client versions: <ul style="list-style-type: none"> ■ Horizon Client 2.0 for iOS or later ■ Horizon Client 2.0 for Android or later
Mobile device operating systems	Unity Touch is supported on the following mobile device operating systems: <ul style="list-style-type: none"> ■ iOS 5.0 and later ■ Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich), and Android 4.1 and 4.2 (Jelly Bean)

Configure Favorite Applications Displayed by Unity Touch

With the Unity Touch feature, tablet and smart phone users can quickly navigate to a View desktop application or file from a Unity Touch sidebar. Although end users can specify which favorite applications appear in the sidebar, for added convenience, administrators can configure a default list of favorite applications.

If you use floating-assignment desktop pools, the favorite applications and favorite files that end users specify will be lost when they disconnect from a desktop unless you enable roaming user profiles in Active Directory.

The default list of favorite applications list remains in effect when an end user first connects to a desktop that is enabled with Unity Touch. However, if the user configures his or her own favorite application list, the default list is ignored. The user's favorite application list stays in the user's roaming profile and is available when the user connects to different machines in a floating or dedicated pool.

If you create a default list of favorite applications and one or more of the applications are not installed in the View desktop operating system, or the paths to these applications are not found in the Start menu, the applications do not appear in the list of favorites. You can use this behavior to set up one master default list of favorite applications that can be applied to multiple virtual machine images with different sets of installed applications.

For example, if Microsoft Office and Microsoft Visio are installed on one virtual machine, and Windows Powershell and VMware vSphere Client are installed on a second virtual machine, you can create one list that includes all four applications. Only the installed applications appear as default favorite applications on each respective desktop.

You can use different methods to specify a default list of favorite applications:

- Add a value to the Windows registry on the virtual machines in the desktop pool
- Create an administrative installation package from the Horizon Agent installer and distribute the package to the virtual machines

- Run the Horizon Agent installer from the command line on the virtual machines

NOTE Unity Touch assumes that shortcuts to applications are located in the Programs folder in the **Start** menu. If any shortcut is located outside of the Programs folder, attach the prefix **Programs** to the shortcut path. For example, Windows Update.lnk is located in the ProgramData\Microsoft\Windows\Start Menu folder. To publish this shortcut as a default favorite application, add the prefix **Programs** to the shortcut path. For example: "Programs/Windows Update.lnk".

Prerequisites

- Verify that Horizon Agent is installed on the virtual machine.
- Verify that you have administrative rights on the virtual machine. For this procedure, you might need to edit a registry setting.
- If you have floating-assignment desktop pools, use Active Directory to set up roaming user profiles. Follow the instructions provided by Microsoft.

Users of floating-assignment desktop pools will be able to see their list of favorite applications and favorite files every time they log in.

Procedure

- (Optional) Create a default list of favorite applications by adding a value to the Windows registry.
 - Open regedit and navigate to the HKLM\Software\VMware, Inc.\VMware Unity registry setting. On a 64-bit virtual machine, navigate to the HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity directory.
 - Create a string value called FavAppList.
 - Specify the default favorite applications.

Use the following format to specify the shortcut paths to the applications that are used in the Start menu.

path-to-app-1|path-to-app-2|path-to-app-3|...

For example:

Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk

- (Optional) Create a default list of favorite applications by creating an administrative installation package from the Horizon Agent installer.
 - a From the command line, use the following format to create the administrative installation package.

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network share to
store the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps
that should be set in the registry""
```

For example:

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-
share\ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of
Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|
Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet
Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|
Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace
2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity
Tools/WebEx Settings.lnk|""
```

- b Distribute the administrative installation package from the network share to the desktop virtual machines by using a standard Microsoft Windows Installer (MSI) deployment method that is employed in your organization.
- (Optional) Create a default list of favorite applications by running the Horizon Agent installer on a command line directly on a virtual machine.

Use the following format.

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of default
favorite apps that should be set in the registry""
```

NOTE The preceding command combines installing Horizon Agent with specifying the default list of favorite applications. You do not have to install Horizon Agent before you run this command.

What to do next

If you performed this task directly on a virtual machine (by editing the Windows registry or installing Horizon Agent from the command line), you must deploy the newly configured virtual machine. You can create a snapshot or make a template and create a desktop pool, or recompose an existing pool. Or you can create an Active Directory group policy to deploy the new configuration.

Configuring Flash URL Redirection for Multicast or Unicast Streaming

Customers can now use Adobe Media Server and multicast or unicast to deliver live video events in a virtual desktop infrastructure (VDI) environment. To deliver multicast or unicast live video streams within a VDI environment, the media stream should be sent directly from the media source to the endpoints, bypassing the remote desktops. The Flash URL Redirection feature supports this capability by intercepting and redirecting the ShockWave Flash (SWF) file from the remote desktop to the client endpoint.

The Flash content is then displayed using the clients' local Flash media players.

Streaming Flash content directly from the Adobe Media Server to the client endpoints lowers the load on the datacenter ESXi host, removes the extra routing through the datacenter, and reduces the bandwidth required to simultaneously stream Flash content to multiple client endpoints.

The Flash URL redirection feature uses a JavaScript that is embedded inside an HTML Web page by the Web page administrator. Whenever a remote desktop user clicks on the designated URL link from within a Web page, the JavaScript intercepts and redirects the SWF file from the remote desktop session to the client endpoint. The endpoint then opens a local Flash Projector outside of the remote desktop session and plays the media stream locally.

To configure Flash URL Redirection, you must set up your HTML Web page and your client devices.

Procedure

- 1 [System Requirements for Flash URL Redirection](#) on page 169
To support Flash URL Redirection, your View deployment must meet certain software and hardware requirements.
- 2 [Verify that the Flash URL Redirection Feature Is Installed](#) on page 170
Before you use this feature, verify that the Flash URL Redirection feature is installed and running on your virtual desktops.
- 3 [Set Up the Web Pages That Provide Multicast or Unicast Streams](#) on page 171
To allow Flash URL redirection to take place, you must embed a JavaScript command in the MIME HTML (MHTML) Web pages that provide links to the multicast or unicast streams. Users display these Web pages in the browsers on their remote desktops to access the video streams.
- 4 [Set Up Client Devices for Flash URL Redirection](#) on page 171
The Flash URL Redirection feature redirects the SWF file from remote desktops to client devices. To allow these client devices to play Flash videos from a multicast or unicast stream, you must verify that the appropriate Adobe Flash Player is installed on the client devices. The clients also must have IP connectivity to the media source.
- 5 [Disable or Enable Flash URL Redirection](#) on page 172
Flash URL Redirection is enabled when you perform a silent installation of Horizon Agent with the `VDM_FLASH_URL_REDIRECTION=1` property. You can disable or reenabling the Flash URL Redirection feature on selected remote desktops by setting a value on a Windows registry key on those virtual machines.

System Requirements for Flash URL Redirection

To support Flash URL Redirection, your View deployment must meet certain software and hardware requirements.

View desktop

- You install Flash URL Redirection by typing the `VDM_FLASH_URL_REDIRECTION` property on the command line during a silent installation of View Agent 6.0 or later. See [“Silent Installation Properties for Horizon Agent,”](#) on page 33.
- The desktops must run Windows 7 64-bit or 32-bit operating systems.
- Supported desktop browsers include Internet Explorer 8, 9, and 10, Chrome 29.x, and Firefox 20.x.

Flash media player and ShockWave Flash (SWF)

You must integrate an appropriate Flash media player such as Strobe Media Playback into your Web site. To stream multicast content, you can use `multicastplayer.swf` or `StrobeMediaPlayback.swf` in your Web pages. To stream live unicast content, you must use `StrobeMediaPlayback.swf`. You can also use `StrobeMediaPlayback.swf` for other supported features such as RTMP streaming and HTTP dynamic streaming.

Horizon Client software

The following Horizon Client releases support multicast and unicast:

- Horizon Client 2.2 for Linux or a later release
- Horizon Client 2.2 for Windows or a later release

The following Horizon Client releases support multicast only (they do not support unicast):

- Horizon Client 2.0 or 2.1 for Linux
- Horizon Client 5.4 for Windows

Horizon Client computer or client access device

- Flash URL Redirection is supported on all operating systems that run Horizon Client for Linux on x86 Thin client devices. This feature is not supported on ARM processors.
- Flash URL Redirection is supported on all operating systems that run Horizon Client for Windows. For details, see the *Using VMware Horizon Client for Windows* document.
- On Windows client devices, you must install Adobe Flash Player 10.1 or later for Internet Explorer.
- On Linux Thin client devices, you must install the `libexpat.so.0` and `libflashplayer.so` files. See [“Set Up Client Devices for Flash URL Redirection,”](#) on page 171.

NOTE With Flash URL Redirection, the multicast or unicast stream is redirected to client devices that might be outside your organization's firewall. Your clients must have access to the Adobe Web server that hosts the ShockWave Flash (SWF) file that initiates the multicast or unicast streaming. If needed, configure your firewall to open the appropriate ports to allow client devices to access this server.

Verify that the Flash URL Redirection Feature Is Installed

Before you use this feature, verify that the Flash URL Redirection feature is installed and running on your virtual desktops.

The Flash URL Redirection feature must be present on every desktop where you intend to support multicast or unicast redirection. For Horizon Agent installation instructions, see [“Silent Installation Properties for Horizon Agent,”](#) on page 33.

Procedure

- 1 Start a remote desktop session that uses PCoIP.
- 2 Open the Task Manager.
- 3 Verify that the `ViewMPServer.exe` process is running on the desktop.

Set Up the Web Pages That Provide Multicast or Unicast Streams

To allow Flash URL redirection to take place, you must embed a JavaScript command in the MIME HTML (MHTML) Web pages that provide links to the multicast or unicast streams. Users display these Web pages in the browsers on their remote desktops to access the video streams.

In addition, you can customize the English error message that is displayed to end users when a problem occurs with Flash URL redirection. Take this optional step if you want to display a localized error message to your end users. You must embed the `var vmwareScriptErrorMessage` configuration, together with your localized text string, in the MHTML Web page.

Prerequisites

Verify that the `swfobject.js` library is imported in the MHTML Web page.

Procedure

- 1 Embed the `viewmp.js` JavaScript command in the MHTML Web page.
For example: `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`
- 2 (Optional) Customize the Flash URL redirection error message that is sent to end users.
For example: `"var vmwareScriptErrorMessage=localized error message"`
- 3 Make sure to embed the `viewmp.js` JavaScript command, and optionally customize the Flash URL redirection error message, before the ShockWave Flash (SWF) file is imported into the MHTML Web page.

When a user displays the Web page in a remote desktop, the `viewmp.js` JavaScript command invokes the Flash URL Redirection mechanism on the remote desktop, which redirects the SWF file from the desktop to the hosting client device.

Set Up Client Devices for Flash URL Redirection

The Flash URL Redirection feature redirects the SWF file from remote desktops to client devices. To allow these client devices to play Flash videos from a multicast or unicast stream, you must verify that the appropriate Adobe Flash Player is installed on the client devices. The clients also must have IP connectivity to the media source.

NOTE With Flash URL Redirection, the multicast or unicast stream is redirected to client devices that might be outside your organization's firewall. Your clients must have access to the Adobe Web server that hosts the SWF file that initiates the multicast or unicast streaming. If needed, configure your firewall to open the appropriate ports to allow client devices to access this server.

Procedure

- ◆ Install Adobe Flash Player on your client devices.

Operating System	Action
Windows	Install Adobe Flash Player 10.1 or later for Internet Explorer.
Linux	<p>a Install the <code>libexpat.so.0</code> file, or verify that this file is already installed.</p> <p>Ensure that the file is installed in the <code>/usr/lib</code> or <code>/usr/local/lib</code> directory.</p> <p>b Install the <code>libflashplayer.so</code> file, or verify that this file is already installed.</p> <p>Ensure that the file is installed in the appropriate Flash plug-in directory for your Linux operating system.</p> <p>c Install the <code>wget</code> program, or verify that the program file is already installed.</p>

Disable or Enable Flash URL Redirection

Flash URL Redirection is enabled when you perform a silent installation of Horizon Agent with the `VDM_FLASH_URL_REDIRECTION=1` property. You can disable or reenble the Flash URL Redirection feature on selected remote desktops by setting a value on a Windows registry key on those virtual machines.

Procedure

- 1 Start the Windows Registry Editor on the virtual machine.
- 2 Navigate to the Windows registry key that controls Flash URL Redirection.

Option	Description
Windows 7 64-bit	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>
Windows 7 32-bit	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>

- 3 Set the value to disable or enable Flash URL Redirection.

Option	Value
Disabled	0
Enabled	1

By default, the value is set to 1.

Configuring Flash Redirection

With the Flash Redirection feature, Flash content is sent to the client system and played in a Flash container window using the Flash Player ActiveX version.

NOTE In this release, the Flash Redirection feature is available as a Tech Preview only.

Although the name of this feature is similar to the feature called Flash URL Redirection, there are important differences, as described in the following table.

Table 14-1. Comparison of the Flash Redirection Feature and Flash URL Redirection

Item of Differentiation	Flash Redirection	Flash URL Redirection
Support level	As a Tech Preview feature, no technical support is offered	Fully supported
Horizon Client types that support this feature	Windows client only	Windows client and Linux client
Display protocol required	PCoIP	PCoIP
Browsers	Internet Explorer 9, 10, or 11 for the agent (remote desktop)	All browsers that are currently supported on Horizon Client and Horizon Agent
Configuration mechanism	Use an agent-side GPO to specify a white list of Web sites that will use Flash Redirection	Modify the source code on the Web page to embed the required JavaScript

Feature Limitations

The Flash Redirection feature has the following limitations:

- Clicking a URL link inside the Flash Player window opens a browser on the client rather than in the remote desktop (agent side).
- The following Flash functionality does not work with Flash Redirection: Autoplay, the Next and Previous buttons, and Theater mode.
- Some Web sites do not work with Flash Redirection on some browser versions. For example, the vimeo.com Web site does not work if you use Internet Explorer 11.
- Flash and Java scripting might not work as expected.
- The Flash Player window might not resize correctly if you resize the browser window or the Horizon Client window.
- The Horizon Client window might freeze while playing Flash content, although you can set a Windows Registry key to work around this issue.

On a 32-bit client, set HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer value to "FALSE" and on a 64-bit client, set HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer to "FALSE".

Requirements for Flash Redirection (Tech Preview)

With Flash Redirection, If you use an Internet Explorer 9, 10, or 11 browser, Flash content is sent to the client system. The client system plays the media content, thereby offloading the demand on the ESXi host.

Flash Redirection is available as a Tech Preview feature with Horizon 7 and Horizon Client 4.0.

Remote desktop

- Horizon Agent 7.0 or later must be installed in a single-user (VDI) remote desktop, with the Flash Redirection option (this option is not selected by default).
See "[Horizon Agent Custom Setup Options](#)," on page 28.
- The appropriate group policy settings must be configured. See "[Install and Configure Flash Redirection](#)," on page 174.
- Flash Redirection is supported on Windows 7, Windows 8, and Windows 8.1 operating systems installed on single-user remote desktops.

- Internet Explorer 9, 10, or 11 must be installed with the corresponding Flash ActiveX plug-in.
 - After installation, in Internet Explorer, the VMware View FlashMMR Server add-on must be enabled.
- Horizon Client computer or client access device**
- Horizon Client 4.0 or later must be installed. (The Flash Redirection option is enabled by default.)
- See the topic about installing Horizon Client, in *Using VMware Horizon Client for Windows* document.
- Flash Redirection is supported on Windows 7, Windows 8, and Windows 8.1 client operating systems.
 - The Flash ActiveX plug-in must be installed and enabled
- Display protocol for the remote session** PCoIP

Install and Configure Flash Redirection

Redirecting Flash content from a remote desktop to a Flash Player window on the local client system requires installing the Flash Redirection feature and Internet Explorer on the remote desktop and the client system and specifying which Web sites will use this feature.

To install this feature on the client system, you must use a Horizon Client 4.0 or later installer. To install this feature on a remote desktop, you must use a Horizon Agent 7.0 or later installer and select the correct installation option, which is not selected by default. To enable this feature and to specify which Web sites will use this feature, you use a group policy.

NOTE You can alternatively use Windows Registry settings on the remote desktop to configure a white list of Web sites to use for Flash Redirection. See [“Use Windows Registry Settings to Configure Flash Redirection,”](#) on page 176.

Prerequisites

- Verify that you can log in as an Administrator domain user on the machine that hosts your Active Directory server.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Verify that the Horizon Agent Configuration ADM Template (`vdm_agent.adm` file) has been added to the OU for the remote desktop. See [“Add View ADM Templates to a GPO,”](#) on page 298.
- Compile a list of the Web sites that will use this feature to redirect Flash content. This list is a white list, meaning that only the URLs specified in this list will be able to use this feature.

Procedure

- 1 On a Windows 7, Windows 8, or Windows 8.1 client system, install the required version of Horizon Client and Flash Player ActiveX version.
 - Install Horizon Client 4.0 or later. See the topic about installing Horizon Client, in *Using VMware Horizon Client for Windows* document.
 - If necessary, install the ActiveX version of Flash Player (rather than the NPAPI version). Flash Player is installed by default in Internet Explorer 10 and 11. For Internet Explorer 9, you might need to go to the following site to download and install Flash Player:
<https://get.adobe.com/flashplayer/>.

- 2 On a Windows 7, Windows 8, or Windows 8.1 remote desktop, install the required version of Horizon Agent and Internet Explorer, with Flash Player.
 - Install Horizon Agent 7.0 or later and be sure to select the option for Flash Redirection (experimental). This option is not selected by default.
 - Install Internet Explorer 9, 10, or 11.
 - If necessary, install the ActiveX version of Flash Player (rather than the NPAPI version). Flash Player is installed by default in Internet Explorer 10 and 11. For Internet Explorer 9, you might need to go to the following site to download and install Flash Player:
<https://get.adobe.com/flashplayer/>.

- 3 On the remote desktop, in Internet Explorer, select **Tools > Manage add-ons** from the menu bar and verify that **VMware View FlashMMR Server** is listed and enabled.
- 4 On the Active Directory server, open the Group Policy Management Editor and edit the Flash Redirection policy settings under **Computer Configuration**.

The settings are located in the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon Agent Configuration > VMware FlashMMR** folder.

Setting	Description
Enable Flash Multimedia Redirection	Specifies whether Flash Redirection (FlashMMR) is enabled on the remote desktop (agent-side). When enabled, this feature forwards Flash multimedia data from the designated URLs through a TCP channel to the client, and invokes the local Flash Player on the client system. This feature greatly reduces demand on the agent-side CPU and network bandwidth.
Minimum Rectangle Size	Specifies the minimum width and height, in pixels, of the rectangle in which the Flash content is played. For example, 400, 300 specifies a width of 400 pixels and a height of 300 pixels. Flash Redirection will be used only if the Flash content is equal to or greater than the values specified in this policy. If this GPO is not configured, the default value used is 320, 200 .

- 5 In the Group Policy Management Editor, edit the Flash Redirection policy settings under **User Configuration**.

The settings are located in the **User Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon Agent Configuration > VMware FlashMMR** folder.

- a Open the setting for making a list of host URLs that you want to use with Flash redirection and select the **Enabled** radio button.
- b Click the **Show** button.
- c Enter the complete URLs in the Name column, and leave the Value column blank.
Be sure to include **http://** or **https://**. You can use regular expressions. For example, you can specify **https://*.google.com** and **http://www.cnn.com**.

- 6 On the agent machine, open a command prompt as an Administrator and change directories to the following directory:

```
%Program Files%\Common Files\VMware\Remote Experience
```

The `mergeflashmmrwhitelist.vbs` file is located in this directory.

- 7 Run the following command to ensure that the white list you configured is added to Internet Explorer's trusted sites and compatibility view.

```
cscript mergeflashmmrwhitelist.vbs
```

- 8 Restart Internet Explorer.

The site or sites are added. You can verify the trusted sites by selecting **Tools > Internet Options** from the Internet Explorer menu bar, and on the **Security** tab, click the **Sites** button. You can verify compatibility settings by selecting **Tools > Compatibility View Settings** from the menu bar.

Use Windows Registry Settings to Configure Flash Redirection

If you are a domain user who does not have Administrator privileges on the Active Directory server, you can alternatively configure Flash Redirection by setting the appropriate values in Windows Registry keys on the remote desktop.

You can use this procedure as an alternative to using GPO settings to configure Flash Redirection.

Prerequisites

- Compile a list of the Web sites that will use this feature to redirect Flash content. This list is a white list, meaning that only the URLs specified in this list will be able to use this feature.
- Verify that Horizon Agent 7.0 or later is installed in the remote desktop, along with Flash Player and Internet Explorer 9, 10, or 11. See [“Install and Configure Flash Redirection,”](#) on page 174.
- Verify that you are using Horizon Client 4.0 or later, along with Flash Player ActiveX version.

Procedure

- 1 Use Horizon Client to access the remote desktop (agent machine).
- 2 Open the Windows Registry Editor (`regedit.exe`) on the agent machine, navigate to the following folder, and set **FlashRedirection** to **1**:

```
HKLM\Software\VMware, Inc.\VMware FlashMMR
```

NOTE This setting enables the Flash Redirection feature, but if this setting is disabled (set to 0) in `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR`, it means Flash Redirection is disabled domain-wide, and requires a domain administrator to enable it.

- 3 Navigate to the following folder:


```
HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
```

If this folder does not already exist, create it.
- 4 In the `VMware FlashMMR` folder, create a sub-key named **UrlWhiteList**.
- 5 Right-click the **UrlWhiteList** key, select **New > String Value**, and for the name, enter the URL of a Web site that will use the Flash Redirection feature.

You can use regular expressions. For example, you could specify `https://*.google.com`. Be sure to leave the **Data** value empty.

- 6 Repeat the previous step to add additional URLs, and when you are finished, close the Registry Editor.
- 7 On the agent machine, open a command prompt as an Administrator and change directories to the following directory:

```
%Program Files%\Common Files\VMware\Remote Experience
```

The `mergeflashmmrwhitelist.vbs` file is located in this directory.

- 8 Run the following command to ensure that the white list you configured is added to Internet Explorer's trusted sites and compatibility view.

```
cscript mergeflashmmrwhitelist.vbs
```

- 9 Restart Internet Explorer.

The site or sites are added. You can verify the trusted sites by selecting **Tools > Internet Options** from the Internet Explorer menu bar, and on the **Security** tab, click the **Sites** button. You can verify compatibility settings by selecting **Tools > Compatibility View Settings** from the menu bar.

Configuring URL Content Redirection

With URL Content Redirection, you can configure specific URLs to always open on the client or in a remote desktop or application.

You can redirect two types of URLs:

- URLs that users type in Internet Explorer's address bar.
- Links in an application such as Outlook or Word that users can click.

You can configure any number of protocols, such as HTTP, mailto, and callto, for redirection. This feature supports redirection in both directions:

- From a client to a remote desktop or application (client to agent)

Based on the rules that you set up, Horizon Client launches either a remote desktop or a remote application to handle the URL. If a desktop is launched, the default application for the URL's protocol processes the URL.
- From a remote desktop or application to a client (agent to client)

Horizon Agent sends the URL to Horizon Client, which launches the default application for the protocol that is specified in the URL.

You can redirect some URLs from the remote desktop or application to the client and other URLs from the client to the remote desktop or application.

NOTE You can have an environment where Horizon Client is installed on a remote desktop, which means that both Horizon Agent and Horizon Client are installed on the same machine. For example, a user logs in to a thin client device and is connected to a remote desktop. From the desktop, the user runs Horizon Client to access remote applications. On this desktop machine, you can install Horizon Agent with the URL Content Redirection feature or install Horizon Client with the feature, but not both. Therefore, on this machine, you can set up either client-to-agent redirection or agent-to-client redirection, but not both.

To set up this feature, you must perform the following tasks:

- For client-to-agent redirection, install Horizon Client with the URL Content Redirection feature. See [“Installing the URL Content Redirection Feature,”](#) on page 179.
- For agent-to-client redirection, install Horizon Agent with the URL Content Redirection feature. See [“Installing the URL Content Redirection Feature,”](#) on page 179.
- Configure GPO settings to indicate, for each protocol, how Horizon Agent or Horizon Client should redirect the URL. See [“VMware Horizon URL Content Redirection Template Settings,”](#) on page 180.

Feature Requirements

This feature has the following requirements:

- Horizon Client 4.0 or later.
- The supported browsers in which you can type or click a URL and have that URL redirected are Internet Explorer 9,10, and 11.
- The display protocol for the remote session must be VMware Blast or PCoIP.

Feature Limitations

The behavior of this feature might have the following unexpected results:

- If the URL opens a country-specific page based on the locale, the locale page that is opened is determined by the source of the link. For example, if the remote desktop (agent source) resides in a data center in Japan and the user's computer resides in the U.S., if the URL is redirected from the agent to the client machine, the page that opens on the U.S. client is the Japanese page.
- If users create favorites from Web pages, the favorites get created after redirection. For example, say a user clicks a link on the client machine and the URL is redirected to a remote desktop (agent). If the user creates a favorite for that page, the favorite gets created on the agent. The next time the user opens the browser on the client machine, the user might expect to find the favorite on the client machine, but the favorite was stored on the agent (remote desktop).
- Files that users download are downloaded to the machine whose browser was used to open the URL. For example, say a user clicks a link on the client machine, and the URL is redirected to a remote desktop. If the link was for downloading a file, or if the link is for a Web page where the user downloads a file, the file is downloaded to the remote desktop rather than the client machine.

The URL Content Redirection feature does not work in the following circumstances:

- Shortened URLs such as `https://goo.gl/abc` can be redirected based on filtering rules, but the filtering mechanism does not look at the original un-shortened URL. For example, if you have a rule that redirects URLs containing `acme.com`, an original URL such as `http://www.acme.com/some-really-long-path`, and a shortened URL of the original URL such as `https://goo.gl/xyz`, the original URL is redirected but not the shortened URL.

Workaround: Create rules to block or redirect URLs from the Web sites most often used for shortening URLs.

- Embedded HTML pages will bypass URL redirection. For example, say a user goes to a URL that does not match a URL redirection rule. If page contains an embedded HTML page (an `iFrame` or inline frame) whose URL does match a redirection rule, the URL redirection rule does not work. The rule works only on the top-level URL.
- URL Content Redirection does not work in situations where Internet Explorer plug-ins are disabled, for example, when the user switches to InPrivate Browsing in Internet Explorer. (People use private browsing so that Web pages and files downloaded from Web pages will not be logged in to the browsing and download history on their computer.) This limitation arises because the URL Redirection feature requires a certain Internet Explorer plug-in to be enabled, and private browsing disables these plug-ins.

Workaround: Use the GPO setting to prevent users from disabling plug-ins. These settings include the following: "Do not allow users to enable or disable add-ons" and "Automatically enable newly installed add-ons." In the Group Policy Management Editor, these settings can be found under **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer**.

Workaround specifically for Internet Explorer: Use the GPO setting to disable InPrivate mode. This setting is called "Turn off InPrivate Browsing." In the Group Policy Management Editor, these settings can be found under **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Privacy**.

These two workarounds are recommended best practices and can prevent issues with redirection that situations other than private browsing can cause.

- URL Redirection does not work if a Windows 10 Universal app is the default handler for a protocol specified in a link. Universal applications, which are built on the Universal Windows Platform so that they can be downloaded to PCs, tablets, and phones, include the Microsoft Edge browser, Mail, Maps, Photos, Groove Music and others. Therefore, if you click a link for which one of these applications is the default handler, the URL will not be redirected. For example, if a user clicks an email link in an application and the default email application is the Mail universal app, the URL specified in the link will not be redirected.

Workaround: Make a different application the default handler of the protocol of URLs that you want to redirect. For example, if Edge is the default browser, make Internet Explorer the default browser.

- Machines that have secure boot enabled will leave the URL Content Redirection feature disabled. URLs cannot be redirected from these machines. URLs can, however, be redirected to these machines.

Installing the URL Content Redirection Feature

Neither the Horizon Agent, nor the Horizon Client, installation wizard lists URL Content Redirection as a feature that you can select. You must install this feature by running the installer with a command-line option.

To support URL Content Redirection from a remote desktop or application to a client, you must install Horizon Agent with the URL Content Redirection feature. To support URL Content Redirection from a client to a remote desktop, you must install Horizon Client with the URL Content Redirection feature.

Installing Horizon Agent with the URL Content Redirection Feature

Start the installation by running the following command in a command prompt window instead of double-clicking the installer file. For example:

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

After you follow the prompts and complete the installation, you can verify that this feature is installed by checking that the `vmware-url-protocol-launch-helper.exe` file and the `vmware-url-filtering-plugin.dll` file are installed in the directory `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection\`. Also verify that the following Internet Explorer add-on is enabled: VMware Horizon View URL Filtering Plugin.

Installing Horizon Client with the URL Content Redirection Feature

Start the installation by running the following command in a command prompt window instead of double-clicking the installer file. For example:

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

After you follow the prompts and complete the installation, you can verify that this feature is installed by checking that the `vmware-url-protocol-launch-helper.exe` file and the `vmware-url-filtering-plugin.dll` file are installed in the directory `%PROGRAMFILES%\VMware\VMware Horizon View Client\`. Also verify that the following Internet Explorer add-on is installed: VMware Horizon View URL Filtering Plugin.

Add the URL Content Redirection ADM Template in Active Directory

You can add the policy settings in the URL Content Redirection ADM file, `urlRedirection-enUS.adm`, to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- If you plan to set policies for links clicked in remote desktops or applications, verify that the URL Content Redirection feature is included when you install Horizon Agent. See [“Configuring URL Content Redirection,”](#) on page 177.

- If you plan to set policies for links clicked in client browsers or applications, verify that the URL Content Redirection feature is included when you install Horizon Client. See “[Configuring URL Content Redirection](#),” on page 177.
- Verify that Active Directory GPOs are created for the URL Content Redirection group policy settings. For rules regarding links clicked from a remote desktop or application, the GPOs must be linked to the OU that contains your desktops and RDS hosts. For links clicked from inside the client system, GPOs must be linked to the OU that contains the client computers.
See “[Active Directory Group Policy Example](#),” on page 297.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with the URL Content Redirection group policy settings. See “[VMware Horizon URL Content Redirection Template Settings](#),” on page 180.

Procedure

- 1 Download the View 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 View are available in this file.
- 2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the URL Content Redirection ADM file, `urlRedirection-enUS.adm`, to your Active Directory server.
- 3 On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
- 4 In the Group Policy Object Editor, right-click the **Computer Configuration > Policies > Administrative Templates** folder and select **Add/Remove Templates**.
- 5 Click **Add**, browse to the `urlRedirection-enUS.adm` file, and click **Open**.
- 6 Click **Close** to add the policy settings in the ADM file to the GPO.
The settings are located in the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon URL Redirection** folder.
- 7 Configure the URL Content Redirection group policy settings.

The group policies are configured for the group of client computers or remote desktops for RDS hosts included in the OU.

VMware Horizon URL Content Redirection Template Settings

The Horizon URL Content Redirection ADM template file (`urlRedirection-enUS.adm`) contains policy settings related to controlling whether a URL link is opened on the client or on the agent side, in a remote desktop or application. For example, for added security, administrators can set a policy so that, for all employees working inside the company network, all URL links that point outside the company network are opened in a remote desktop or application.

This ADM file is 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.

URL Content Redirection can occur when end users click a URL link in a browser or an application, such as a Microsoft Word document or an email, or if a user clicks or types a URL into an Internet Explorer 9, 10, or 11 browser. URL links can be links to Web pages, telephone numbers, email addresses, and more.

Syntax for URL Content Redirection Rules

When specifying which URLs to open on the client or agent, you can use regular expressions. Separate multiple entries with semicolons. Spaces are not allowed between entries.

Following are some examples.

Entry	Description
.*	(Dot-star) Specifies that all URLs should be redirected. If you use this setting for the agentRules option, all URLs are redirected to the agent side, which means URLs are opened in a remote desktop or application. If you use this setting for the clientRules option, the specified URLs are redirected to the client.
.*.acme.com;.*.example.com	Specifies that all URLs that have the text .acme.com or example.com in them should be redirected.
[space or leave empty]	To specify that no URLs should be directed, use a space or leave the setting empty. For example, leaving clientRules empty specifies that no URLs should be redirected to the client.

For **agentRules** you must also use the **brokerHostname** option to specify the IP address or fully qualified domain name of the connection server, and you must use the **remotelItem** option to specify the display name of the desktop or application pool, as shown in View Administrator.

Agent-to-Client Redirection

Add this template to the GPO for a remote desktop or application pool if you want certain URLs to be redirected to the Windows client.

For example, agent-to-client redirection might be used to conserve resources or as an added security layer. If employees are working in a remote desktop or application and they want to watch videos, for example, you might redirect those URLs to the client machine so that no extra load is put on the data center. Or for security purposes, for employees working outside the company network, you might want all URLs that point to external locations outside the company network to be opened on an employee's own client machine.

You could, for example, configure rules so that any content that is not company-related, that is, any URLs that do not point to the company network, are redirected to open on the client machine. In this case you could use the following settings, which include regular expressions:

- For **agentRules**: `.*.mycompany.com`
This rule means that any URL that contains the text **mycompany.com** should be opened on the agent.
- For **clientRules**: `.*`
This rule means that all URLs should be opened on the client, with the default client browser.

The feature uses the following process for applying the rules:

- 1 When a user clicks a link in a remote application or desktop, the client rules are checked first.
- 2 If a pattern in the URL matches a client rule, the agent rules are checked next.
- 3 If there is a conflict between the agent rules and the client rules, the link is opened locally, which means in this case, on the agent machine.
- 4 If there is no conflict, the URL is redirected to the client.

In the example above, there is a rules conflict because URLs with **mycompany.com** are a subset of all URLs. Because of this conflict, URLs with **mycompany.com** in them are opened locally. If you click a link with **mycompany.com** in the URL while in a remote desktop, the URL will be opened on that remote desktop. If you click a link with **mycompany.com** in the URL in it from a client system, the URL will be opened on the client.

Client-to-Agent Redirection

Add this template to the GPO for a group of client computers if you want certain URLs to be redirected to a remote desktop or application. For example, for security purposes you might want all URLs that point to the company network to be opened in a remote desktop or application. In that case you could set **agentRules** to:

```
.*.mycompany.com
```

To redirect URLs to a remote desktop or application pool, you must also specify which pool to use. Use the **brokerHostname** option to specify the IP address or fully qualified domain name of the connection server, and use the **remoteItem** option to specify the display name of the desktop or application pool, as shown in View Administrator.

If the URL is redirected to a remote desktop, the link is opened in the default browser for that desktop. If the URL is redirected to a remote application, the link is opened using the specified application pool. The end user must be entitled to the desktop or application pool specified.

You can add this template to GPOs for both agent and client, but if you do so, ensure that the rules do not conflict, or that any conflicts are intentional.

Template Setting Details

The following table describes policy settings in the Horizon URL Content Redirection ADM template file. The template contains Computer Configuration settings only.

Table 14-2. Horizon URL Content Redirection Template Settings

Setting	Properties
IE Policy: Users can't disable URL Redirection plugin	Determines whether users can disable URL Content Redirection. This setting is disabled by default.
IE Policy: Automatically activate newly installed plugins	Determines whether newly installed Internet Explorer plug-ins are automatically activated. This setting is disabled by default.
Url Redirection Enabled	Determines whether this feature is turned on. This setting is enabled by default. You can use this setting to disable the feature even if the component has been installed.
Url Redirection Protocol 'http'	For all URLs that use the HTTP protocol, specifies the URLs that should be redirected. For example, if you set agentRules to /*.mycompany.com then all URLs that have "mycompany.com" in them are redirected to a remote desktop or remote application. You can further specify which connection server to use by setting brokerHostname , and you can specify which desktop or application pool to use by setting remoteItem to the display name of the pool, as shown in View Administrator. If you set clientRules to /*.mycompany.com then all URLs that have "mycompany.com" in them are redirected to the Windows-based client and opened in the default browser on the client. NOTE As a best practice, set the same rules for the HTTP protocol and the HTTPS protocol. That way, if a user types a partial URL, such as mycompany.com into Internet Explorer, if that site automatically redirects from HTTP to HTTPS, the URL Content Redirection feature will work as desired. In this case, if you set a rule for HTTPS but not HTTP, the partial URL that the user types would not be redirected. This setting is disabled by default.

Table 14-2. Horizon URL Content Redirection Template Settings (Continued)

Setting	Properties
Url Redirection Protocol 'https'	For all URLs that use the HTTPS protocol, specifies the URLs that should be redirected. The options are the same as for Url Redirection Protocol 'http'. NOTE As a best practice, set the same rules for the HTTPS protocol and the HTTP protocol. This setting is disabled by default.
Url Redirection Protocol 'callto'	For all URLs that use the callto protocol, specifies the URLs that should be redirected. The options are the same as for Url Redirection Protocol 'http'. This setting is disabled by default.
Url Redirection Protocol 'email'	For all URLs that use the email or mailto protocol, specifies the URLs that should be redirected. The options are the same as for Url Redirection Protocol 'http'. This setting is disabled by default.
Url Redirection Protocol '[...]	This is a template that you can modify for any additional protocol. If you do not need to configure any additional protocol, you can delete or comment out this entry before adding the ADM template to Active Directory.

NOTE For client-to-agent redirection, if you configure a protocol that does not have a default handler, after you configure a GPO setting for this protocol, you must launch Horizon Client once before URLs that specify this protocol are redirected.

Configuring Real-Time Audio-Video

Real-Time Audio-Video allows View users to run Skype, Webex, Google Hangouts, and other online conferencing applications on their remote desktops. With Real-Time Audio-Video, webcam and audio devices that are connected locally to the client system are redirected to the remote desktop. This feature redirects video and audio data to the desktop with a significantly lower bandwidth than can be achieved by using USB redirection.

Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications, and supports standard webcams, audio USB devices, and analog audio input.

This feature installs the VMware Virtual Webcam and VMware Virtual Microphone on the desktop operating system. The VMware Virtual Webcam uses a kernel-mode webcam driver that provides enhanced compatibility with browser-based video applications and other 3rd-party conferencing software.

When a conferencing or video application is launched, it displays and uses these VMware virtual devices, which handle the audio-video redirection from the locally-connected devices on the client. The VMware Virtual Webcam and Microphone appear in the Device Manager on the desktop operating system.

The drivers for the audio and webcam devices must be installed on your Horizon Client systems to enable the redirection.

Configuration Choices for Real-Time Audio-Video

After you install Horizon Agent with Real-Time Audio-Video, the feature works on your View desktops without any further configuration. The default values for the webcam frame rate and image resolution are recommended for most standard devices and applications.

You can configure group policy settings to change these default values to adapt to particular applications, webcams, or environments. You can also set a policy to disable or enable the feature altogether. An ADM Template file lets you install Real-Time Audio-Video group policy settings on Active Directory or on individual desktops. See “[Configuring Real-Time Audio-Video Group Policy Settings](#),” on page 194.

If users have multiple webcams and audio input devices built in or connected to their client computers, you can configure preferred webcams and audio input devices that will be redirected to their desktops. See “[Selecting Preferred Webcams and Microphones](#),” on page 186.

NOTE You can select a preferred audio device, but no other audio configuration options are available.

When webcam images and audio input are redirected to a remote desktop, you cannot access the webcam and audio devices on the local computer. Conversely, when these devices are in use on the local computer, you cannot access them on the remote desktop.

For information about supported applications, see the VMware knowledge base article, *Guidelines for Using Real-Time Audio-Video with 3rd-Party Applications on Horizon View Desktops*, at <http://kb.vmware.com/kb/2053754>.

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices, and with standard conferencing applications like Skype, WebEx, and Google Hangouts. To support Real-Time Audio-Video, your View deployment must meet certain software and hardware requirements.

View remote desktop

You install the Real-Time Audio-Video feature by installing View Agent 6.0 or later, or Horizon Agent 7.0 or later. This feature is supported in desktop pools that are deployed on single-user virtual machines but not in RDS desktop pools. See “[Install Horizon Agent on a Virtual Machine](#),” on page 26.

Horizon Client software

Horizon Client 2.2 for Windows or a later release

Horizon Client 2.2 for Linux or a later release. For Horizon Client for Linux 3.1 or earlier, this feature is available only with the version of Horizon Client for Linux provided by third-party vendors. For Horizon Client for Linux 3.2 and later, this feature is also available with the version of the client available from VMware.

Horizon Client 2.3 for Mac OS X or a later release

Horizon Client 4.0 for iOS or a later release.

Horizon Client 4.0 for Android or a later release.

Horizon Client computer or client access device

- All operating systems that run Horizon Client for Windows.
- All operating systems that run Horizon Client for Linux on x86 devices. This feature is not supported on ARM processors.
- Mac OS X Mountain Lion (10.8) and later. It is disabled on all earlier Mac OS X operating systems.
- All operating systems that run Horizon Client for iOS.

- All operating systems than run Horizon Client for Android.
- For details about supported client operating systems, see the *Using VMware Horizon Client* document for the appropriate system or device.
- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. To support Real-Time Audio-Video, you do not have to install the device drivers on the desktop operating system where the agent is installed.

Display protocol for View

- PCoIP
- VMware Blast (requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later)

Real-Time Audio-Video is not supported in RDP desktop sessions.

Ensuring That Real-Time Audio-Video Is Used Instead of USB Redirection

Real-Time Audio-Video supports webcam and audio input redirection for use in conferencing applications. The USB redirection feature that can be installed with Horizon Agent does not support webcam redirection. If you redirect audio input devices through USB redirection, the audio stream does not synchronize properly with video during Real-Time Audio-Video sessions, and you lose the benefit of reducing the demand on network bandwidth. You can take steps to ensure that webcams and audio input devices are redirected to your desktops through Real-Time Audio-Video, not USB redirection.

If your desktops are configured with USB redirection, end users can connect and display their locally connected USB devices by selecting the **Connect USB Device** option in the Windows client menu bar or the **Desktop > USB** menu in the Mac OS X client. Linux clients block USB redirection of audio and video devices by default and do not provide the USB device options to end users.

If an end user selects a USB device from the **Connect USB Device** or **Desktop > USB** list, that device becomes unusable for video or audio conferencing. For example, if a user makes a Skype call, the video image might not appear or the audio stream might be degraded. If an end user selects a device during a conferencing session, the webcam or audio redirection is disrupted.

To hide these devices from end users and prevent potential disruptions, you can configure USB redirection group policy settings to disable the display of webcams and audio input devices in VMware Horizon Client.

In particular, you can create USB redirection filtering rules for Horizon Agent and specify the `audio-in` and `video` Device Family Names to be disabled. For information about setting group policies and specifying filtering rules for USB redirection, see [“Using Policies to Control USB Redirection,”](#) on page 220.



CAUTION If you do not set up USB redirection filtering rules to disable the USB device families, inform your end users that they cannot select webcam or audio devices from the **Connect USB Device** or **Desktop > USB** list in the VMware Horizon Client menu bar.

Selecting Preferred Webcams and Microphones

If a client computer has more than one webcam and microphone, you can configure a preferred webcam and default microphone that Real-Time Audio-Video will redirect to the desktop. These devices can be built in or connected to the local client computer.

On a Windows client computer, you select a preferred webcam by setting a registry key value. On a Mac OS X client computer, you can specify a preferred webcam or microphone by using the Mac OS X defaults system. On a Linux client computer, you can specify a preferred webcam or microphone by editing a configuration file. Real-Time Audio-Video redirects the preferred webcam if it is available. If not, Real-Time Audio-Video uses the first webcam that is provided by system enumeration.

To select a default microphone, you can configure the Sound control in the Windows, Mac OS X, or Linux operating system on the client computer.

Select a Default Microphone on a Windows Client System

If you have multiple microphones on your client system, only one of them is used on your View desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

IMPORTANT If you are using a USB microphone, do not connect it from the **Connect USB Device** menu in Horizon Client. To do so routes the device through USB redirection so that the device cannot use the Real-Time Audio-Video feature.

Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 If you are currently on a call, stop the call.
- 2 Right-click the speaker icon in your system tray and select **Recording devices**.
You can alternatively open the Sound control from the Control Panel and click the **Recording** tab.
- 3 In the **Recording** tab of the Sound dialog box, right-click the microphone you prefer to use.
- 4 Select **Set as Default Device** and click **OK**.
- 5 Start a new call from your View desktop.

Select a Preferred Webcam on a Windows Client System

With the Real-Time Audio-Video feature, if you have multiple webcams on your client system, only one of them is used on your View desktop. To specify which webcam is preferred, you can set a registry key value.

The preferred webcam is used on the remote desktop if it is available, and if not, another webcam is used.

Prerequisites

- Verify that you have a USB webcam installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 Attach the webcam you want to use.
- 2 Start a call and then stop a call.

This process creates a log file.

- 3 Open the debug log file with a text editor.

Operating System	Log File Location
Windows XP	C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt
Windows 7 or Windows 8	C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt

The format of the log file is debug-20YY-MM-DD-XXXXXX.txt, where 20YY is the year, MM is the month, DD is the day, and XXXXXX is a number.

- 4 Search the log file for [ViewMMDevRedir] VideoInputBase::LogDevEnum to find the log file entries that reference the attached webcams.

Here is an excerpt from the log file identifying the Microsoft Lifecam HD-5000 webcam:

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found
```

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000 SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#
```

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam HD-5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000 SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

- 5 Copy the user ID of the preferred webcam.
For example, copy vid_045e&pid_076d&mi_00#8&11811f49&0&0000 to set the Microsoft LifeCam HD-5000 as the default webcam.
- 6 Start the Registry Editor (regedit.exe) and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV.
- 7 Paste the ID portion of the string into the REG_SZ value, **srcWCamId**.
For example, paste vid_045e&pid_076d&mi_00#8&11811f49&0&0000 into **srcWCamId**.
- 8 Save your changes and exit the registry.
- 9 Start a new call.

Select a Default Microphone on a Mac OS X Client System

If you have multiple microphones on your client system, only one microphone is used on your remote desktop. You can use System Preferences on your client system to specify which microphone is the default microphone on the remote desktop.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

This procedure describes how to choose a microphone from the user interface of the client system. Administrators can also configure a preferred microphone by using the Mac OS X defaults system. See [“Configure a Preferred Webcam or Microphone on a Mac OS X Client System,”](#) on page 189.

IMPORTANT If you are using a USB microphone, do not connect it from the **Connection > USB** menu in Horizon Client. To do so routes the device through USB redirection and the device cannot use the Real-Time Audio-Video feature.

Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 On your client system, select **Apple menu > System Preferences** and click **Sound**.
- 2 Open the Input pane of Sound preferences.
- 3 Select the microphone that you prefer to use.

The next time that you connect to a remote desktop and start a call, the desktop uses the default microphone that you selected on the client system.

Configuring Real-Time Audio-Video on a Mac OS X Client

You can configure Real-Time Audio-Video settings at the command line by using the Mac OS X defaults system. With the defaults system, you can read, write, and delete Mac OS X user defaults by using Terminal (`/Applications/Utilities/Terminal.app`).

Mac OS X defaults belong to domains. Domains typically correspond to individual applications. The domain for the Real-Time Audio-Video feature is `com.vmware.rtav`.

Syntax for Configuring Real-Time Audio-Video

You can use the following commands to configure the Real-Time Audio-Video feature.

Table 14-3. Command Syntax for Real-Time Audio-Video Configuration

Command	Description
<code>defaults write com.vmware.rtav srcWCamId "webcam-userid"</code>	Sets the preferred webcam to use on remote desktops. When this value is not set, the webcam is selected automatically by system enumeration. You can specify any webcam connected to (or built into) the client system.
<code>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</code>	Sets the preferred microphone (audio-in device) to use on remote desktops. When this value is not set, remote desktops use the default recording device set on the client system. You can specify any microphone connected to (or built into) the client system.
<code>defaults write com.vmware.rtav srcWCamFrameWidth pixels</code>	Sets the image width. The value defaults to a hardcoded value of 320 pixels. You can change the image width to any pixel value.
<code>defaults write com.vmware.rtav srcWCamFrameHeight pixels</code>	Sets the image height. The value defaults to a hardcoded value of 240 pixels. You can change the image height to any pixel value.
<code>defaults write com.vmware.rtav srcWCamFrameRate fps</code>	Sets the frame rate. The value defaults to 15 fps. You can change the frame rate to any value.
<code>defaults write com.vmware.rtav LogLevel "level"</code>	Sets the logging level for the Real-Time Audio-Video log file (<code>~/Library/Logs/VMware/vmware-RTAV-pid.log</code>). You can set the logging level to trace or debug.

Table 14-3. Command Syntax for Real-Time Audio-Video Configuration (Continued)

Command	Description
<code>defaults write com.vmware.rtav IsDisabled <i>value</i></code>	Determines whether Real-Time Audio-Video is enabled or disabled. Real-Time Audio-Video is enabled by default. (This value is not in effect.) To disable Real-Time Audio-Video on the client, set the value to true.
<code>defaults read com.vmware.rtav</code>	Displays Real-Time Audio-Video configuration settings.
<code>defaults delete com.vmware.rtav <i>setting</i></code>	Deletes a Real-Time Audio-Video configuration setting, for example: <code>defaults delete com.vmware.rtav srcWCamFrameWidth</code>

NOTE You can adjust frame rates from 1 fps up to a maximum of 25 fps and resolution up to a maximum of 1920x1080. A high resolution at a fast frame rate might not be supported on all devices or in all environments.

Configure a Preferred Webcam or Microphone on a Mac OS X Client System

With the Real-Time Audio-Video feature, if you have multiple webcams or microphones on your client system, only one webcam and one microphone can be used on your remote desktop. You specify which webcam and microphone are preferred at the command line by using the Mac OS X defaults system.

With the Real-Time Audio-Video feature, webcams, audio input devices, and audio output devices work without requiring USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

In most environments, there is no need to configure a preferred microphone or webcam. If you do not set a preferred microphone, remote desktops use the default audio device set in the client system's System Preferences. See [“Select a Default Microphone on a Mac OS X Client System,”](#) on page 187. If you do not configure a preferred webcam, the remote desktop selects the webcam by enumeration.

Prerequisites

- If you are configuring a preferred USB webcam, verify that the webcam is installed and operational on your client system.
- If you are configuring a preferred USB microphone or other type of microphone, verify that the microphone is installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 On your Mac OS X client system, start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the Real-Time Audio-Video log file.
 - a Attach the webcam or audio device.
 - b In the **Applications** folder, double-click **VMware Horizon View Client** (Horizon Client 3.0) or **VMware Horizon Client** (Horizon Client 3.1 and later) to start Horizon Client.
 - c Start a call and then stop the call.

- 2 Find log entries for the webcam or microphone in the Real-Time Audio-Video log file.
 - a In a text editor, open the Real-Time Audio-Video log file.

The Real-Time Audio-Video log file is named `~/Library/Logs/VMware/vmware-RTAV-pid.log`, where *pid* is the process ID of the current session.

- b Search the Real-Time Audio-Video log file for entries that identify the attached webcams or microphones.

The following example shows how webcam entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)  UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509  SystemId=0xfa20000005ac8509
```

The following example shows how microphone entries might appear in the Real-Time Audio-Video log file:

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255  Name=Built-in Microphone  UserId=Built-in Microphone#AppleHDAEngineInput:1B,
0,1,0:1  SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255  Name=Built-in Input  UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

- 3 Find the webcam or microphone that you prefer in the Real-Time Audio-Video log file and make a note of its user ID.

The user ID appears after the string `UserId=` in the log file. For example, the user ID of the internal face time camera is `FaceTime HD Camera (Built-in)` and the user ID of the internal microphone is `Built-in Microphone`.

- 4 In Terminal (`/Applications/Utilities/Terminal.app`), use the `defaults write` command to set the preferred webcam or microphone.

Option	Action
Set the preferred webcam	Type <code>defaults write com.vmware.rtav srcWCamId "<i>webcam-userid</i>"</code> , where <i>webcam-userid</i> is the user ID of the preferred webcam, which you obtained from the Real-Time Audio-Video log file. For example: <code>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</code>
Set the preferred microphone	Type <code>defaults write com.vmware.rtav srcAudioInId "<i>audio-device-userid</i>"</code> , where <i>audio-device-userid</i> is the user ID of the preferred microphone, which you obtained from the Real-Time Audio-Video log file. For example: <code>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</code>

- 5 (Optional) Use the `defaults read` command to verify your changes to the Real-Time Audio-Video feature.

For example: `defaults read com.vmware.rtav`

The command lists all of the Real-Time Audio-Video settings.

The next time you connect to a remote desktop and start a new call, the desktop uses the preferred webcam or microphone that you configured, if it is available. If the preferred webcam or microphone is not available, the remote desktop can use another available webcam or microphone.

Select a Default Microphone on a Linux Client System

If you have multiple microphones on your client system, only one of them is used on your View desktop. To specify which microphone is the default, you can use the Sound control on your client system.

With the Real-Time Audio-Video feature, audio input devices and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

This procedure describes choosing a default microphone from the user interface of the client system. Administrators can also configure a preferred microphone by editing a configuration file. See [“Select a Preferred Webcam or Microphone on a Linux Client System,”](#) on page 191.

Prerequisites

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 In the Ubuntu graphical user interface, select **System > Preferences > Sound**.
You can alternatively click the **Sound** icon on the right side of the toolbar at the top of the screen.
- 2 Click the **Input** tab in the Sound Preferences dialog box.
- 3 Select the preferred device and click **Close**.

Select a Preferred Webcam or Microphone on a Linux Client System

With the Real-Time Audio-Video feature, if you have multiple webcams and microphones on your client system, only one webcam and one microphone can be used on your View desktop. To specify which webcam and microphone are preferred, you can edit a configuration file.

The preferred webcam or microphone is used on the View desktop if it is available, and if not, another webcam or microphone is used.

With the Real-Time Audio-Video feature, webcams, audio input devices, and audio output devices work without requiring the use of USB redirection, and the amount network bandwidth required is greatly reduced. Analog audio input devices are also supported.

To set the properties in the `/etc/vmware/config` file and specify a preferred device, you must determine the device ID.

- For webcams, you set the `rtav.srcWCamId` property to the value of the webcam description found in the log file, as described in the procedure that follows.
- For audio devices, you set the `rtav.srcAudioInId` property to the value of the Pulse Audio `device.description` field.

To find the value of this field you can search the log file, as described in the procedure that follows.

Prerequisites

Depending on whether you are configuring a preferred webcam, preferred microphone, or both, perform the appropriate prerequisite tasks:

- Verify that you have a USB webcam installed and operational on your client system.

- Verify that you have a USB microphone or another type of microphone installed and operational on your client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for your remote desktop.

Procedure

- 1 Launch the client, and start a webcam or microphone application to trigger an enumeration of camera devices or audio devices to the client log.
 - a Attach the webcam or audio device you want to use.
 - b Use the command `vmware-view` to start Horizon Client.
 - c Start a call and then stop the call.

This process creates a log file.

2 Find log entries for the webcam or microphone.

- a Open the debug log file with a text editor.

The log file with real-time audio-video log messages is located at `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. The client log is located at `/tmp/vmware-<username>/vmware-view-<pid>.log`.

- b Search the log file to find the log file entries that reference the attached webcams and microphones.

The following example shows an extract of the webcam selection:

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=Microsoft®
LifeCam HD-6000 for Notebooks   UserId=Microsoft LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

The following example shows an extract of the audio device selection, and the current audio level for each:

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering
enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of
Microsoft LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
```

Warnings are shown if any of the source audio levels for the selected device do not meet the PulseAudio criteria if the source is not set to 100% (0dB), or if the selected source device is muted, as follows:

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 Copy the description of the device and use it to set the appropriate property in the `/etc/vmware/config` file.

For a webcam example, copy `Microsoft® LifeCam HD-6000 for Notebooks` to specify the Microsoft webcam as the preferred webcam and set the property as follows:

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

For this example you could also set the property to `rtav.srcWCamId="Microsoft"`.

For an audio device example, copy `Logitech USB Headset Analog Mono` to specify the Logitech headset as the preferred audio device and set the property as follows:

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 Save your changes and close the `/etc/vmware/config` configuration file.
- 5 Log off of the desktop session and start a new session.

Configuring Real-Time Audio-Video Group Policy Settings

You can configure group policy settings that control the behavior of Real-Time Audio-Video (RTAV) on your View desktops. These settings determine a virtual webcam's maximum frame rate and image resolution. The settings allow you to manage the maximum bandwidth that any one user can consume. An additional setting disables or enables the RTAV feature.

You do not have to configure these policy settings. Real-Time Audio-Video works with the frame rate and image resolution that are set for the webcam on client systems. The default settings are recommended for most webcam and audio applications.

For examples of bandwidth use during Real-Time Audio-Video, see [“Real-Time Audio-Video Bandwidth,”](#) on page 196.

These policy settings affect your View desktops, not the client systems to which the physical devices are connected. To configure these settings on your desktops, add the RTAV Group Policy Administrative Template (ADM) file in Active Directory.

For information about configuring settings on client systems, see the VMware knowledge base article, *Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients*, at <http://kb.vmware.com/kb/2053644>.

Add the RTAV ADM Template in Active Directory and Configure the Settings

You can add the policy settings in the RTAV ADM file, `vdm_agent_rtav.adm`, to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the RTAV setup option is installed on your desktops. This setup option is installed by default but can be deselected during installation. The settings have no effect if RTAV is not installed. See [“Install Horizon Agent on a Virtual Machine,”](#) on page 26.
- Verify that Active Directory GPOs are created for the RTAV group policy settings. The GPOs must be linked to the OU that contains your desktops. See [“Active Directory Group Policy Example,”](#) on page 297.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with RTAV group policy settings. See [“Real-Time Audio-Video Group Policy Settings,”](#) on page 195.

Procedure

- 1 Download the View 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 View are available in this file.
- 2 Unzip the VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip file and copy the RTAV ADM file, vdm_agent_rtav.adm, to your Active Directory server.
- 3 On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
- 4 In the Group Policy Object Editor, right-click the **Computer Configuration > Administrative Templates** folder and select **Add/Remove Templates**.
- 5 Click **Add**, browse to the vdm_agent_rtav.adm file, and click **Open**.
- 6 Click **Close** to apply the policy settings in the ADM file to the GPO.

The settings are located in the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware Horizon Agent Configuration > View RTAV Configuration** folder.
- 7 Configure the RTAV group policy settings.

Real-Time Audio-Video Group Policy Settings

The Real-Time Audio-Video (RTAV) group policy settings control the virtual webcam's maximum frame rate and maximum image resolution. An additional setting lets you disable or enable the RTAV feature. These policy settings affect View desktops, not the client systems where the physical devices are connected.

If you do not configure the RTAV group policy settings, RTAV uses the values that are set on the client systems. On client systems, the default webcam frame rate is 15 frames per second. The default webcam image resolution is 320x240 pixels.

The **Resolution - Max image...** group policy settings determine the maximum values that can be used. The frame rate and resolution that are set on client systems are absolute values. For example, if you configure the RTAV settings for maximum image resolution to 640x480 pixels, the webcam displays any resolution that is set on the client up to 640x480 pixels. If you set the image resolution on the client to a value higher than 640x480 pixels, the client resolution is capped at 640x480 pixels.

Not all configurations can achieve the maximum group policy settings of 1920x1080 resolution at 25 frames per second. The maximum frame rate that your configuration can achieve for a given resolution depends upon the webcam being used, the client system hardware, the Horizon Agent virtual hardware, and the available bandwidth.

The **Resolution - Default image...** group policy settings determine the default values that are used when resolution values are not set by the user.

Group Policy Setting	Description
Disable RTAV	<p>When you enable this setting, the Real-Time Audio-Video feature is disabled.</p> <p>When this setting is not configured or disabled, Real-Time Audio-Video is enabled.</p> <p>This setting is located in the View RTAV Configuration folder.</p>
Max frames per second	<p>Determines the maximum rate per second at which the webcam can capture frames. You can use this setting to limit the webcam frame rate in low-bandwidth network environments.</p> <p>The minimum value is one frame per second. The maximum value is 25 frames per second.</p> <p>When this setting is not configured or disabled, no maximum frame rate is set. Real-Time Audio-Video uses the frame rate that is selected for the webcam on the client system.</p> <p>By default, client webcams have a frame rate of 15 frames per second. If no setting is configured on the client system and the Max frames per second setting is not configured or disabled, the webcam captures 15 frames per second.</p> <p>This setting is located in the View RTAV Configuration > View RTAV Webcam Settings folder.</p>
Resolution - Max image width in pixels	<p>Determines the maximum width, in pixels, of image frames that are captured by the webcam. By setting a low maximum image width, you can lower the resolution of captured frames, which can improve the imaging experience in low-bandwidth network environments.</p> <p>When this setting is not configured or disabled, a maximum image width is not set. RTAV uses the image width that is set on the client system. The default width of a webcam image on a client system is 320 pixels.</p> <p>The maximum limit for any webcam image is 1920x1080 pixels. If you configure this setting with a value that is higher than 1920 pixels, the effective maximum image width is 1920 pixels.</p> <p>This setting is located in the View RTAV Configuration > View RTAV Webcam Settings folder.</p>
Resolution - Max image height in pixels	<p>Determines the maximum height, in pixels, of image frames that are captured by the webcam. By setting a low maximum image height, you can lower the resolution of captured frames, which can improve the imaging experience in low-bandwidth network environments.</p> <p>When this setting is not configured or disabled, a maximum image height is not set. RTAV uses the image height that is set on the client system. The default height of a webcam image on a client system is 240 pixels.</p> <p>The maximum limit for any webcam image is 1920x1080 pixels. If you configure this setting with a value that is higher than 1080 pixels, the effective maximum image height is 1080 pixels.</p> <p>This setting is located in the View RTAV Configuration > View RTAV Webcam Settings folder.</p>
Resolution - Default image resolution width in pixels	<p>Determines the default resolution width, in pixels, of image frames that are captured by the webcam.</p> <p>This setting is used when no resolution value is defined by the user.</p> <p>When this setting is not configured or disabled, the default image width is 320 pixels.</p> <p>The value that is configured by this policy setting takes effect only if both View Agent 6.0 or later and Horizon Client 3.0 or later are used. For older versions of View Agent and Horizon Client, this policy setting has no effect, and the default image width is 320 pixels.</p> <p>This setting is located in the View RTAV Configuration > View RTAV Webcam Settings folder.</p>
Resolution - Default image resolution height in pixels	<p>Determines the default resolution height, in pixels, of image frames that are captured by the webcam.</p> <p>This setting is used when no resolution value is defined by the user.</p> <p>When this setting is not configured or disabled, the default image height is 240 pixels.</p> <p>The value that is configured by this policy setting takes effect only if both View Agent 6.0 or later and Horizon Client 3.0 or later are used. For older versions of View Agent and Horizon Client, this policy setting has no effect, and the default image height is 240 pixels.</p> <p>This setting is located in the View RTAV Configuration > View RTAV Webcam Settings folder.</p>

Real-Time Audio-Video Bandwidth

Real-Time Audio-Video bandwidth varies according to the webcam's image resolution and frame rate, and the image and audio data being captured.

The sample tests shown in [Table 14-4](#) measure the bandwidth that Real-Time Audio-Video uses in a View environment with standard webcam and audio input devices. The tests measure the bandwidth to send both video and audio data from Horizon Client to Horizon Agent. The total bandwidth that is required to run a desktop session from Horizon Client might be higher than these numbers. In these tests, the webcam captures images at 15 frames per second for each image resolution.

Table 14-4. Sample Bandwidth Results for Sending Real-Time Audio-Video Data from Horizon Client to Horizon Agent

Image Resolution (Width x Height)	Bandwidth Used (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

Configuring Scanner Redirection

By using scanner redirection, View users can scan information in their remote desktops and applications with scanning and imaging devices that are connected locally to their client computers. Scanner redirection is available in Horizon 6.0.2 and later releases.

Scanner redirection supports standard scanning and imaging devices that are compatible with the TWAIN and WIA formats.

After you install Horizon Agent with the Scanner Redirection setup option, the feature works on your remote desktops and applications without further configuration. You do not have to configure scanner-specific drivers on remote desktops or applications.

You can configure group policy settings to change default values to adapt to particular scanning and imaging applications or environments. You can also set a policy to disable or enable the feature altogether. With an ADM template file, you can install scanner redirection group policy settings in Active Directory or on individual desktops. See [“Configuring Scanner Redirection Group Policy Settings,”](#) on page 199.

When scanning data is redirected to a remote desktop or application, you cannot access the scanning or imaging device on the local computer. Conversely, when a device is in use on the local computer, you cannot access it on the remote desktop or application.

System Requirements for Scanner Redirection

To support scanner redirection, your View deployment must meet certain software and hardware requirements.

View remote desktop or application

This feature is supported on RDS desktops, RDS applications, and VDI desktops that are deployed on single-user virtual machines.

You must install View Agent 6.0.2 or later, and select the Scanner Redirection setup option, on the parent or template virtual machines or RDS hosts.

On Windows Desktop and Windows Server guest operating systems, the Horizon Agent Scanner Redirection setup option is deselected by default.

The following guest operating systems are supported on single-user virtual machines and, where noted, on RDS hosts:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop or RDS host

- Windows Server 2012 R2 configured as a desktop or RDS host

IMPORTANT The Desktop Experience feature must be installed on Windows Server guest operating systems, whether they are configured as desktops or as RDS hosts.

The scanner device drivers do not have to be installed on the desktop operating system where Horizon Agent is installed.

Horizon Client software	Horizon Client 3.2 for Windows or a later release
Horizon Client computer or client access device	Supported operating systems: <ul style="list-style-type: none"> ■ 32-bit or 64-bit Windows 7 ■ 32-bit or 64-bit Windows 8.x ■ 32-bit or 64-bit Windows 10 <p>The scanner device drivers must be installed, and the scanner must be operable, on the client computer.</p>
Scanning device standard	TWAIN or WIA
Display protocol for View	PCoIP Scanner redirection is not supported in RDP desktop sessions.

User Operation of Scanner Redirection

With scanner redirection, users can operate physical scanners and imaging devices that are connected to their client computers as virtual devices that perform scanning operations in their remote desktops and applications.

Users can operate their virtual scanners in a way that closely parallels the way that they use the scanners on their locally connected client computers.

- After the Scanner Redirection option is installed with Horizon Agent, a scanner tool tray icon () is added to the desktop. On RDS applications, the tool tray icon is redirected to the local client computer.

You do not have to use the scanner tool tray icon. Scanning redirection works without any further configuration. You can use the icon to configure options such as changing which device to use if more than one device is connected to the client computer.

- When you click the scanner icon, the Scanner Redirection for VMware Horizon menu is displayed. No scanners appear in the menu list if incompatible scanners are connected to the client computer.
- By default, scanning devices are autoselected. TWAIN and WIA scanners are selected separately. You can have one TWAIN scanner and one WIA scanner selected at the same time.
- If more than one locally connected scanner is configured, you can select a different scanner than the one that is selected by default.
- WIA scanners are displayed in the remote desktop's Device Manager menu, under **Imaging devices**. The WIA scanner is named **VMware Virtual WIA Scanner**.
- In the Scanner Redirection for VMware Horizon menu, you can click the **Preferences** option and select options such as hiding webcams from the scanner redirection menu and determining how to select the default scanner.

You can also control these features by configuring scanner redirection group policy settings in Active Directory. See [“Scanner Redirection Group Policy Settings,”](#) on page 200.

- When you operate a TWAIN scanner, the TWAIN Scanner Redirection for VMware Horizon menu provides additional options for selecting regions of an image, scanning in color, black and white, or grayscale, and choosing other common functions.
- To display the TWAIN user interface window for TWAIN scanning software that does not display the window by default, you can select an **Always show Scanner Settings dialog** option in the VMware Horizon Scanner Redirection Preferences dialog box.

Note that most TWAIN scanning software displays the TWAIN user interface window by default. For this software, the window is always displayed, whether you select or deselect the **Always show Scanner Settings dialog** option.

NOTE If you run two RDS applications that are hosted on different farms, two scanner redirection tool tray icons appear on the client computer. Typically, only one scanner is connected to a client computer. In this case, both icons operate the same device, and it does not matter which icon you select. In some situations, you might have two locally connected scanners and run two RDS applications that run on different farms. In that case, you must open each icon to see which scanner redirection menu controls which RDS application.

For end-user instructions for operating redirected scanners, see the *Using VMware Horizon Client for Windows* document.

Configuring Scanner Redirection Group Policy Settings

You can configure group policy settings that control the behavior of scanner redirection on your View desktops and applications. With these policy settings, you can control centrally, from Active Directory, the options that are available in the VMware Horizon Scanner Redirection Preferences dialog box on users' desktops and applications.

You do not have to configure these policy settings. Scanner redirection works with the default settings that are configured for scanning devices on remote desktops and client systems.

These policy settings affect your remote desktops and applications, not the client systems where the physical scanners are connected. To configure these settings on your desktops and applications, add the Scanner Redirection Group Policy Administrative Template (ADM) file in Active Directory.

Add the Scanner Redirection ADM Template in Active Directory

You can add the policy settings in the scanner redirection ADM file, `vdm_agent_scanner.adm`, to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the Scanner Redirection setup option is installed on your desktops and RDS hosts. The group policy settings have no effect if scanner redirection is not installed. See [“Install Horizon Agent on a Virtual Machine,”](#) on page 26.
- Verify that Active Directory GPOs are created for the scanner redirection group policy settings. The GPOs must be linked to the OU that contains your desktops and RDS hosts. See [“Active Directory Group Policy Example,”](#) on page 297.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with scanner redirection group policy settings. See [“Scanner Redirection Group Policy Settings,”](#) on page 200.

Procedure

- 1 Download the View 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 View are available in this file.
- 2 Unzip the VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip file and copy the scanner redirection ADM file, vdm_agent_scanner.adm, to your Active Directory server.
- 3 On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
- 4 In the Group Policy Object Editor, right-click the **Computer Configuration > Administrative Templates** folder and select **Add/Remove Templates**.
- 5 Click **Add**, browse to the vdm_agent_scanner.adm file, and click **Open**.
- 6 Click **Close** to apply the policy settings in the ADM file to the GPO.

The settings are located in the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Scanner Redirection** folder.

Most settings are also added to the **User Configuration** folder, located in **User Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Scanner Redirection**.
- 7 Configure the scanner redirection group policy settings.

Scanner Redirection Group Policy Settings

The scanner redirection group policy settings control the options that are available in the VMware Horizon Scanner Redirection Preferences dialog box on users' desktops and applications.

The scanner redirection ADM file contains both Computer Configuration and User Configuration policies. The User Configuration policies allow you to set different configurations for users of VDI desktops, RDS desktops, and RDS applications. Different User Configuration policies can take effect even when users' desktop sessions and applications are running on the same RDS hosts.

Group Policy Setting	Description
Disable functionality	<p>Disables the scanner redirection feature.</p> <p>This setting is available as a Computer Configuration policy only.</p> <p>When you enable this setting, scanners cannot be redirected and do not appear in the scanner menu on users' desktops and applications.</p> <p>When you disable this setting or do not configure it, scanner redirection works and scanners appear in the scanner menu.</p>
Lock config	<p>Locks the scanner redirection user interface and prevents users from changing configuration options on their desktops and applications.</p> <p>This setting is available as a Computer Configuration policy only.</p> <p>When you enable this setting, users cannot configure the options that are available from the tray menu on their desktops and applications. Users can display the VMware Horizon Scanner Redirection Preferences dialog box, but the options are inactive and cannot be changed.</p> <p>When you disable this setting or do not configure it, users can configure the options in the VMware Horizon Scanner Redirection Preferences dialog box.</p>

Group Policy Setting	Description
Compression	<p>Sets the image compression rate during the image transfer to the remote desktop or application. You can choose from the following compression modes:</p> <ul style="list-style-type: none"> ■ Disable. Image compression is disabled. ■ Lossless. Lossless (zlib) compression is used without loss of image quality. ■ JPEG. JPEG compression is used with loss of quality. You specify the level of image quality in the JPEG compression quality field. JPEG compression quality must be a value between 0 and 100. <p>When you enable this setting, the selected compression mode is set for all users affected by this policy. However, users can change the Compression option in the VMware Horizon Scanner Redirection Preferences dialog box, overriding the policy setting.</p> <p>When you disable this policy setting or do not configure it, JPEG compression mode is used.</p>
Hide Webcam	<p>Prevents webcams from appearing in the scanner selection menu in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>This setting is available as a Computer Configuration and User Configuration policy.</p> <p>By default, webcams can be redirected to desktops and applications. Users can select webcams and use them as virtual scanners to capture images.</p> <p>When you enable this setting as a Computer Configuration policy, webcams are hidden from all users of the affected computers. Users cannot change the Hide Webcam option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting as a User Configuration policy, webcams are hidden from all affected users. However, users can change the Hide Webcam option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting in both Computer Configuration and User Configuration, the Hide Webcam setting in Computer Configuration overrides the corresponding policy setting in User Configuration for all users of the affected computers.</p> <p>When you disable this setting or do not configure it in either policy configuration, the Hide Webcam setting is determined by the corresponding policy setting (either User Configuration or Computer Configuration) or by user selection in the VMware Horizon Scanner Redirection Preferences dialog box.</p>
Default Scanner	<p>Provides centralized management of scanner autoselection.</p> <p>This setting is available as a Computer Configuration and User Configuration policy.</p> <p>You select scanner autoselection options separately for TWAIN and WIA scanners. You can choose from the following autoselection options:</p> <ul style="list-style-type: none"> ■ None. Do not select scanners automatically. ■ Autoselect Automatically select the locally connected scanner. ■ Last used Automatically select the last-used scanner. ■ Specified Select the scanner name that you type in the Specified scanner text box. <p>When you enable this setting as a Computer Configuration policy, the setting determines the scanner autoselection mode for all users of the affected computers. Users cannot change the Default Scanner option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting as a User Configuration policy, the setting determines the scanner autoselection mode for all affected users. However, users can change the Default Scanner option in the VMware Horizon Scanner Redirection Preferences dialog box.</p> <p>When you enable this setting in both Computer Configuration and User Configuration, the scanner autoselection mode in Computer Configuration overrides the corresponding policy setting in User Configuration for all users of the affected computers.</p> <p>When you disable this setting or do not configure it in either policy configuration, the scanner autoselection mode is determined by the corresponding policy setting (either User Configuration or Computer Configuration) or by user selection in the VMware Horizon Scanner Redirection Preferences dialog box.</p>

Configuring Serial Port Redirection

With serial port redirection, users can redirect locally connected, serial (COM) ports such as built-in RS232 ports or USB to Serial adapters. Devices such as printers, bar code readers, and other serial devices can be connected to these ports and used in the remote desktops.

Serial port redirection is available in Horizon 6 version 6.1.1 and later releases with Horizon Client for Windows 3.4 and later releases.

After you install Horizon Agent and set up the serial port redirection feature, the feature can work on your remote desktops without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop, and COM2 is redirected as COM2, unless a COM port already exists on the remote desktop. If so, the COM port is mapped to avoid conflicts. For example, if COM1 and COM2 already exist on the remote desktop, COM1 on the client is mapped to COM3 by default. You do not have to configure the COM ports or install device drivers on the remote desktops.

To make a redirected COM port active, a user selects the **Connect** option from the menu on the serial port tool tray icon during a desktop session. A user can also set a COM port device to connect automatically whenever the user logs in to the remote desktop. See [“User Operation of Serial Port Redirection,”](#) on page 203.

You can configure group policy settings to change the default configuration. For example, you can lock the settings so that users cannot change the COM port mappings or properties. You can also set a policy to disable or enable the feature altogether. With an ADM template file, you can install serial port redirection group policy settings in Active Directory or on individual desktops. See [“Configuring Serial Port Redirection Group Policy Settings,”](#) on page 205.

When a redirected COM port is opened and in use on a remote desktop, you cannot access the port on the local computer. Conversely, when a COM port is in use on the local computer, you cannot access the port on the remote desktop.

Requirements for Serial Port Redirection

With this feature, users can redirect locally connected, serial (COM) ports, such as built-in RS232 ports or USB to Serial adapters, to their remote desktops. To support serial port redirection, your View deployment must meet certain software and hardware requirements.

View remote desktop

The remote desktops must have View Agent 6.1.1 or later, or Horizon Agent 7.0 or later, installed with the Serial Port Redirection setup option, on the parent or template virtual machines. This setup option is deselected by default.

The following guest operating systems are supported on single-user virtual machines:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop

This feature is not currently supported for Windows Server RDS hosts.

Serial port device drivers do not have to be installed on the desktop operating system where the agent is installed.

Horizon Client computer or client access device

- The client system must have Horizon Client for Windows 3.4 or later installed.
- Serial port redirection is supported on 32-bit or 64-bit Windows 7 client systems, 32-bit or 64-bit Windows 8.x client systems, and 32-bit or 64-bit Windows 10 client systems.
- Any required serial port device drivers must be installed, and the serial port must be operable, on the client computer. You do not need to install the device drivers on the remote desktop operating system where the agent is installed.

Display protocol for View

- PCoIP
- VMware Blast Extreme (requires Horizon Client 4.0 or later and Horizon Agent 7.0 or later)

VMware Horizon serial port redirection is not supported in RDP desktop sessions.

User Operation of Serial Port Redirection

Users can operate physical COM port devices that are connected to their client computers and use serial port virtualization to connect the devices to their remote desktops, where the devices are accessible to 3rd party applications.

- After the Serial Port Redirection option is installed with Horizon Agent, a serial port tool tray icon () is added to the remote desktop.

The icon appears only if you use the required versions of Horizon Agent and Horizon Client for Windows, and you connect over PCoIP. The icon does not appear if you connect to a remote desktop from a Mac, Linux, or mobile client.

You can use the icon to configure options to connect, disconnect, and customize the mapped COM ports.

- When you click the serial port icon, the **Serial COM Redirection for VMware Horizon** menu appears.
- By default, the locally connected COM ports are mapped to corresponding COM ports on the remote desktop. For example: **COM1 mapped to COM3**. The mapped ports are not connected by default.
- To use a mapped COM port, you must manually select the **Connect** option in the **Serial COM Redirection for VMware Horizon** menu, or the **Autoconnect** option must be set during a previous desktop session or by configuring a group policy setting. **Autoconnect** configures a mapped port to connect automatically when a remote desktop session is started.
- When you select the **Connect** option, the redirected port is active. In the Device Manager in the guest operating system on the remote desktop, the redirected port is shown as **Serial Port Redirector for VMware Horizon (COMn)**.

When the COM port is connected, you can open the port in a 3rd-party application, which can exchange data with the COM port device that is connected to the client machine. While a port is open in an application, you cannot disconnect the port in the **Serial COM Redirection for VMware Horizon** menu.

Before you can disconnect the COM port, you must close the port in the application or close the application. You can then select the **Disconnect** option to disconnect the port and make the physical COM port available for use on the client machine.

- In the **Serial COM Redirection for VMware Horizon** menu, you can right-click a redirected port to select the **Port Properties** command.

In the COM Properties dialog box, you can configure a port to connect automatically when a remote desktop session is started, ignore the Data Set Ready (DSR) signal, and map the local port on the client to a different COM port on the remote desktop by selecting a port in the **Custom port name** drop-down list.

A remote desktop port might be shown as overlapped. For example, you might see **COM1 (Overlapped)**. In this case, the virtual machine is configured with a COM port in the virtual hardware on the ESXi host. You can use a redirected port even when it is mapped to an overlapped port on the virtual machine. The virtual machine receives serial data through the port from the ESXi host or from the client system.

- In the Device Manager in the guest operating system, you can use the **Properties > Port Settings** tab to configure settings for a redirected COM port. For example, you can set the default baud rate and data bits. However, the settings you configure in Device Manager are ignored if the application specifies the port settings.

For end-user instructions for operating redirected serial COM ports, see the *Using VMware Horizon Client for Windows* document.

Guidelines for Configuring Serial Port Redirection

Through the group policy settings, you can configure serial port redirection and control the extent to which users can customize redirected COM ports. Your choices depend on the user roles and 3rd-party applications in your organization.

For details about the group policy settings, see [“Serial Port Redirection Group Policy Settings,”](#) on page 206.

- If your users run the same 3rd-party applications and COM port devices, make sure that the redirected ports are configured in the same way. For example, in a bank or retail store that uses point-of-sale devices, make sure that all COM port devices are connected to the same ports on the client endpoints, and all ports are mapped to the same redirected COM ports on the remote desktops.

Set the **PortSettings** policy setting to map client ports to redirected ports. Select the **Autoconnect** item in **PortSettings** to ensure that the redirected ports are connected at the start of each desktop session. Enable the **Lock Configuration** policy setting to prevent users from changing the port mappings or customizing the port configurations. In this scenario, users never have to connect or disconnect manually and cannot accidentally make a redirected COM port inaccessible to a 3rd-party application.

- If your users are knowledge workers who use a variety of 3rd-party applications and might also use their COM ports locally on their client machines, make sure that users can connect and disconnect from the redirected COM ports.

You might set the **PortSettings** policy setting if the default port mappings are incorrect. You might or might not set the **Autoconnect** item, depending on your users' requirements. Do not enable the **Lock Configuration** policy setting.

- Make sure that your 3rd-party applications open the COM port that is mapped to the remote desktop.
- Make sure that the baud rate that is in use for a device matches the baud rate that the 3rd-party application is attempting to use.
- You can redirect up to five COM ports from a client system to a remote desktop.

Configuring Serial Port Redirection Group Policy Settings

You can configure group policy settings that control the behavior of serial port redirection on your remote desktops. With these policy settings, you can control centrally, from Active Directory, the options that are available in the **Serial COM Redirection for VMware Horizon** menu on users' desktops.

You do not have to configure these policy settings. Serial port redirection works with the default settings that are configured for redirected COM ports on remote desktops and client systems.

These policy settings affect your remote desktops, not the client systems where the physical COM port devices are connected. To configure these settings on your desktops, add the Serial Port Redirection Group Policy Administrative Template (ADM) file in Active Directory.

Add the Serial Port Redirection ADM Template in Active Directory

You can add the policy settings in the serial port redirection ADM file, `vdm_agent_serialport.adm`, to group policy objects (GPOs) in Active Directory and configure the settings in the Group Policy Object Editor.

Prerequisites

- Verify that the Serial Port Redirection setup option is installed on your desktops. The group policy settings have no effect if serial port redirection is not installed. See [“Install Horizon Agent on a Virtual Machine,”](#) on page 26.
- Verify that Active Directory GPOs are created for the serial port redirection group policy settings. The GPOs must be linked to the OU that contains your desktops. See [“Active Directory Group Policy Example,”](#) on page 297.
- Verify that the MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Familiarize yourself with serial port redirection group policy settings. See [“Serial Port Redirection Group Policy Settings,”](#) on page 206.

Procedure

- 1 Download the View 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-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.
- 2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip` file and copy the serial port redirection ADM file, `vdm_agent_serialport.adm`, to your Active Directory server.
- 3 On the Active Directory server, edit the GPO by selecting **Start > Administrative Tools > Group Policy Management**, right-clicking the GPO, and selecting **Edit**.
- 4 In the Group Policy Object Editor, right-click the **Computer Configuration > Administrative Templates** folder and select **Add/Remove Templates**.
- 5 Click **Add**, browse to the `vdm_agent_serialport.adm` file, and click **Open**.
- 6 Click **Close** to apply the policy settings in the ADM file to the GPO.

The settings are located in the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Serial COM** folder.

Most settings are also added to the **User Configuration** folder, located in **User Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Serial COM**.

- 7 Configure the serial port redirection group policy settings.

Serial Port Redirection Group Policy Settings

The serial port redirection group policy settings control the redirected COM port configuration, including the options that are available in the **Serial COM Redirection for VMware Horizon** menu on remote desktops.

The serial port redirection ADM file contains both Computer Configuration and User Configuration policies. The User Configuration policies allow you to set different configurations for specified users of VDI desktops. Policy settings that are configured in Computer Configuration take precedence over the corresponding settings that are configured in User Configuration.

Group Policy Setting	Description
PortSettings	<p>Determines the mapping between the COM port on the client system and the redirected COM port on the remote desktop and determines other settings that affect the redirected COM port.</p> <p>You configure each redirected COM port individually. Five PortSettings policy settings are available, PortSettings1 through PortSettings5, allowing up to five COM ports to be mapped from the client to the remote desktop. Select one PortSettings policy setting for each COM port that you intend to configure.</p> <p>When you enable the PortSettings policy setting, you can configure the following items that affect the redirected COM port:</p> <ul style="list-style-type: none"> ■ The Source port number setting specifies the number of the physical COM port that is connected to the client system. ■ The Destination virtual port number setting specifies the number of the redirected virtual COM port on the remote desktop. ■ The Autoconnect setting automatically connects the COM port to the redirected COM port at the start of each desktop session. ■ With the IgnoreDSR setting, the redirected COM port device ignores the Data Set Ready (DSR) signal. ■ The Pause before close port (in milliseconds) setting specifies the time to wait (in milliseconds) after a user closes the redirected port and before the port is actually closed. Certain USB to Serial adapters require this delay to ensure that transmitted data is preserved. This setting is intended for troubleshooting purposes. ■ The Serial2USBModeChangeEnabled setting resolves issues that apply to USB to Serial adapters that use the Prolific chipset, including the GlobalSat BU353 GPS adapter. If you do not enable this setting for Prolific chipset adapters, connected devices can transmit data but not receive data. ■ The Disable errors in wait mask setting disables the error value in the COM port mask. This troubleshooting setting is required for certain applications. For details, see the Microsoft documentation of the <code>WaitCommEvent</code> function at http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx. ■ The HandleBtDisappear setting supports Bluetooth COM port behavior. This setting is intended for troubleshooting purposes. ■ The UsbToComTroubleshooting setting resolves some issues that apply to USB to Serial port adapters. This setting is intended for troubleshooting purposes. <p>When you enable the PortSettings setting for a particular COM port, users can connect and disconnect the redirected port, but users cannot configure properties of the port on the remote desktop. For example, users cannot set the port to be redirected automatically when they log in to the desktop, and they cannot ignore the DSR signal. These properties are controlled by the group policy setting.</p> <p>NOTE A redirected COM port is connected and active only if the physical COM port is connected locally to the client system. If you map a COM port that does not exist on the client, the redirected port appears as inactive and not available in the tool tray menu on the remote desktop.</p> <p>When the PortSettings setting is disabled or not configured, the redirected COM port uses the settings that users configure on the remote desktop. The Serial COM Redirection for VMware Horizon menu options are active and available to users.</p> <p>This setting is available as a Computer Configuration and User Configuration policy.</p>
Local settings priority	<p>Gives priority to the settings that are configured on the remote desktop.</p> <p>When you enable this policy, the serial port redirection settings that a user configures on the remote desktop take precedence over the group policy settings. A group policy setting takes effect only if a setting is not configured on the remote desktop.</p> <p>When this setting is disabled or not configured, group policy settings take precedence over the settings that are configured on the remote desktop.</p> <p>This setting is available as a Computer Configuration and User Configuration policy.</p>
Disable functionality	<p>Disables the serial port redirection feature.</p> <p>When you enable this setting, COM ports are not redirected to the remote desktop. The serial port tool tray icon on the remote desktop is not displayed.</p> <p>When this setting is disabled, serial port redirection works, the serial port tool tray icon is displayed, and COM ports appear in the Serial COM Redirection for VMware Horizon menu.</p> <p>When this setting is not configured, settings that are local to the remote desktop determine whether serial port redirection is disabled or enabled.</p> <p>This setting is available as a Computer Configuration policy only.</p>

Group Policy Setting	Description
Lock configuration	<p>Locks the serial port redirection user interface and prevents users from changing configuration options on the remote desktop.</p> <p>When you enable this setting, users cannot configure the options that are available from the tool tray menu on their desktops. Users can display the Serial COM Redirection for VMware Horizon menu, but the options are inactive and cannot be changed.</p> <p>When this setting is disabled, users can configure the options in the Serial COM Redirection for VMware Horizon menu.</p> <p>When this setting is not configured, local program settings on the remote desktop determine whether users can configure the COM port redirection settings.</p>
Bandwidth limit	<p>Sets a limit on the data transfer speed, in kilobytes per second, between the redirected serial port and client systems.</p> <p>When you enable this setting, you can set a value in the Bandwidth limit (in kilobytes per second) box that determines the maximum data transfer speed between the redirected serial port and the client. A value of 0 disables the bandwidth limit.</p> <p>When this setting is disabled, no bandwidth limit is set.</p> <p>When this setting is not configured, local program settings on the remote desktop determine whether a bandwidth limit is set.</p> <p>This setting is available as a Computer Configuration policy only.</p>

Configure USB to Serial Adapters

You can configure USB to Serial adapters that use a Prolific chipset to be redirected to remote desktops by the serial port redirection feature.

To ensure that data is transmitted properly on Prolific chipset adapters, you can enable a serial port redirection group policy setting in Active Directory or on an individual desktop virtual machine.

If you do not configure the group policy setting to resolve issues for Prolific chipset adapters, connected devices can transmit data but not receive data.

You do not have to configure a policy setting or registry key on client systems.

Prerequisites

- Verify that the Serial Port Redirection setup option is installed on your desktops. The group policy settings have no effect if serial port redirection is not installed. See [“Install Horizon Agent on a Virtual Machine,”](#) on page 26.
- Verify that the Serial Port Redirection ADM file is added in Active Directory or on the desktop virtual machine. See [“Add the Serial Port Redirection ADM Template in Active Directory,”](#) on page 205.
- Familiarize yourself with the **Serial2USBModeChangeEnabled** item in the **PortSettings** group policy setting. See [“Serial Port Redirection Group Policy Settings,”](#) on page 206.

Procedure

- 1 In Active Directory or on the virtual machine, open the Group Policy Object Editor.
- 2 Navigate to the **Computer Configuration > Policies > Administrative Templates > Classic Administrative Templates > VMware View Agent Configuration > Serial COM** folder.
- 3 Select the **PortSettings** folder.
- 4 Select and enable a **PortSettings** group policy setting.
- 5 Specify the source and destination COM port numbers to map the COM port.
- 6 Select the **Serial2USBModeChangeEnabled** check box.
- 7 Configure other items in the **PortSettings** policy setting as needed.

8 Click **OK** and close the Group Policy Object Editor.

USB to Serial adapters can be redirected to remote desktops, and can receive data successfully, when users start their next desktop sessions.

Managing Access to Windows Media Multimedia Redirection (MMR)

View provides the Windows Media MMR feature for VDI desktops that run on single-user machines and for RDS desktops.

MMR delivers the multimedia stream directly to client computers. With MMR, the multimedia stream is processed, that is, decoded, on the client system. The client system plays the media content, thereby offloading the demand on the ESXi host.

MMR data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.

If the secure tunnel is enabled, MMR connections between Horizon Clients and the View Secure Gateway are secure, but connections from the View Secure Gateway to desktop machines are not encrypted. If the secure tunnel is disabled, MMR connections from Horizon Clients to the desktop machines are not encrypted.

Enabling Multimedia Redirection in View

You can take steps to ensure that MMR is accessible only to Horizon Client systems that have sufficient resources to handle local multimedia decoding and that are connected to View on a secure network.

By default, the global policy in View Administrator, **Multimedia redirection (MMR)** is set to **Deny**.

To use MMR, you must explicitly set this value to **Allow**.

To control access to MMR, you can enable or disable the **Multimedia redirection (MMR)** policy globally, for individual desktop pools, or for specific users.

For instructions for setting global policies in View Administrator, see [“View Policies,”](#) on page 257.

System Requirements for Windows Media MMR

To support Windows Media Multimedia Redirection (MMR), your View deployment must meet certain software and hardware requirements. Windows Media MMR is provided in Horizon 6.0.2 and later releases.

View remote desktop

- This feature is supported on VDI desktops that are deployed on single-user virtual machines and on RDS desktops.

View Agent 6.1.1 or later is required to support this feature on RDS desktops.

View Agent 6.0.2 or later is required to support this feature on single-user machines.

- The following guest operating systems are supported:
 - 64-bit or 32-bit Windows 7 SP1 Enterprise or Ultimate (single-user machine). Windows 7 Professional is not supported.
 - 64-bit or 32-bit Windows 8/8.1 Professional or Enterprise (single-user machine)
 - Windows Server 2008 R2 configured as an RDS host
 - Windows Server 2012 and 2012 R2 configured as an RDS host

- **3D Rendering** can be enabled or disabled on the desktop pool.
- Users must play videos on Windows Media Player 12 or later or in Internet Explorer 8 or later.

To use Internet Explorer, you must disable Protected Mode. In the Internet Options dialog box, click the **Security** tab and deselect **Enable Protected Mode**.

Horizon Client software Horizon Client 3.2 for Windows or a later release is required to support Windows Media MMR on single-user machines.

Horizon Client computer or client access device ■ The clients must run 64-bit or 32-bit Windows 7 or Windows 8/8.1 operating systems.

Supported media formats Media formats that are supported on Windows Media Player are supported. For example: M4V; MOV; MP4; WMP; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3; WAV.

NOTE DRM-protected content is not redirected through Windows Media MMR.

View policies In View Administrator, set the **Multimedia redirection (MMR)** policy to **Allow**. The default value is **Deny**.

Back-end firewall If your View deployment includes a back-end firewall between your DMZ-based security servers and your internal network, verify that the back-end firewall allows traffic to port 9427 on your desktops.

Determine Whether to Use Windows Media MMR Based on Network Latency

By default, Windows Media MMR adapts to network conditions on single-user desktops that run on Windows 8 or later and RDS desktops that run on Windows Server 2012 or 2012 R2 or later. If the network latency between Horizon Client and the remote desktop is 29 milliseconds or lower, the video is redirected with Windows Media MMR. If the network latency is 30 milliseconds or higher, the video is not redirected. Instead, it is rendered on the ESXi host and sent to the client over PCoIP.

This feature applies to Windows 8 or later single-user desktops and Windows Server 2012 or 2012 R2 or later RDS desktops. Users can run any supported client system, Windows 7 or Windows 8/8.1.

This feature does not apply to Windows 7 single-user desktops or Windows Server 2008 R2 RDS desktops. On these guest operating systems, Windows Media MMR always performs multimedia redirection, regardless of network latency.

You can override this feature, forcing Windows Media MMR to perform multimedia redirection regardless of the network latency, by configuring the `RedirectionPolicy` registry setting on the desktop.

Procedure

- 1 Start the Windows Registry Editor on the remote desktop.
- 2 Navigate to the Windows registry key that controls the redirection policy.

Option	Description
64-bit desktop	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware tsmmr
32-bit desktop	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr

- 3 Set the `RedirectionPolicy` value to `always`.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

- 4 Restart Windows Media Player on the desktop to allow the updated value to take effect.

Managing Access to Client Drive Redirection

When you deploy Horizon Client 3.5 or later and View Agent 6.2 or later or Horizon Agent 7.0 or later with client drive redirection, folders and files are sent across the network with encryption. Client drive redirection connections between clients and the View Secure Gateway and connections from the View Secure Gateway to desktop machines are secure.

With earlier client or agent releases, client drive redirection folders and files are sent across the network without encryption and might contain sensitive data, depending on the content being redirected.

If the secure tunnel is enabled, client drive redirection connections between Horizon Client and the View Secure Gateway are secure, but connections from the View Secure Gateway to desktop machines are not encrypted. If the secure tunnel is disabled, client drive redirection connections from Horizon Client to the desktop machines are not encrypted.

To ensure that this data cannot be monitored on the network, use client drive redirection only on a secure network if Horizon Client is earlier than version 3.5 or agent is earlier than version 6.2.

The **Client Drive Redirection** setup option in the agent installer is selected by default. As a best practice, enable the **Client Drive Redirection** setup option only in desktop pools where users require this feature.

Use Group Policy to Disable Client Drive Redirection

You can disable client drive redirection by configuring a Microsoft Remote Desktop Services group policy setting for remote desktops and RDS hosts in Active Directory.

For more information about client drive redirection, see the *Using VMware Horizon Client* document for the specific type of desktop client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

NOTE This setting overrides local registry and Smart Policies settings that enable the client drive redirection feature.

Prerequisites

If your View deployment includes a back-end firewall between your DMZ-based security servers and your internal network, verify that the back-end firewall allows traffic to port 9427 on your single-user and RDS desktops. TCP connections on port 9427 are required to support client drive redirection.

Procedure

- 1 In the Group Policy Editor, go to **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection**.

This navigation path is for Active Directory on Windows Server 2012. The navigation path differs on other Windows operating systems.

- 2 Enable the **Do not allow drive redirection** group policy setting.

Use Registry Settings to Configure Client Drive Redirection

You can use Windows registry key settings to control client drive redirection behavior on a remote desktop. This feature requires Horizon Agent 7.0 or later and Horizon Client 4.0 or later.

The Windows registry settings that control client drive redirection behavior on a remote desktop are located in the following path:

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

You can use the Windows Registry Editor on the remote desktop to edit local registry settings.

NOTE Client drive redirection policies set with Smart Policies take precedence over local registry settings.

Disabling Client Drive Redirection

To disable client drive redirection, create a new string value named `disabled` and set its value to `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

The value is `false` (enabled) by default.

Preventing Write Access to Shared Folders

To prevent write access to all folders that are shared with the remote desktop, create a new string value named `permissions` and set its value to any string that begins with `r`, except for `rw`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

The value is `rw` (all shared folders are readable and writeable) by default.

Sharing Specific Folders

To share specific folders with the remote desktop, create a new key named `default shares` and create a new subkey for each folder to share with the remote desktop. For each subkey, create a new string value named `name` and set its value to the path of the folder to share. The following example shares the folders `C:\ebooks` and `C:\spreadsheets`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

If you set `name` to `*all`, all client drives are shared with the remote desktop. The `*all` setting is supported only on Windows client systems.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

To prevent the client from sharing additional folders (that is, folders that are not specified with the `default shares` key), create a string value named `ForcedByAdmin` and set its value to `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

When the value is `true`, the Sharing dialog box does not appear when users connect to the remote desktop in Horizon Client. The value is `false` (clients can share additional folders) by default.

The following example shares the folders `C:\ebooks` and `C:\spreadsheets`, makes both folders read-only, and prevents the client from sharing additional folders.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Using USB Devices with Remote Desktops and Applications

15

Administrators can configure the ability to use USB devices, such as thumb flash drives, cameras, VoIP (voice-over-IP) devices, and printers, from a remote desktop. This feature is called USB redirection, and it supports using the Blast Extreme, PCoIP, or Microsoft RDP display protocol. A remote desktop can accommodate up to 128 USB devices.

You can also redirect locally connected USB thumb flash drives and hard disks for use in RDS desktops and applications. Other types of USB devices, including other types of storage devices, are not supported in RDS desktops and applications.

When you use this feature in desktop pools that are deployed on single-user machines, most USB devices that are attached to the local client system become available in the remote desktop. You can even connect to and manage an iPad from a remote desktop. For example, you can sync your iPad with iTunes installed in your remote desktop. On some client devices, such as Windows and Mac OS X computers, the USB devices are listed in a menu in Horizon Client. You use the menu to connect and disconnect the devices.

In most cases, you cannot use a USB device in your client system and in your remote desktop or application at the same time. Only a few types of USB devices can be shared between a remote desktop and the local computer. These devices include smart card readers and human interface devices such as keyboards and pointing devices.

Administrators can specify which types of USB devices end users are allowed to connect to. For composite devices that contain multiple types of devices, such as a video input device and a storage device, on some client systems, administrators can split the device so that one device (for example, the video input device) is allowed but the other device (for example, the storage device) is not.

The USB redirection feature is available only on some types of clients. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the "Using VMware Horizon Client" document for the specific type of desktop or mobile client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

IMPORTANT When you deploy the USB redirection feature, you can take steps to protect your organization from the security vulnerabilities that can affect USB devices. See ["Deploying USB Devices in a Secure View Environment,"](#) on page 217.

This chapter includes the following topics:

- ["Limitations Regarding USB Device Types,"](#) on page 214
- ["Overview of Setting Up USB Redirection,"](#) on page 215
- ["Network Traffic and USB Redirection,"](#) on page 216
- ["Automatic Connections to USB Devices,"](#) on page 216
- ["Deploying USB Devices in a Secure View Environment,"](#) on page 217

- [“Using Log Files for Troubleshooting and to Determine USB Device IDs,”](#) on page 219
- [“Using Policies to Control USB Redirection,”](#) on page 220
- [“Troubleshooting USB Redirection Problems,”](#) on page 230

Limitations Regarding USB Device Types

Although View does not explicitly prevent any devices from working in a remote desktop, due to factors such as network latency and bandwidth, some devices work better than others. By default, some devices are automatically filtered, or blocked, from being used.

In Horizon 6.0.1, together with Horizon Client 3.1 or later, you can plug USB 3.0 devices into USB 3.0 ports on the client machine, on Windows, Linux, and Mac OS X clients. USB 3.0 devices are supported only with a single stream. Because multiple stream support is not implemented in this release, USB device performance is not enhanced. Some USB 3.0 devices that require a constant high throughput to function correctly might not work in a VDI session, due to network latency.

In earlier View releases, although super-speed USB 3.0 devices are not supported, USB 3.0 devices do often work when plugged into a USB 2.0 port on the client machine. However, there might be exceptions, depending on the type of USB chipset on the motherboard of the client system.

The following types of devices might not be suitable for USB redirection to a remote desktop that is deployed on a single-user machine:

- Due to the bandwidth requirements of webcams, which typically consume more than 60 Mbps of bandwidth, webcams are not supported through USB redirection. For webcams, you can use the Real-Time Audio-Video feature.
- 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. If you have the Real-Time Audio-Video feature, audio input and output devices will work well using that feature, and you do not need to use USB redirection for those devices.
- USB CD/DVD burning is not supported.
- Performance of some USB devices varies greatly, depending on the network latency and reliability, especially over a WAN. For example, a single USB storage device read-request requires three round-trips between the client and the remote desktop. A read of a complete file might require multiple USB read operations, and the larger the latency, the longer the round-trip will take.

The file structure can be very large, depending on the format. Large USB disk drives can take several minutes to appear in the desktop. Formatting a USB device as NTFS rather than FAT helps to decrease the initial connection time. An unreliable network link causes retries, and performance is further reduced.

Similarly, USB CD/DVD readers, as well as scanners and touch devices such as signature tablets, do not work well over a latent network such as a WAN.

- The redirection of USB scanners depends on the state of the network, and scans might take longer than normal to complete.

You can redirect the following types of devices to an RDS desktop or application:

- USB thumb flash drives
- USB hard disks

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.

Overview of Setting Up USB Redirection

To set up your deployment so that end users can connect removable devices, such as USB flash drives, cameras, and headsets, you must install certain components on both the remote desktop or RDS host and the client device, and you must verify that the global setting for USB devices is enabled in View Administrator.

This checklist includes both required and optional tasks for setting up USB redirection in your enterprise.

The USB redirection feature is available only on some types of clients, such as Windows, Mac OS X, and partner-supplied Linux clients. To find out whether this feature is supported on a particular type of client, see the feature support matrix included in the "Using VMware Horizon Client" document for the specific type of client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

IMPORTANT When you deploy the USB redirection feature, you can take steps to protect your organization from the security vulnerabilities that can affect USB devices. For example, you can use group policy settings to disable USB redirection for some remote desktops and users, or to restrict which types of USB devices can be redirected. See ["Deploying USB Devices in a Secure View Environment,"](#) on page 217.

- 1 When you run the Horizon Agent installation wizard on the remote desktop source or RDS host, be sure to include the USB Redirection component.

This component is deselected by default. You must select the component to install it.

- 2 When you run the VMware Horizon Client installation wizard on the client system, be sure to include the USB Redirection component.

This component is included by default.

- 3 Verify that access to USB devices from a remote desktop or application is enabled in View Administrator.

In View Administrator, go to **Policies > Global Policies** and verify that **USB access** is set to **Allow**.

- 4 (Optional) Configure Horizon Agent group policies to specify which types of devices are allowed to be redirected.

See ["Using Policies to Control USB Redirection,"](#) on page 220.

- 5 (Optional) Configure similar settings on the client device.

You can also configure whether devices are automatically connected when Horizon Client connects to the remote desktop or application, or when the end user plugs in a USB device. The method of configuring USB settings on the client device depends on the type of device. For example, for Windows client endpoints, you can configure group policies, whereas for Mac OS X endpoints, you use a command-line command. For instructions, see the "Using VMware Horizon Client" document for the specific type of client device.

- 6 Have end users connect to a remote desktop or application and plug their USB devices into the local client system.

If the driver for the USB device is not already installed in the remote desktop or RDS host, the guest operating system detects the USB device and searches for a suitable driver, just as it would on a physical Windows computer.

Network Traffic and USB Redirection

USB redirection works independently of the display protocol (RDP or PCoIP) and USB traffic usually uses TCP port 32111.

Network traffic between a client system and a remote desktop or application can travel various routes, depending on whether the client system is inside the corporate network and how the administrator has chosen to set up security.

- 1 If the client system is inside the corporate network, so that a direct connection can be made between the client and desktop or application, USB traffic uses TCP port 32111.
- 2 If the client system is outside the corporate network, the client can connect through a View security server.

A security server resides within a DMZ and acts as a proxy host for connections inside your trusted network. This design provides an additional layer of security by shielding the View Connection Server instance from the public-facing Internet and by forcing all unprotected session requests through the security server.

A DMZ-based security server deployment requires a few ports to be opened on the firewall to allow clients to connect with security servers inside the DMZ. You must also configure ports for communication between security servers and the View Connection Server instances in the internal network.

For information on specific ports, see "Firewall Rules for DMZ-Based Security Servers" in the *View Architecture Planning Guide*.

- 3 If the client system is outside the corporate network, you can use View Administrator to enable the HTTPS Secure Tunnel. The client then makes a further HTTPS connection to the View Connection Server or security server host when users connect to a remote desktop or application. The connection is tunneled using HTTPS port 443 to the security server, and then the onward connection for USB traffic from the server to the remote desktop or application uses TCP port 32111. USB device performance is slightly degraded when using this tunnel.

NOTE If you are using a zero client, USB traffic is redirected using a PCoIP virtual channel, rather than through TCP 32111. Data is encapsulated and encrypted by the PCoIP Secure Gateway using TCP/UDP port 4172. If you are using only zero clients, it is not necessary to open TCP port 32111.

Automatic Connections to USB Devices

On some client systems, administrators, end users, or both can configure automatic connections of USB devices to a remote desktop. Automatic connections can be made either when the user plugs a USB device in to the client system or when the client connects to the remote desktop.

Some devices, such as smart phones and tablets, require automatic connections because these devices are restarted, and therefore disconnected, during an upgrade. If these devices are not set to automatically reconnect to the remote desktop, during an upgrade, after the devices restart, they connect to the local client system instead.

Configuration properties for automatic USB connections that administrators set on the client, or that end users set by using a Horizon Client menu item, apply to all USB devices unless the devices are configured to be excluded from USB redirection. For example, in some client versions, webcams and microphones are excluded from USB redirection by default because these devices work better through the Real-Time Audio-

Video feature. In some cases, a USB device might not be excluded from redirection by default but might require administrators to explicitly exclude the device from redirection. For example, the following types of USB devices are not good candidates for USB redirection and must not be automatically connected to a remote desktop:

- USB Ethernet devices. If you redirect a USB Ethernet device, your client system might lose network connectivity if that device is the only Ethernet device.
- Touch screen devices. If you redirect a touch screen device, the remote desktop will receive touch input but not keyboard input.

If you have set the remote desktop to autoconnect USB devices, you can configure a policy to exclude specific devices such as touch screens and network devices. For more information, see [“Configuring Filter Policy Settings for USB Devices,”](#) on page 223.

On Windows clients, as an alternative to using settings that automatically connect all but excluded devices, you can edit a configuration file on the client that sets Horizon Client to reconnect only a specific device or devices, such as smart phones and tablets, to the remote desktop. For instructions, see *Using VMware Horizon Client for Windows*.

Deploying USB Devices in a Secure View Environment

USB devices can be vulnerable to a security threat called BadUSB, in which the firmware on some USB devices can be hijacked and replaced with malware. For example, a device can be made to redirect network traffic or to emulate a keyboard and capture keystrokes. You can configure the USB redirection feature to protect your View deployment against this security vulnerability.

By disabling USB redirection, you can prevent any USB devices from being redirected to your users' View desktops and applications. Alternatively, you can disable redirection of specific USB devices, allowing users to have access only to specific devices on their desktops and applications.

The decision whether to take these steps depends on the security requirements in your organization. These steps are not mandatory. You can install USB redirection and leave the feature enabled for all USB devices in your View deployment. At a minimum, consider seriously the extent to which your organization should try to limit its exposure to this security vulnerability.

Disabling USB Redirection for All Types of Devices

Some highly secure environments require you to prevent all USB devices that users might have connected to their client devices from being redirected to their remote desktops and applications. You can disable USB redirection for all desktop pools, for specific desktop pools, or for specific users in a desktop pool.

Use any of the following strategies, as appropriate for your situation:

- When you install Horizon Agent on a desktop image or RDS host, deselect the **USB redirection** setup option. (The option is deselected by default.) This approach prevents access to USB devices on all remote desktops and applications that are deployed from the desktop image or RDS host.
- In View Administrator, edit the **USB access** policy for a specific pool to either deny or allow access. With this approach, you do not have to change the desktop image and can control access to USB devices in specific desktop and application pools.

Only the global **USB access** policy is available for RDS desktop and application pools. You cannot set this policy for individual RDS desktop or application pools.

- In View Administrator, after you set the policy at the desktop or application pool level, you can override the policy for a specific user in the pool by selecting the **User Overrides** setting and selecting a user.
- Set the Exclude All Devices policy to **true**, on the Horizon Agent side or on the client side, as appropriate.

- Use Smart Policies to create a policy that disables the **USB redirection** Horizon Policy setting. With this approach, you can disable USB redirection on a specific remote desktop if certain conditions are met. For example, you can configure a policy that disables USB redirection when users connect to a remote desktop from outside your corporate network.

If you set the `Exclude All Devices` policy to **true**, Horizon Client prevents all USB devices from being redirected. You can use other policy settings to allow specific devices or families of devices to be redirected. If you set the policy to **false**, Horizon Client allows all USB devices to be redirected except those that are blocked by other policy settings. You can set the policy on both Horizon Agent and Horizon Client. The following table shows how the `Exclude All Devices` policy that you can set for Horizon Agent and Horizon Client combine to produce an effective policy for the client computer. By default, all USB devices are allowed to be redirected unless otherwise blocked.

Table 15-1. Effect of Combining Exclude All Devices Policies

Exclude All Devices Policy on Horizon Agent	Exclude All Devices Policy on Horizon Client	Combined Effective Exclude All Devices Policy
false or not defined (include all USB devices)	false or not defined (include all USB devices)	Include all USB devices
false (include all USB devices)	true (exclude all USB devices)	Exclude all USB devices
true (exclude all USB devices)	Any or not defined	Exclude all USB devices

If you have set `Disable Remote Configuration Download` policy to **true**, the value of `Exclude All Devices` on Horizon Agent is not passed to Horizon Client, but Horizon Agent and Horizon Client enforce the local value of `Exclude All Devices`.

These policies are included in the Horizon Agent Configuration ADM template file (`vdm_agent.adm`). For more information, see [“USB Settings in the Horizon Agent Configuration ADM Template,”](#) on page 227.

Disabling USB Redirection for Specific Devices

Some users might have to redirect specific locally-connected USB devices so that they can perform tasks on their remote desktops or applications. For example, a doctor might have to use a Dictaphone USB device to record patients' medical information. In these cases, you cannot disable access to all USB devices. You can use group policy settings to enable or disable USB redirection for specific devices.

Before you enable USB redirection for specific devices, make sure that you trust the physical devices that are connected to client machines in your enterprise. Be sure that you can trust your supply chain. If possible, keep track of a chain of custody for the USB devices.

In addition, educate your employees to ensure that they do not connect devices from unknown sources. If possible, restrict the devices in your environment to those that accept only signed firmware updates, are FIPS 140-2 Level 3-certified, and do not support any kind of field-updatable firmware. These types of USB devices are hard to source and, depending on your device requirements, might be impossible to find. These choices might not be practical, but they are worth considering.

Each USB device has its own vendor and product ID that identifies it to the computer. By configuring Horizon Agent Configuration group policy settings, you can set an include policy for known device types. With this approach, you remove the risk of allowing unknown devices to be inserted into your environment.

For example, you can prevent all devices except a known device vendor and product ID, `vid/pid=0123/abcd`, from being redirected to the remote desktop or application:

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

NOTE This example configuration provides protection, but a compromised device can report any `vid/pid`, so a possible attack could still occur.

By default, View blocks certain device families from being redirected to the remote desktop or application. For example, HID (human interface devices) and keyboards are blocked from appearing in the guest. Some released BadUSB code targets USB keyboard devices.

You can prevent specific device families from being redirected to the remote desktop or application. For example, you can block all video, audio, and mass storage devices:

```
ExcludeDeviceFamily o:video;audio;storage
```

Conversely, you can create a whitelist by preventing all devices from being redirected but allowing a specific device family to be used. For example, you can block all devices except storage devices:

```
ExcludeAllDevices Enabled
```

```
IncludeDeviceFamily o:storage
```

Another risk can arise when a remote user logs into a desktop or application and infects it. You can prevent USB access to any View connections that originate from outside the company firewall. The USB device can be used internally but not externally.

Be aware that if you block TCP port 32111 to disable external access to USB devices, time zone synchronization will not work because port 32111 is also used for time zone synchronization. For zero clients, the USB traffic is embedded inside a virtual channel on UDP port 4172. Because port 4172 is used for the display protocol as well as for USB redirection, you cannot block port 4172. If required, you can disable USB redirection on zero clients. For details, see the zero client product literature or contact the zero client vendor.

Setting policies to block certain device families or specific devices can help to mitigate the risk of being infected with BadUSB malware. These policies do not mitigate all risk, but they can be an effective part of an overall security strategy.

Using Log Files for Troubleshooting and to Determine USB Device IDs

Useful log files for USB are located on both the client system and the remote desktop operating system or RDS host. Use the log files in both locations for troubleshooting. To find product IDs for specific devices, use the client-side logs.

If you are trying to configure USB device splitting or filtering, or if you are trying to determine why a particular device does not appear in a Horizon Client menu, look in the client-side logs. Client logs are produced for the USB arbitrator and the Horizon View USB Service. Logging on Windows and Linux clients is enabled by default. On Mac OS X clients, logging is disabled by default. To enable logging on Mac OS X clients, see *Using VMware Horizon Client for Mac OS X*.

When you configure policies for splitting and filtering out USB devices, some values you set require the VID (vendor ID) and PID (product ID) for the USB device. To find the VID and PID, you can search on the Internet for the product name combined with `vid` and `pid`. Alternatively, you can look in the client-side log file after you plug in the USB device to the local system when Horizon Client is running. The following table shows the default location of the log files.

Table 15-2. Log File Locations

Client or Agent	Path to Log Files
Windows client	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt

Table 15-2. Log File Locations (Continued)

Client or Agent	Path to Log Files
Mac OS X client	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Linux client	(Default location) /tmp/vmware-root/vmware-view-usbd-*.log

If a problem with the device occurs after the device is redirected to the remote desktop or application, examine both the client- and agent-side logs.

Using Policies to Control USB Redirection

You can configure USB policies for both the remote desktop or application (Horizon Agent) and Horizon Client. These policies specify whether the client device should split composite USB devices into separate components for redirection. You can split devices to restrict the types of USB devices that the client makes available for redirection, and to make Horizon Agent prevent certain USB devices from being forwarded from a client computer.

If you have older versions of Horizon Agent or Horizon Client installed, not all the features of the USB redirection policies are available. [Table 15-3](#) shows how View applies the policies for different combinations of Horizon Agent and Horizon Client.

Table 15-3. Compatibility of USB Policy Settings

Horizon Agent Version	Horizon Client Version	Effect of USB Policy Settings on USB Redirection
5.1 or later	5.1 or later	USB policy settings are applicable to both Horizon Agent and Horizon Client. You can use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. Horizon Agent can send device splitting and filtering policy settings to Horizon Client. You can use Horizon Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop. NOTE In View Agent 6.1 or later and Horizon Client 3.3 or later, these USB redirection policy settings apply to RDS desktops and applications as well as to remote desktops that run on single-user machines.
5.1 or later	5.0.x or earlier	USB policy settings apply only to Horizon Agent. You can use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. You cannot use Horizon Client USB policy settings to control which devices can be redirected from a client computer to a desktop. Horizon Client cannot receive device splitting and filtering policy settings from Horizon Agent. Existing registry settings for USB redirection by Horizon Client remain valid.
5.0.x or earlier	5.1 or later	USB policy settings apply only to Horizon Client. You can use Horizon Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop. You cannot use Horizon Agent USB policy settings to block USB devices from being forwarded to a desktop. Horizon Agent cannot send device splitting and filtering policy settings to Horizon Client.
5.0.x or earlier	5.0.x or earlier	USB policy settings do not apply. Existing registry settings for USB redirection by Horizon Client remain valid.

If you upgrade Horizon Client, any existing registry settings for USB redirection, such as `HardwareIdFilters`, remain valid until you define USB policies for Horizon Client.

On client devices that do not support client-side USB policies, you can use the USB policies for Horizon Agent to control which USB devices are allowed to be forwarded from the client to a desktop or application.

Configuring Device Splitting Policy Settings for Composite USB Devices

Composite USB devices consist of a combination of two or more different devices, such as a video input device and a storage device or a microphone and a mouse device. If you want to allow one or more of the components to be available for redirection, you can split the composite device into its component interfaces, exclude certain interfaces from redirection and include others.

You can set a policy that automatically splits composite devices. If automatic device splitting does not work for a specific device, or if automatic splitting does not produce the results your application requires, you can split composite devices manually.

Automatic Device Splitting

If you enable automatic device splitting View attempts to split the functions, or devices, in a composite device according to the filter rules that are in effect. For example, a dictation microphone might be split automatically so that the mouse device remains local to the client, but the rest of the devices are forwarded to the remote desktop.

The following table shows how the value of the `Allow Auto Device Splitting` setting determines whether Horizon Client attempts to split composite USB devices automatically. By default, automatic splitting is disabled.

Table 15-4. Effect of Combining Disable Automatic Splitting Policies

Allow Auto Device Splitting Policy on Horizon Agent	Allow Auto Device Splitting Policy on Horizon Client	Combined Effective Allow Auto Device Splitting Policy
Allow – Default Client Setting	false (automatic splitting disabled)	Automatic splitting disabled
Allow – Default Client Setting	true (automatic splitting enabled)	Automatic splitting enabled
Allow – Default Client Setting	Not defined	Automatic splitting enabled
Allow – Override Client Setting	Any or not defined	Automatic splitting enabled
Not defined	Not defined	Automatic splitting disabled

NOTE These policies are included in the Horizon Agent Configuration ADM template file (`vdm_agent.adm`). For more information, see [“USB Settings in the Horizon Agent Configuration ADM Template,”](#) on page 227.

By default, View disables automatic splitting, and excludes any audio-output, keyboard, mouse, or smart-card components of a composite USB device from redirection.

View applies the device splitting policy settings before it applies any filter policy settings. If you have enabled automatic splitting and do not explicitly exclude a composite USB device from being split by specifying its vendor and product IDs, View examines each interface of the composite USB device to decide which interfaces should be excluded or included according to the filter policy settings. If you have disabled automatic device splitting and do not explicitly specify the vendor and product IDs of a composite USB device that you want to split, View applies the filter policy settings to the entire device.

If you enable automatic splitting, you can use the `Exclude Vid/Pid Device From Split` policy to specify the composite USB devices that you want to exclude from splitting.

Manual Device Splitting

You can use the `Split Vid/Pid Device` policy to specify the vendor and product IDs of a composite USB device that you want to split. You can also specify the interfaces of the components of a composite USB device that you want to exclude from redirection. View does not apply any filter policy settings to components that you exclude in this way.

IMPORTANT If you use the `Split Vid/Pid Device` policy, View does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as `Include Vid/Pid Device` to include those components.

[Table 15-5](#) shows the modifiers that specify how Horizon Client handles a Horizon Agent device splitting policy setting if there is an equivalent device splitting policy setting for Horizon Client. These modifiers apply to all device-splitting policy settings.

Table 15-5. Splitting Modifiers for Device-Splitting Policy Settings on Horizon Agent

Modifier	Description
<code>m</code> (merge)	Horizon Client applies the Horizon Agent device splitting policy setting in addition to the Horizon Client device splitting policy setting.
<code>o</code> (override)	Horizon Client uses the Horizon Agent device splitting policy setting instead of the Horizon Client device splitting policy setting.

[Table 15-6](#) shows examples of how Horizon Client processes the settings for `Exclude Device From Split by Vendor/Product ID` when you specify different splitting modifiers.

Table 15-6. Examples of Applying Splitting Modifiers to Device-Splitting Policy Settings

Exclude Device From Split by Vendor/Product ID on Horizon Agent	Exclude Device From Split by Vendor/Product ID on Horizon Client	Effective Exclude Device From Split by Vendor/Product ID Policy Setting Used by Horizon Client
<code>m:vid-XXXX_pid-XXXX</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>
<code>o:vid-XXXX_pid-XXXX</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX</code>
<code>m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>
<code>o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>	<code>vid-YYYY_pid-YYYY</code>	<code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code>

Horizon Agent does not apply the device splitting policy settings on its side of the connection.

Horizon Client evaluates the device splitting policy settings in the following order of precedence.

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

A device splitting policy setting that excludes a device from being split takes precedence over any policy setting to split the device. If you define any interfaces or devices to be excluded from splitting, Horizon Client excludes the matching component devices from being available for redirection.

Examples of Setting Policies to Split Composite USB Devices

Set splitting policies for desktops to exclude devices with specific vendor and product IDs from redirection after automatic splitting and pass these policies to client computers:

- For Horizon Agent, set the `Allow Auto Device Splitting` policy to `Allow - Override Client Setting`.

- For Horizon Agent, set the Exclude VidPid From Split policy to **o:vid-xxx_pid-yyyy**, where *xxx* and *yyyy* are the appropriate IDs.

Allow automatic device splitting for desktops and specify policies for splitting specific devices on client computers:

- For Horizon Agent, set the Allow Auto Device Splitting policy to Allow – Override Client Setting.
- For the client device, set the Include Vid/Pid Device filter policy to include the specific device that you want to split; for example, **vid-0781_pid-554c**.
- For the client device, set the Split Vid/Pid Device policy to **vid-0781_pid-554c(exintf:00;exintf:01)** for example, to split a specified composite USB device so that interface 00 and interface 01 are excluded from redirection.

Configuring Filter Policy Settings for USB Devices

Filter policy settings that you configure for Horizon Agent and Horizon Client establish which USB devices can be redirected from a client computer to a remote desktop or application. USB device filtering is often used by companies to disable the use of mass storage devices on remote desktops, or to block a specific type of device from being forwarded, such as a USB-to-Ethernet adapter that connects the client device to the remote desktop.

When you connect to a desktop or application, Horizon Client downloads the Horizon Agent USB policy settings and uses them in conjunction with the Horizon Client USB policy settings to decide which USB devices it will allow you to redirect from the client computer.

View applies any device splitting policy settings before it applies the filter policy settings. If you have split a composite USB device, View examines each of the device's interfaces to decide which should be excluded or included according to the filter policy settings. If you have not split a composite USB device, View applies the filter policy settings to the entire device.

The device splitting policies are included in the Horizon Agent Configuration ADM template file (`vdm_agent.adm`). For more information, see [“USB Settings in the Horizon Agent Configuration ADM Template,”](#) on page 227.

Interaction of Agent-Enforced USB Settings

The following table shows the modifiers that specify how Horizon Client handles a Horizon Agent filter policy setting for an agent-enforceable setting if an equivalent filter policy setting exists for Horizon Client.

Table 15-7. Filter Modifiers for Agent-Enforceable Settings

Modifier	Description
m (merge)	Horizon Client applies the Horizon Agent filter policy setting in addition to the Horizon Client filter policy setting. In the case of Boolean, or true/false, settings, if the client policy is not set, the agent settings are used. If the client policy is set, the agent settings are ignored, except for the Exclude All Devices setting. If the Exclude All Devices policy is set on the agent side, the policy overrides the client setting.
o (override)	Horizon Client uses the Horizon Agent filter policy setting instead of the Horizon Client filter policy setting.

For example, the following policy on the agent side overrides any include rules on the client side, and only device VID-0911_PID-149a will have an include rule applied:

```
IncludeVidPid: o:VID-0911_PID-149a
```

You can also use asterisks as wildcard characters; for example: **o:vid-0911_pid-******

IMPORTANT If you configure the agent side without the **o** or **m** modifier, the configuration rule is considered invalid and will be ignored.

Interaction of Client-Interpreted USB Settings

The following table shows the modifiers that specify how Horizon Client handles a Horizon Agent filter policy setting for a client-interpreted setting.

Table 15-8. Filter Modifiers for Client-Interpreted Settings

Modifier	Description
Default (d in the registry setting)	If a Horizon Client filter policy setting does not exist, Horizon Client uses the Horizon Agent filter policy setting. If a Horizon Client filter policy setting exists, Horizon Client applies that policy setting and ignores the Horizon Agent filter policy setting.
Override (o in the registry setting)	Horizon Client uses the Horizon Agent filter policy setting instead of any equivalent Horizon Client filter policy setting.

Horizon Agent does not apply the filter policy settings for client-interpreted settings on its side of the connection.

The following table shows examples of how Horizon Client processes the settings for Allow Smart Cards when you specify different filter modifiers.

Table 15-9. Examples of Applying Filter Modifiers to Client-Interpreted Settings

Allow Smart Cards Setting on Horizon Agent	Allow Smart Cards Setting on Horizon Client	Effective Allow Smart Cards Policy Setting Used by Horizon Client
Disable – Default Client Setting (d: false in the registry setting)	true (Allow)	true (Allow)
Disable – Override Client Setting (o: false in the registry setting)	true (Allow)	false (Disable)

If you set the Disable Remote Configuration Download policy to **true**, Horizon Client ignores any filter policy settings that it receives from Horizon Agent.

Horizon Agent always applies the filter policy settings in agent-enforceable settings on its side of the connection even if you configure Horizon Client to use a different filter policy setting or disable Horizon Client from downloading filter policy settings from Horizon Agent. Horizon Client does not report that Horizon Agent is blocking a device from being forwarded.

Precedence of Settings

Horizon Client evaluates the filter policy settings according to an order of precedence. A filter policy setting that excludes a matching device from being redirected takes precedence over the equivalent filter policy setting that includes the device. If Horizon Client does not encounter a filter policy setting to exclude a device, Horizon Client allows the device to be redirected unless you have set the Exclude All Devices policy to **true**. However, if you have configured a filter policy setting on Horizon Agent to exclude the device, the desktop or application blocks any attempt to redirect the device to it.

Horizon Client evaluates the filter policy settings in order of precedence, taking into account the Horizon Client settings and the Horizon Agent settings together with the modifier values that you apply to the Horizon Agent settings. The following list shows the order of precedence, with item 1 having the highest precedence.

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device

- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family
- 7 Allow Audio Input Devices, Allow Audio Output Devices, Allow HIDBootable, Allow HID (Non Bootable and Not Mouse Keyboard), Allow Keyboard and Mouse Devices, Allow Smart Cards, and Allow Video Devices
- 8 Combined effective Exclude All Devices policy evaluated to exclude or include all USB devices

You can set Exclude Path and Include Path filter policy settings only for Horizon Client. The Allow filter policy settings that refer to separate device families have equal precedence.

If you configure a policy setting to exclude devices based on vendor and product ID values, Horizon Client excludes a device whose vendor and product ID values match this policy setting even though you might have configured an Allow policy setting for the family to which the device belongs.

The order of precedence for policy settings resolves conflicts between policy settings. If you configure Allow Smart Cards to allow the redirection of smart cards, any higher precedence exclusion policy setting overrides this policy. For example, you might have configured an Exclude Vid/Pid Device policy setting to exclude smart-card devices with matching path or vendor and product ID values, or you might have configured an Exclude Device Family policy setting that also excludes the smart-card device family entirely.

If you have configured any Horizon Agent filter policy settings, Horizon Agent evaluates and enforces the filter policy settings in the following order of precedence on the remote desktop or application, with item 1 having the highest precedence.

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family
- 4 Include Device Family
- 5 Agent-enforced Exclude All Devices policy set to exclude or include all USB devices

Horizon Agent enforces this limited set of filter policy settings on its side of the connection.

By defining filter policy settings for Horizon Agent, you can create a filtering policy for non-managed client computers. The feature also allows you to block devices from being forwarded from client computers, even if the filter policy settings for Horizon Client permit the redirection.

For example, if you configure a policy that permits Horizon Client to allow a device to be redirected, Horizon Agent blocks the device if you configure a policy for Horizon Agent to exclude the device.

Examples of Setting Policies to Filter USB Devices

The vendor IDs and product IDs used in these examples are examples only. For information about determining the vendor ID and product ID for a specify device, see [“Using Log Files for Troubleshooting and to Determine USB Device IDs,”](#) on page 219.

- On the client, exclude a particular device from being redirected:

Exclude Vid/Pid Device: Vid-0341_Pid-1a11

- Block all storage devices from being redirected to this desktop or application pool. Use an agent-side setting:

Exclude Device Family: o:storage

- For all users in a desktop pool, block audio and video devices to ensure that these devices will always be available for the Real-Time Audio-Video feature. Use an agent-side setting::

Exclude Device Family: o:video;audio

Note that another strategy would be to exclude specific devices by vendor and product ID.

- On the client, block all devices from being redirected except one particular device:

Exclude All Devices: true
 Include Vid/Pid Device: Vid-0123_Pid-abcd

- Exclude all devices made by a particular company because these devices cause problems for your end users. Use an agent-side setting:

Exclude Vid/Pid Device: o:Vid-0341_Pid-*

- On the client, include two specific devices but exclude all others:

Exclude All Devices: true
 Include Vid/Pid Device: Vid-0123_Pid-abcd;Vid-1abc_Pid-0001

USB Device Families

You can specify a family when you are creating USB filtering rules for Horizon Client, or View Agent or Horizon Agent.

NOTE Some devices do not report a device family.

Table 15-10. USB Device Families

Device Family Name	Description
audio	Any audio-input or audio-output device.
audio-in	Audio-input devices such as microphones.
audio-out	Audio-output devices such as loudspeakers and headphones.
bluetooth	Bluetooth-connected devices.
comm	Communications devices such as modems and wired networking adapters.
hid	Human interface devices excluding keyboards and pointing devices.
hid-bootable	Human interface devices that are available at boot time excluding keyboards and pointing devices.
imaging	Imaging devices such as scanners.
keyboard	Keyboard device.
mouse	Pointing device such as a mouse.
other	Family not specified.
pda	Personal digital assistants.
physical	Force feedback devices such as force feedback joysticks.
printer	Printing devices.
security	Security devices such as fingerprint readers.
smart-card	Smart-card devices.
storage	Mass storage devices such as flash drives and external hard disk drives.
unknown	Family not known.
vendor	Devices with vendor-specific functions.
video	Video-input devices.

Table 15-10. USB Device Families (Continued)

Device Family Name	Description
wireless	Wireless networking adapters.
wusb	Wireless USB devices.

USB Settings in the Horizon Agent Configuration ADM Template

You can define USB policy settings for both Horizon Agent and Horizon Client. On connection, Horizon Client downloads the USB policy settings from Horizon Agent and uses them in conjunction with the Horizon Client USB policy settings to decide which devices it will allow to be available for redirection from the client computer.

The Horizon Agent Configuration ADM template file (`vdm_agent.adm`) contains policy settings related to the authentication and environmental components of Horizon Agent, including USB redirection. The settings apply at the computer level. Horizon Agent preferentially reads the settings from the GPO at the computer level, and otherwise from the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`

Settings for Configuring USB Device Splitting

The following table describes each policy setting for splitting composite USB devices in the Horizon Agent Configuration ADM template file. Horizon Agent does not enforce these settings. Horizon Agent passes the settings to Horizon Client for interpretation and enforcement according to whether you specify the merge (m) or override (o) modifier. Horizon Client uses the settings to decide whether to split composite USB devices into their component devices, and whether to exclude the component devices from being available for redirection. For a description of how View applies the policies for splitting composite USB devices, see [“Configuring Device Splitting Policy Settings for Composite USB Devices,”](#) on page 221.

Table 15-11. Horizon Agent Configuration Template: Device-Splitting Settings

Setting	Properties
Allow Auto Device Splitting Property: AllowAutoDeviceSplitting	Allows the automatic splitting of composite USB devices. The default value is undefined, which equates to false .
Exclude Vid/Pid Device From Split Property: SplitExcludeVidPid	Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: o:vid-0781_pid-55** The default value is undefined.
Split Vid/Pid Device Property: SplitVidPid	Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is {m o}:vid-xxx_pid-yyy(exintf:zz[;exintf:ww]) or {m o}:vid-xxx_pid-yyy(exintf:zz[;exintf:ww]) You can use the exintf keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (*) in place of individual digits in an ID. For example: o:vid-0781_pid-554c(exintf:01;exintf:02) NOTE View does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as Include Vid/Pid Device to include those components. The default value is undefined.

Horizon Agent -Enforced USB Settings

The following table describes each agent-enforced policy setting for USB in the Horizon Agent Configuration ADM template file. Horizon Agent uses the settings to decide if a USB device can be forwarded to the host machine. Horizon Agent also passes the settings to Horizon Client for interpretation and enforcement according to whether you specify the merge (m) or override (o) modifier. Horizon Client uses the settings to decide if a USB device is available for redirection. As Horizon Agent always enforces an agent-enforced policy setting that you specify, the effect might be to counteract the policy that you have set for Horizon Client. For a description of how View applies the policies for filtering USB devices, see [“Configuring Filter Policy Settings for USB Devices,”](#) on page 223.

Table 15-12. Horizon Agent Configuration Template: Agent-Enforced Settings

Setting	Properties
Exclude All Devices Property: ExcludeAllDevices	Excludes all USB devices from being forwarded. If set to true , you can use other policy settings to allow specific devices or families of devices to be forwarded. If set to false , you can use other policy settings to prevent specific devices or families of devices from being forwarded. If set to true and passed to Horizon Client, this setting always overrides the setting on Horizon Client. You cannot use the merge (m) or override (o) modifier with this setting. The default value is undefined, which equates to false .
Exclude Device Family Property: ExcludeFamily	Excludes families of devices from being forwarded. The format of the setting is {m o}:family_name_1[;family_name_2]... For example: o:bluetooth;smart-card If you have enabled automatic device splitting, View examines the device family of each interface of a composite USB device to decide which interfaces should be excluded. If you have disabled automatic device splitting, View examines the device family of the whole composite USB device. The default value is undefined.
Exclude Vid/Pid Device Property: ExcludeVidPid	Excludes devices with specified vendor and product IDs from being forwarded. The format of the setting is {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: m:vid-0781_pid-****;vid-0561_pid-554c The default value is undefined.
Include Device Family Property: IncludeFamily	Includes families of devices that can be forwarded. The format of the setting is {m o}:family_name_1[;family_name_2]... For example: m:storage The default value is undefined.
Include Vid/Pid Device Property: IncludeVidPid	Includes devices with specified vendor and product IDs that can be forwarded. The format of the setting is {m o}:vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: o:vid-0561_pid-554c The default value is undefined.

Client-Interpreted USB Settings

The following table describes each client-interpreted policy setting in the Horizon Agent Configuration ADM template file. Horizon Agent does not enforce these settings. Horizon Agent passes the settings to Horizon Client for interpretation and enforcement. Horizon Client uses the settings to decide if a USB device is available for redirection.

Table 15-13. Horizon Agent Configuration Template: Client-Interpreted Settings

Setting	Properties
Allow Audio Input Devices Property: AllowAudioIn	Allows audio input devices to be forwarded. The default value is undefined, which equates to true .
Allow Audio Output Devices Property: AllowAudioOut	Allows audio output devices to be forwarded. The default value is undefined, which equates to false .
Allow HIDBootable Property: AllowHIDBootable	Allows input devices other than keyboards or mice that are available at boot time (also known as hid-bootable devices) to be forwarded. The default value is undefined, which equates to true .

Table 15-13. Horizon Agent Configuration Template: Client-Interpreted Settings (Continued)

Setting	Properties
Allow Other Input Devices	Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be forwarded. The default value is undefined.
Allow Keyboard and Mouse Devices Property: AllowKeyboardMouse	Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be forwarded. The default value is undefined, which equates to false .
Allow Smart Cards Property: AllowSmartcard	Allows smart-card devices to be forwarded. The default value is undefined, which equates to false .
Allow Video Devices Property: AllowVideo	Allows video devices to be forwarded. The default value is undefined, which equates to true .

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,”](#) on page 221.
- 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,”](#) on page 219.

- 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.

Reducing and Managing Storage Requirements

16

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,”](#) on page 233
- [“Reducing Storage Requirements with Instant Clones,”](#) on page 239
- [“Reducing Storage Requirements with View Composer,”](#) on page 240
- [“Storage Sizing for Instant-Clone and View Composer Linked-Clone Desktop Pools,”](#) on page 241
- [“Storage Overcommit for View Composer Linked-Clone Virtual Machines,”](#) on page 245
- [“View Composer Linked-Clone Data Disks,”](#) on page 247
- [“Storing View Composer Linked Clones on Local Datastores,”](#) on page 248
- [“Storing Replicas and Clones on Separate Datastores for Instant Clones and View Composer Linked Clones,”](#) on page 249
- [“Configure View Storage Accelerator for View Composer Linked Clones,”](#) on page 250
- [“Reclaim Disk Space on View Composer Linked Clones,”](#) on page 251
- [“Using VAAI Storage for View Composer Linked Clones,”](#) on page 253
- [“Set Storage Accelerator and Space Reclamation Blackout Times for View Composer Linked Clones,”](#) on page 254

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 snapshotting, 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 (VAAI) feature because Virtual SAN does not use NAS devices.
- Virtual SAN datastores are not compatible with Virtual Volumes datastores for this release.

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. For more information, see the *vSphere Configuration Maximums* document, available from <https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>.
- 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), REPLICATED_DISK (for replicas), and VM_HOME (for virtual machine files such as .vmx and .vmsn files). For example, a REPLICATED_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. This mapping allows vSphere to offload intensive storage operations such as snapshotting, cloning, and replication to the storage system. The result, for example, is that a cloning operation that previously took an hour might now take just a few minutes using Virtual Volumes.

IMPORTANT Although one of the key benefits of Virtual Volumes is the ability to use Software Policy-Based Management (SPBM), for this release of View, no default granular storage policies are created by View, as they are when you use the Virtual SAN feature. Instead, you can set a global default storage policy in vCenter Server that will apply 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 (VAAI).
- Virtual Volumes datastores are not compatible with Virtual SAN datastores for this release.
- 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 linked 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 16-1](#) 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 16-1. 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 243.

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 246.

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 16-2](#) 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 244.

Table 16-2. 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 16-3 shows how the sizing formulas calculate estimated storage requirements for the sample desktop pool.

Table 16-3. 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 16-4 shows the formulas that calculate the estimated sizes of clone disks when you edit a pool or store replicas on a separate datastore.

Table 16-4. 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 16-5 shows how the sizing formulas calculate estimated storage requirements for the sample pool.

Table 16-5. 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 16-6 shows the storage overcommit levels you can set.

Table 16-6. 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 245. 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	<ol style="list-style-type: none"> a Click Add. b Proceed through the Add Desktop Pool wizard until the vCenter Settings page appears.
Existing desktop pool	<ol style="list-style-type: none"> 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 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.

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 new 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.

You can enable View Storage Accelerator on pools that contain linked clones and pools that contain full virtual machines.

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. Hence, 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. In an existing pool, View Storage Accelerator digest files are not configured for virtual machines until they 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 254.

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 `vmadmin -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 <i>View Upgrades</i> 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 254.

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 Policies for Desktop and Application Pools

17

You can configure policies to control the behavior of desktop and application pools, machines, and users. You use View Administrator to set policies for client sessions. You can use Active Directory group policy settings to control the behavior of Horizon Agent, Horizon Client for Windows, and features that affect single-user machines, RDS hosts, PCoIP, or VMware Blast.

This chapter includes the following topics:

- [“Setting Policies in View Administrator,”](#) on page 255
- [“Using Smart Policies,”](#) on page 257
- [“Using Active Directory Group Policies,”](#) on page 263
- [“Using View Group Policy Administrative Template Files,”](#) on page 264
- [“View ADM and ADMX Template Files,”](#) on page 264
- [“Horizon Agent Configuration ADM Template Settings,”](#) on page 266
- [“PCoIP Policy Settings,”](#) on page 271
- [“VMware Blast Policy Settings,”](#) on page 282
- [“Using Remote Desktop Services Group Policies,”](#) on page 283
- [“Setting Up Location-Based Printing,”](#) on page 292
- [“Active Directory Group Policy Example,”](#) on page 297

Setting Policies in View Administrator

You use View Administrator to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. Policies that affect specific users and desktop pools are called user-level policies and desktop pool-level policies. Policies that affect all sessions and users are called global policies.

User-level policies inherit settings from the equivalent desktop pool-level policy settings. Similarly, desktop pool-level policies inherit settings from the equivalent global policy settings. A desktop pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and desktop pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, you can set a global policy to **Deny** and the equivalent desktop pool-level policy to **Allow**, or vice versa.

NOTE Only global policies are available for RDS desktop and application pools. You cannot set user-level policies or pool-level policies for RDS desktop and application pools.

Configure Global Policy Settings

You can configure global policies to control the behavior of all client sessions users.

Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 257.

Procedure

- 1 In View Administrator, select **Policies > Global Policies**.
- 2 Click **Edit policies** in the **View Policies** pane.
- 3 Click **OK** to save your changes.

Configure Policies for Desktop Pools

You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 257.

Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the ID of the desktop pool and click the **Policies** tab.
The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
- 3 Click **Edit Policies** in the **View Policies** pane.
- 4 Click **OK** to save your changes.

Configure Policies for Users

You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop pool-level policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See [“View Policies,”](#) on page 257.

Procedure

- 1 In View Administrator, select **Catalog > Desktop Pools**.
- 2 Double-click the ID of the desktop pool and click the **Policies** tab.
The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Desktop Pool Policy** column.
- 3 Click **User Overrides** and then click **Add User**.
- 4 To find a user, click **Add**, type the name or description of the user, and then click **Find**.
- 5 Select one or more users from the list, click **OK**, and then click **Next**.
The Add Individual Policy dialog box appears.
- 6 Configure the View policies and click **Finish** to save your changes.

View Policies

You can configure View policies to affect all client sessions, or you can apply them to affect specific desktop pools or users.

[Table 17-1](#) describes each View policy setting.

Table 17-1. View Policies

Policy	Description
Multimedia redirection (MMR)	<p>Determines whether MMR is enabled for client systems.</p> <p>MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on remote desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played.</p> <p>The default value is Deny.</p> <p>If client systems have insufficient resources to handle local multimedia decoding, leave the setting as Deny.</p> <p>Multimedia Redirection (MMR) data is sent across the network without application-based encryption and might contain sensitive data, depending on the content being redirected. To ensure that this data cannot be monitored on the network, use MMR only on a secure network.</p>
USB Access	<p>Determines whether remote desktops can use USB devices connected to the client system.</p> <p>The default value is Allow. To prevent the use of external devices for security reasons, change the setting to Deny.</p>
PCoIP hardware acceleration	<p>Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session.</p> <p>This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the remote desktop.</p> <p>The default value is Allow at Medium priority.</p>

Using Smart Policies

You can use Smart Policies to create policies that control the behavior of the USB redirection, virtual printing, clipboard redirection, client drive redirection, and PCoIP display protocol features on specific remote desktops.

With Smart Policies, you can create policies that take effect only if certain conditions are met. For example, you can configure a policy that disables the client drive redirection feature if a user connects to a remote desktop from outside your corporate network.

Requirements for Smart Policies

To use Smart Policies, your View environment must meet certain requirements.

- You must install Horizon Agent 7.0 or later and VMware User Environment Manager 9.0 or later on the remote desktops that you want to manage with Smart Policies.
- Users must use Horizon Client 4.0 or later to connect to remote desktops that you manage with Smart Policies.

Installing User Environment Manager

To use Smart Policies to control the behavior of remote desktop features on a remote desktop, you must install User Environment Manager 9.0 or later on the remote desktop.

You can download the User Environment Manager installer from the VMware Downloads page. You must install the VMware UEM FlexEngine client component on each remote desktop that you want to manage with User Environment Manager. You can install the User Environment Manager Management Console component on any desktop from which you want to manage the User Environment Manager environment.

For a linked-clone pool, you install User Environment Manager in the parent virtual machine that you use as a base image for the linked clones. For an RDS desktop pool, you install User Environment Manager on the RDS host that provides the RDS desktop sessions.

For User Environment Manager system requirements and complete installation instructions, see the *User Environment Manager Administrator's Guide* document.

Configuring User Environment Manager

You must configure User Environment Manager before you can use it to create policies for remote desktop features.

To configure User Environment Manager, follow the configuration instructions in the *User Environment Manager Administrator's Guide*. The following configuration steps supplement the information in that document.

- When configuring the VMware UEM FlexEngine client component on remote desktops, create FlexEngine logon and logoff scripts. Use the **-HorizonViewMultiSession -r** parameter for the logon script and the **-HorizonViewMultiSession -s** parameter for the logoff script.

NOTE Do not use logon scripts to start other applications on a remote desktop. Additional logon scripts can delay remote desktop logon for up to 10 minutes.

- Enable the user group policy setting `Run logon scripts synchronously` on remote desktops. This setting is located in the folder `User Configuration\Policies\Administrative Templates\System\Scripts`.
- Enable the computer group policy setting `Always wait for the network at computer startup and logon` on remote desktops. This setting is located in the folder `Computer Configuration\Administrative Template\System\Logon`.
- For Windows 8.1 remote desktops, disable the computer group policy setting `Configure Logon Script Delay`. This setting is located in the folder `Computer Configuration\Administrative Templates\System\Group Policy`.
- To ensure that Horizon Policy settings are refreshed when users reconnect to desktop sessions, use the User Environment Manager Management Console to create a triggered task. Set the trigger to **Reconnect session**, set the action to **User Environment refresh**, and select **Horizon Policies** for the refresh.

NOTE If you create the triggered task while a user is logged in to the remote desktop, the user must log off from the desktop for the triggered task to take effect.

Horizon Policy Settings

You control the behavior of remote desktop features in User Environment Manager by creating a Horizon policy.

[Table 17-2](#) describes the settings that you can select when you define a Horizon policy in User Environment Manager.

Table 17-2. Horizon Policy Settings

Setting	Description
USB redirection	Determines whether USB redirection is enabled on the remote desktop. The USB redirection feature allows users to use locally attached USB devices, such as thumb flash drives, cameras, and printers, from the remote desktop.
Printing	Determines whether virtual printing is enabled on the remote desktop. The virtual printing feature allows users to print to a virtual printer or a USB printer that is attached to the client computer from the remote desktop.
Clipboard	Determines the direction in which clipboard redirection is allowed. You can select one of these values: <ul style="list-style-type: none"> ■ Disable. Clipboard redirection is disabled in both directions. ■ Allow all. Clipboard redirection is enabled. Users can copy and paste from the client system to the remote desktop and from the remote desktop to the client system. ■ Allow copy from client to agent. Users can copy and paste only from the client system to the remote desktop. ■ Allow copy from agent to client. Users can copy and paste only from the remote desktop to the client system.
Client drive redirection	Determines whether client drive redirection is enabled on the remote desktop and if shared drives and folders are writeable. You can select one of these values: <ul style="list-style-type: none"> ■ Disable. Client drive redirection is disabled on the remote desktop. ■ Allow all. Client drives and folders are shared with the remote desktop and are readable and writeable. ■ Read-only. Client drives and folders are shared with the remote desktop and are readable, but not writeable. <p>If you do not configure this setting, whether shared drives and folders are writeable depends on local registry settings. For more information, see “Use Registry Settings to Configure Client Drive Redirection,” on page 212.</p>
PCoIP profile	Configures a bandwidth profile for PCoIP sessions on the remote desktop. You can select a predefined bandwidth profile, for example, LAN (10 Mbps or higher) . Selecting a predefined bandwidth profile prevents the agent from attempting to transmit at a higher rate than the link capacity. If you select the default profile, the maximum bandwidth is 90000 kilobits per second. For more information, see “PCoIP Profile Reference,” on page 259.

In general, Horizon policy settings that you configure for remote desktop features in User Environment Manager override any equivalent registry key and group policy settings.

PCoIP Profile Reference

With Smart Policies, you can use the PCoIP profile policy setting to configure a bandwidth profile for PCoIP sessions on remote desktops.

[Table 17-3](#) describes each PCoIP profile.

Table 17-3. PCoIP Profiles

PCoIP Profile	Max Session BW (Kbps)	Min Session BW (Kbps)	Enable BTL	Max Initial Image Quality	Min Image Quality	Max FPS	Max Audio BW (Kbps)	Image Quality Performance
High-speed LAN (20 Mbps)	900000	100	Yes	100	50	60	1600	50
LAN (10 Mbps or higher)	900000	100	Yes	90	50	30	1600	50
Dedicated WAN (5 Mbps, default)	900000	100	No	80	40	30	500	50
Broadband WAN (2 Mbps)	5000	100	No	70	40	20	500	50
Low-speed WAN (1 Mbps)	2000	100	No	70	30	15	200	25
Extremely low-speed connection (up to 500 kbps)	1000	100	No	70	30	5	90	0

Adding Conditions to Horizon Policy Definitions

When you define a Horizon Policy in User Environment Manager, you can add conditions that must be met for the policy to take effect. For example, you can add a condition that disables the client drive redirection feature only if a user connects to the remote desktop from outside your corporate network.

You can add multiple conditions for the same remote desktop feature. For example, you can add one condition that enables local printing if a user is a member of the HR group and another condition that enables local printing if the remote desktop is in the Win7 pool.

For detailed information about adding and editing conditions in the User Environment Manager Management Console, see the *User Environment Manager Administrator's Guide*.

Using the Horizon Client Property Condition

When a user connects or reconnects to a remote desktop, Horizon Client gathers information about the client computer and Connection Server sends that information to the remote desktop. You can add the Horizon Client Property condition to a Horizon Policy definition to control when the policy takes effect based on the information that the remote desktop receives.

NOTE The Horizon Client Property condition is effective only if a user launches the remote desktop with the PCoIP display protocol or the VMware Blast display protocol. If a user launches the remote desktop with the RDP display protocol, the Horizon Client Property condition has no effect.

[Table 17-4](#) describes the predefined properties that you can select from the **Properties** drop-down menu when you use the Horizon Client Property condition. Each predefined property corresponds to a ViewClient_ registry key.

Table 17-4. Predefined Properties for the Horizon Client Property Condition

Property	Corresponding Registry Key	Description
Client location	ViewClient_Broker_GatewayLocation	<p>Specifies the location of the user's client system. Valid values are as follows:</p> <ul style="list-style-type: none"> ■ Internal - the policy takes effect only if a user connects to the remote desktop from inside the corporate network ■ External - the policy takes effect only if a user connects to the remote desktop from outside the corporate network <p>For information about setting the gateway location for a Connection Server or security server host, see the <i>View Administration</i> document.</p> <p>For information about setting the gateway location for an Access Point appliance, see the <i>Deploying and Configuring Access Point</i> document.</p>
Launch tag(s)	ViewClient_Launch_Matched_Tags	<p>Specifies one or more tags. Separate multiple tags with a comma or semicolon. The policy takes effect only if the tag that enabled the remote desktop launch to occur matches one of the specified tags.</p> <p>For information about assigning tags to Connection Server instances and desktop pools, see "Restricting Remote Desktop Access," on page 160.</p>
Pool name	ViewClient_Launch_ID	<p>Specifies a desktop pool ID. The policy takes effect only if the ID of the desktop pool the user selected when launching the remote desktop matches the specified desktop pool ID. For example, if the user selected the Win7 pool and this property is set to Win7, the policy takes effect.</p> <p>NOTE You cannot use this property to specify an application pool.</p>

The **Properties** drop-down menu is also a text box, and you can manually enter any ViewClient_ registry key in the text box. Do not include the ViewClient_ prefix when you enter the registry key. For example, to specify ViewClient_Broker_URL, enter Broker_URL.

You can use the Windows Registry Editor (`regedit.exe`) on the remote desktop to view the ViewClient_ registry keys. Horizon Client writes client computer information to the system registry path `HKEY_CURRENT_USER\Volatile Environment` on remote desktops that are deployed on single-user machines. For remote desktops that are deployed in RDS sessions, Horizon Client writes the client computer information to the system registry path `HKEY_CURRENT_USER\Volatile Environment\x`, where *x* is the session ID on the RDS host.

Using Other Conditions

The User Environment Manager Management Console provides many conditions. The following conditions can be especially useful when creating policies for remote desktop features.

Group Member	You can use this condition to configure the policy to take effect only if a user is a member of a specific group.
Remote Display Protocol	You can use this condition to configure the policy to take effect only if the user selects a particular display protocol. The condition settings include RDP, PCoIP, and Blast.
IP Address	You can use this condition to configure the policy that takes effect only if a user connects from inside or outside the corporate network. Use the condition settings to specify an internal IP address range or an external IP address range.

NOTE You can also use the **Client location** property in the Horizon Client Property condition.

For descriptions of all the available conditions, see the *User Environment Manager Administrator's Guide* document.

Create a Horizon Policy in User Environment Manager

You use the User Environment Manager Management Console to create a Horizon policy in User Environment Manager. When you define a Horizon policy, you can add conditions that must be met for the policy to take effect.

Prerequisites

- Install and configure User Environment Manager. See [“Installing User Environment Manager,”](#) on page 258 and [“Configuring User Environment Manager,”](#) on page 258.
- Become familiar with the Horizon Policy settings. See [“Horizon Policy Settings,”](#) on page 259.
- Become familiar with the conditions that you can add to Horizon Policy definitions. See [“Adding Conditions to Horizon Policy Definitions,”](#) on page 260.

For complete information about using the User Environment Manager Management Console, see the *User Environment Manager Administrator's Guide* document.

Procedure

- 1 In the User Environment Manager Management Console, select the **User Environment** tab and click **Horizon Policies** in the tree view.
Existing Horizon policy definitions, if any, appear in the Horizon Policies pane.
- 2 Right-click **Horizon Policies** and select **Create Horizon Policy definition** to create a new policy.
The Horizon Policy dialog box appears.

- 3 Select the **Settings** tab and define the policy settings.
 - a In the General Settings section, type a name for the policy in the **Name** text box.
For example, if the policy will affect the client drive redirection feature, you might name the policy CDR.
 - b In the Horizon Policy Settings section, select the remote desktop features and settings to include in the policy.
You can select multiple remote desktop features.
- 4 (Optional) To add a condition to the policy, select the **Conditions** tab, click **Add**, and select a condition.
You can add multiple conditions to a policy definition.
- 5 Click **Save** to save the policy.

User Environment Manager processes the Horizon policy each time a user connects or reconnects to the remote desktop.

User Environment Manager processes multiple policies in alphabetical order based on the policy name. Horizon policies appear in alphabetical order in the Horizon Policies pane. If policies conflict, the last policy processed takes precedence. For example, if you have a policy named Sue that enables USB redirection for the user named Sue, and another policy named Pool that disables USB redirection for the desktop pool named Win7, the USB redirection feature is enabled when Sue connects to a remote desktop in the Win7 desktop pool.

Using Active Directory Group Policies

You can use Microsoft Windows Group Policy to optimize and secure remote desktops, control the behavior of View components, and to configure location-based printing.

Group Policy is a feature of Microsoft Windows operating systems that provides centralized management and configuration of computers and remote users in an Active Directory environment.

Group policy settings are contained in entities called group policy objects (GPOs). GPOs are associated with Active Directory objects. You can apply GPOs to View components at a domain-wide level to control various areas of the View environment. After they are applied, GPO settings are stored in the local Windows Registry of the specified component.

You use the Microsoft Windows Group Policy Object Editor to manage group policy settings. The Group Policy Object Editor is a Microsoft Management Console (MMC) snap-in. The MMC is part of the Microsoft Group Policy Management Console (GPMC). See the Microsoft TechNet Web site for information on installing and using the GPMC.

Creating an OU for Remote Desktops

You should create an organizational unit (OU) in Active Directory specifically for your remote desktops.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your remote desktops, create a GPO for your View group policies and link it to the OU that contains your remote desktops.

See the Microsoft Active Directory documentation on the Microsoft TechNet Web site for information on creating OUs and GPOs.

Enabling Loopback Processing for Remote Desktops

By default, a user's policy settings come from the set of GPOs that are applied to the user object in Active Directory. However, in the View environment, GPOs should apply to users based on the computer they log in to.

When you enable loopback processing, a consistent set of policies applies to all users that log in to a particular computer, regardless of their location in Active Directory.

See the Microsoft Active Directory documentation for information on enabling loopback processing.

NOTE Loopback processing is only one approach to handling GPOs in View. You might need to implement a different approach.

Using View Group Policy Administrative Template Files

View provides several component-specific Group Policy Administrative (ADM and ADMX) template files. You can optimize and secure remote desktops and applications by adding the policy settings in these ADM and ADMX template files to a new or existing GPO in Active Directory.

All ADM and ADMX files that provide group policy settings for View are available in a bundled .zip file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. You can download the 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 bundled .zip file.

The View ADM and ADMX template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all remote desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the remote desktop or application they connect to. User Configuration policies override equivalent Computer Configuration policies.

Microsoft Windows applies policies at desktop startup and when users log in.

View ADM and ADMX Template Files

The View ADM and ADMX template files provide group policy settings that let you control and optimize View components.

Table 17-5. View ADM and ADMX Template Files

Template Name	Template File	Description
Horizon Agent Configuration	<code>vdm_agent.adm</code>	Contains policy settings related to the authentication and environmental components of Horizon Agent. See "Horizon Agent Configuration ADM Template Settings," on page 266.
Horizon Client Configuration	<code>vdm_client.adm</code>	Contains policy settings related to Horizon Client for Windows. Clients that connect from outside the View Connection Server host domain are not affected by policies applied to Horizon Client. See the <i>Using VMware Horizon Client for Windows</i> document.

Table 17-5. View ADM and ADMX Template Files (Continued)

Template Name	Template File	Description
VMware Horizon URL Redirection	urlRedirection-enUS.adm	<p>Contains policy settings related to the URL Content Redirection Feature. If you add this template to a GPO for a remote desktop pool or application pool, certain URL links clicked inside the remote desktops or app can be redirected to a Windows-based client and opened in a client-side browser.</p> <p>If you add this template to a client-side GPO, when a user clicks certain URL links in a Windows-based client system, the URL can be opened in a remote desktop or application.</p> <p>See “VMware Horizon URL Content Redirection Template Settings,” on page 180 and see the <i>Using VMware Horizon Client for Windows</i> document.</p>
View Server Configuration	vdm_server.adm	<p>Contains policy settings related to View Connection Server.</p> <p>See the <i>View Administration</i> document.</p>
View Common Configuration	vdm_common.adm	<p>Contains policy settings that are common to all View components.</p> <p>See the <i>View Administration</i> document.</p>
View PCoIP Session Variables	pcoip.adm	<p>Contains policy settings related to the PCoIP display protocol.</p> <p>See “PCoIP Policy Settings,” on page 271.</p>
View PCoIP Client Session Variables	pcoip.client.adm	<p>Contains policy settings related to the PCoIP display protocol that affect Horizon Client for Windows.</p> <p>See the <i>Using VMware Horizon Client for Windows</i> document.</p>
View Persona Management Configuration	ViewPM.adm	<p>Contains policy settings related to View Persona Management.</p> <p>See “View Persona Management Group Policy Settings,” on page 318.</p>
View Remote Desktop Services	vmware_rdsh.admx vmware_rdsh_server.admx	<p>Contains policy settings related to Remote Desktop Services.</p> <p>See “Using Remote Desktop Services Group Policies,” on page 283.</p>
Real-Time Audio-Video Configuration	vdm_agent_rtav.adm	<p>Contains policy settings related to webcams that are used with the Real-Time Audio-Video feature.</p> <p>See “Real-Time Audio-Video Group Policy Settings,” on page 195.</p>
Scanner Redirection	vdm_agent_scanner.adm	<p>Contains policy settings related to scanning devices that are redirected for use in remote desktops and applications.</p> <p>See “Scanner Redirection Group Policy Settings,” on page 200.</p>
Serial Port Redirection	vdm_agent_serialport.adm	<p>Contains policy settings related to serial (COM) ports that are redirected for use in remote VDI desktops.</p> <p>See “Serial Port Redirection Group Policy Settings,” on page 206.</p>

Horizon Agent Configuration ADM Template Settings

The Horizon Agent Configuration ADM template file (`vdm_agent.adm`) contains policy settings related to the authentication and environmental components of Horizon Agent.

This ADM file is available in a bundled .zip file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.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.

The following table describes policy settings in the Horizon Agent Configuration ADM template file other than those settings that are used with USB devices. The template contains both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting.

Table 17-6. Horizon Agent Configuration Template Settings

Setting	Computer	User	Properties
<code>AllowDirectRDP</code>	X		<p>Determines whether clients other than Horizon Client devices can connect directly to remote desktops with RDP. When this setting is disabled, the agent permits only View-managed connections through Horizon Client. When connecting to a remote desktop from Horizon Client for Mac OS X, do not disable the <code>AllowDirectRDP</code> setting. If this setting is disabled, the connection fails with an <code>Access is denied</code> error. By default, while a user is logged in to a View desktop session, you can use RDP to connect to the virtual machine from outside of View. The RDP connection terminates the View desktop session, and the View user's unsaved data and settings might be lost. The View user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the <code>AllowDirectRDP</code> setting.</p> <p>IMPORTANT For View to operate correctly, the Windows Remote Desktop Services service must be running on the guest operating system of each desktop. You can use this setting to prevent users from making direct RDP connections to their desktops.</p> <p>This setting is enabled by default.</p>
<code>AllowSingleSignon</code>	X		<p>Determines whether single sign-on (SSO) is used to connect users to desktops and applications. When this setting is enabled, users are required to enter their credentials only once, when they log in to the server. When this setting is disabled, users must reauthenticate when the remote connection is made.</p> <p>This setting is enabled by default.</p>
<code>CommandsToRunOnConnect</code>	X		<p>Specifies a list of commands or command scripts to be run when a session is connected for the first time. See “Running Commands on View Desktops,” on page 271 for more information.</p>
<code>CommandsToRunOnDisconnect</code>	X		<p>Specifies a list of commands or command scripts to be run when a session is disconnected. See “Running Commands on View Desktops,” on page 271 for more information.</p>
<code>CommandsToRunOnReconnect</code>	X		<p>Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect. See “Running Commands on View Desktops,” on page 271 for more information.</p>

Table 17-6. Horizon Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
ConnectionTicketTimeout	X		Specifies the amount of time in seconds that the View connection ticket is valid. Horizon Client devices use a connection ticket for verification and single sign-on when connecting to the agent. For security reasons, a connection ticket is valid for a limited amount of time. When a user connects to a remote desktop, authentication must take place within the connection ticket timeout period or the session times out. If this setting is not configured, the default timeout period is 900 seconds.
CredentialFilterExceptions	X		Specifies the executable files that are not allowed to load the agent CredentialFilter. Filenames must not include a path or suffix. Use a semicolon to separate multiple filenames.
Disable Time Zone Synchronization	X	X	Determines whether the time zone of the View desktop is synchronized with the time zone of the connected client. An enabled setting applies only if the <code>Disable time zone forwarding</code> setting of the Horizon Client Configuration policy is not set to disabled. This setting is disabled by default.
Enable multi-media acceleration	X		Determines whether multimedia redirection (MMR) is enabled on the View desktop. MMR is a Windows Media Foundation filter that forwards multimedia data from specific codecs on the remote system directly through a TCP socket to the client. The data is then decoded directly on the client, where it is played. You can disable MMR if the client has insufficient resources to handle local multimedia decoding. This setting is enabled by default.
Enable system tray redirection for Hosted Apps	X		Determines whether system tray redirection is enabled while a user is running remote applications. This setting is located in the VMware View Agent Configuration > Unity Touch and Hosted Apps folder in the Group Policy Management Editor. This setting is enabled by default.
Enable Unity Touch	X		Determines whether the Unity Touch functionality is enabled on the View desktop. Unity Touch supports the delivery of remote applications in View and allows mobile device users to access applications in the Unity Touch sidebar. This setting is located in the VMware View Agent Configuration > Unity Touch and Hosted Apps folder in the Group Policy Management Editor. This setting is enabled by default.
ShowDiskActivityIcon	X		This setting is not supported in this release.
Toggle Display Settings Control	X		Determines whether to disable the Settings tab in the Display control panel when a client session uses the PCoIP display protocol. This setting is enabled by default.

NOTE The Connect using DNS Name setting was removed in the Horizon 6 version 6.1 release. You can set the View LDAP attribute, **pae-PreferDNS**, to tell View Connection Server to give preference to DNS names when sending the addresses of desktop machines and RDS hosts to clients and gateways. See "Give Preference to DNS Names When View Connection Server Returns Address Information" in the *View Installation* document.

USB Settings for the Horizon Agent

See ["USB Settings in the Horizon Agent Configuration ADM Template,"](#) on page 227.

Client System Information Sent to View Desktops

When a user connects or reconnects to a View desktop, Horizon Client gathers information about the client system and View Connection Server sends that information to the remote desktop.

Horizon Agent writes the client computer information to the system registry path `HKCU\Volatile Environment` on remote desktops that are deployed on single-user machines.

For remote desktops that are deployed in RDS sessions, Horizon Agent writes the client computer information to the system registry path `HKCU\Volatile Environment\x`, where *x* is the session ID, on the RDS host.

You can add commands to the Horizon Agent `CommandsToRunOnConnect`, `CommandsToRunOnReconnect`, and `CommandsToRunOnDisconnect` group policy settings to run commands or command scripts that read this information from the system registry when users connect and reconnect to desktops. See ["Running Commands on View Desktops,"](#) on page 271 for more information.

[Table 17-7](#) describes the registry keys that contain client system information and lists the types of client systems that support them.

Table 17-7. Client System Information

Registry Key	Description	Supported Desktops	Supported Client Systems
<code>ViewClient_IP_Address</code>	The IP address of the client system.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
<code>ViewClient_MAC_Address</code>	The MAC address of the client system.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android
<code>ViewClient_Machine_Name</code>	The machine name of the client system.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
<code>ViewClient_Machine_Domain</code>	The domain of the client system.	VDI (single-user machine) RDS	Windows, Metro
<code>ViewClient_LoggedOn_Username</code>	The user name that was used to log in to the client system.	VDI (single-user machine) RDS	Windows, Linux, Mac

Table 17-7. Client System Information (Continued)

Registry Key	Description	Supported Desktops	Supported Client Systems
ViewClient_LoggedOn_Domainname	The domain name that was used to log in to the client system.	VDI (single-user machine) RDS	Windows, Metro For Linux and Mac clients, see ViewClient_Machine_Domain.ViewClient_LoggedOn_Domainname is not given by the Linux or Mac client because Linux and Mac accounts are not bound to Windows domains.
ViewClient_Type	The thin client name or operating system type of the client system.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Broker_DNS_Name	The DNS name of the View Connection Server instance.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_URL	The URL of the View Connection Server instance.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Tunneled	The status of the tunnel connection for the View Connection Server, which can be either true (enabled) or false (disabled).	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Tunnel_URL	The URL of the View Connection Server tunnel connection, if the tunnel connection is enabled.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_Remote_IP_Address	The IP address of the client system that is seen by the View Connection Server instance.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_TZID	The Olson time zone ID. To disable time zone synchronization, enable the Horizon Agent Disable Time Zone Synchronization group policy setting.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS
ViewClient_Windows_Timezone	The GMT standard time. To disable time zone synchronization, enable the Horizon Agent Disable Time Zone Synchronization group policy setting.	VDI (single-user machine) RDS	Windows, Metro
ViewClient_Broker_DomainName	Domain name used to authenticate to View Connection Server.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Broker_UserName	Username used to authenticate to View Connection Server.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.

Table 17-7. Client System Information (Continued)

Registry Key	Description	Supported Desktops	Supported Client Systems
ViewClient_Client_ID	Specifies the Unique Client HardwareId used as a link to the license key.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Displays.Number	Specifies the number of monitors being used on the client.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Displays.Topology	Specifies the arrangement, resolution, and dimensions of displays on the client.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Keyboard.Type	Specifies the type of keyboard being used on the client. For example: Japanese, Korean.	VDI (single-user machine) RDS	Windows
ViewClient_Launch_SessionType	Specifies the session type. The type can be desktop or application.	VDI (single-user machine) RDS	Value is sent directly from View Connection Server, not gathered by Horizon Client.
ViewClient_Mouse.Identifier	Specifies the type of mouse.	VDI (single-user machine) RDS	Windows
ViewClient_Mouse.NumButtons	Specifies the number of buttons supported by the mouse.	VDI (single-user machine) RDS	Windows
ViewClient_Mouse.SampleRate	Specifies the rate, in reports per second, at which input from a PS/2 mouse is sampled.	VDI (single-user machine) RDS	Windows
ViewClient_Protocol	Specifies the protocol being used.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Language	Specifies the operating system language.	VDI (single-user machine) RDS	Windows, Linux, Mac, Android, iOS, Metro
ViewClient_Launch_ID	Specifies the desktop pool Unique ID.	VDI (single-user machine)	Windows, Linux, Mac, Android, iOS, Metro

NOTE The definitions of `ViewClient_LoggedOn_Username` and `ViewClient_LoggedOn_Domainname` in [Table 17-7](#) apply to Horizon Client 2.2 for Windows or later releases.

For Horizon Client 5.4 for Windows or earlier releases, `ViewClient_LoggedOn_Username` sends the user name that was entered in Horizon Client, and `ViewClient_LoggedOn_Domainname` sends the domain name that was entered in Horizon Client.

Horizon Client 2.2 for Windows is a later release than Horizon Client 5.4 for Windows. Starting with Horizon Client 2.2, the release numbers for Windows are consistent with the Horizon Client releases on other operating systems and devices.

Running Commands on View Desktops

You can use the Horizon Agent `CommandsToRunOnConnect`, `CommandsToRunOnReconnect`, and `CommandsToRunOnDisconnect` group policy settings to run commands and command scripts on View desktops when users connect, reconnect, and disconnect.

To run a command or a command script, add the command name or the file path of the script to the group policy setting's list of commands. For example:

```
date
```

```
C:\Scripts\myscript.cmd
```

To run scripts that require console access, prepend the `-C` or `-c` option followed by a space. For example:

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

Supported file types include `.CMD`, `.BAT`, and `.EXE`. `.VBS` files will not run unless they are parsed with `csript.exe` or `wscript.exe`. For example:

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

The total length of the string, including the `-C` or `-c` option, should not exceed 260 characters.

PCoIP Policy Settings

The PCoIP ADM template file (`pcoip.adm`) contains policy settings related to the PCoIP display protocol. You can configure settings to default values that can be overridden by an administrator, or you can configure settings to non-overridable values.

This ADM file is available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.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.

The View PCoIP Session Variables ADM template file contains two subcategories:

Overridable Administrator Defaults	Specifies PCoIP policy setting default values. These settings can be overridden by an administrator. These settings write registry keys values to <code>HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults</code> .
Not Overridable Administrator Settings	Contains the same settings as Overridable Administrator Defaults, but these settings cannot be overridden by an administrator. These settings write registry key values to <code>HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin</code> .

The template contains Computer Configuration settings only.

Non-Policy Registry Keys

If a local machine setting needs to be applied and cannot be placed under `HKLM\Software\Policies\Teradici`, local machine settings can be placed in registry keys in `HKLM\Software\Teradici`. The same registry keys can be placed in `HKLM\Software\Teradici` as in `HKLM\Software\Policies\Teradici`. If the same registry key is present in both locations, the setting in `HKLM\Software\Policies\Teradici` overrides the local machine value.

PCoIP General Settings

The View PCoIP ADM template file contains group policy settings that configure general settings such as PCoIP image quality, USB devices, and network ports.

Table 17-8. PCoIP General Policy Settings

Setting	Description
Configure clipboard redirection	<p>Determines the direction in which clipboard redirection is allowed. You can select one of these values:</p> <ul style="list-style-type: none"> ■ Enabled client to agent only (That is, allow copy and paste only from the client system to the remote desktop.) ■ Disabled in both directions ■ Enabled in both directions ■ Enabled agent to client only (That is, allow copy and paste only from the remote desktop to the client system.) <p>Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection does not function.</p> <p>This setting applies to Horizon Agent only.</p> <p>When this setting is disabled or not configured, the default value is Enabled client to agent only.</p>
Configure PCoIP client image cache size policy	<p>Controls the size of the PCoIP client image cache. The client uses image caching to store portions of the display that were previously transmitted. Image caching reduces the amount of data that is retransmitted.</p> <p>This setting applies only to Windows, Linux, and Mac clients when Horizon Client, Horizon Agent, and View Connection Server are a View 5.0 or later release.</p> <p>When this setting is not configured or disabled, PCoIP uses a default client image cache size of 250 MB.</p> <p>In Horizon Client 3.1 or later releases, if you specify a number that is smaller than the amount of available memory divided by 2, the cache size is set using the following formula:</p> $\text{user-setting} - 10 \text{ MB}$ <p>In Horizon Client 3.1 or later releases, if you specify a number that is larger than the available memory divided by 2, the cache size is set using the following formula:</p> $\text{available-memory} / 2 - 10 \text{ MB}$ <p>For example, if you specify a maximum cache size of 1024 MB, and the available memory is 1600 MB, the maximum cache size is set to 790 MB.</p> <p>For all Horizon Client versions, the default size is 250 MB and the minimum size is 50 MB.</p> <p>In Horizon Client 1.6 or later releases, the maximum size is 1024 MB. In Horizon Client 1.5 or earlier releases, the maximum size is 300 MB.</p>
Configure PCoIP event log cleanup by size in MB	<p>Enables the configuration of the PCoIP event log cleanup by size in MB.</p> <p>When this policy is configured, the setting controls how large a log file can grow before it is cleaned up. For a non-zero setting of <i>m</i>, log files larger than <i>m</i> MB are automatically and silently deleted. A setting of 0 indicates that no file cleanup by size takes place.</p> <p>When this policy is disabled or not configured, the default event log cleanup by size is 100 MB.</p> <p>The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.</p>

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description
Configure PCoIP event log cleanup by time in days	<p>Enables the configuration of the PCoIP event log cleanup by time in days.</p> <p>When this policy is configured, the setting controls how many days can pass before the log file is cleaned up. For a non-zero setting of <i>n</i>, log files older than <i>n</i> days are automatically and silently deleted. A setting of 0 indicates that no file cleanup by time takes place.</p> <p>When this policy is disabled or not configured, the default event log cleanup is 7 days.</p> <p>The log file cleanup is performed once at session startup. A change to the setting is not applied until the next session.</p>
Configure PCoIP event log verbosity	<p>Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose).</p> <p>When this setting is enabled, you can set the verbosity level from 0 to 3. When the setting is not configured or disabled, the default event log verbosity level is 2.</p> <p>When this setting is modified during an active PCoIP session, the new setting takes effect immediately.</p>
Configure PCoIP image quality levels	<p>Controls how PCoIP renders images during periods of network congestion. The Minimum Image Quality, Maximum Initial Image Quality, and Maximum Frame Rate values interoperate to provide fine control in network-bandwidth constrained environments.</p> <p>Use the Minimum Image Quality value to balance image quality and frame rate for limited-bandwidth scenarios. You can specify a value between 30 and 100. The default value is 40. A lower value allows higher frame-rates, but with a potentially lower quality display. A higher value provides higher image quality, but with potentially lower frame rates when network bandwidth is constrained. When network bandwidth is not constrained, PCoIP maintains maximum quality regardless of this value.</p> <p>Use the Maximum Initial Image Quality value to reduce the network bandwidth peaks required by PCoIP by limiting the initial quality of the changed regions of the display image. You can specify a value between 30 and 100. The default value is 80. A lower value reduces the image quality of content changes and decreases peak bandwidth requirements. A higher value increases the image quality of content changes and increases peak bandwidth requirements. Unchanged regions of the image progressively build to a lossless (perfect) quality regardless of this value. A value of 80 or lower best utilizes the available bandwidth.</p> <p>The Minimum Image Quality value cannot exceed the Maximum Initial Image Quality value.</p> <p>Use the Maximum Frame Rate value to manage the average bandwidth consumed per user by limiting the number of screen updates per second. You can specify a value between 1 and 120 frames per second. The default value is 30. A higher value can use more bandwidth but provides less jitter, which allows smoother transitions in changing images such as video. A lower value uses less bandwidth but results in more jitter.</p> <p>These image quality values apply to the soft host only and have no effect on a soft client.</p> <p>When this setting is disabled or not configured, the default values are used.</p> <p>When this setting is modified during an active PCoIP session, the new setting takes effect immediately.</p>

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description
Configure frame rate vs image quality preference	<p>Configure the frame rate and image quality preference from 0 (highest frame rate) to 100 (highest image quality). If this policy is disabled or not configured, the default setting is 50.</p> <p>Higher value (max: 100) means you prefer high image quality even if frame rate is choppy. Lower value (min: 0) means you prefer a fluent experience with aggressive image quality.</p> <p>This setting could work with the <code>Configure PCoIP image quality levels GPO</code>, which determines the max initial image quality level and min image quality level. While the <code>Frame rate and image quality preference</code> can adjust the image quality level for each frame, it cannot exceed the max/min quality level threshold configured by <code>Configure PCoIP image quality levels GPO</code>.</p> <p>When this policy is changed during run time, it could take effect immediately.</p>
Configure PCoIP session encryption algorithms	<p>Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation.</p> <p>Checking one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm.</p> <p>This setting applies to both agent and client. The endpoints negotiate the actual session encryption algorithm that is used. If FIPS140-2 approved mode is enabled, the Disable AES-128-GCM encryption value is always overridden so that AES-128-GCM encryption is enabled.</p> <p>Supported encryption algorithms, in order of preference, are SALSA20/12-256, AES-GCM-128, and AES-GCM-256. By default, all supported encryption algorithms are available for negotiation by this endpoint.</p> <p>If both endpoints are configured to support all three algorithms and the connection does not use a Security Gateway (SG), the SALSA20 algorithm will be negotiated and used. However, if the connection uses an SG, SALSA20 is automatically disabled and AES128 will be negotiated and used. If either endpoint or the SG disables SALSA20 and either endpoint disables AES128, then AES256 will be negotiated and used.</p>

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description								
Configure PCoIP USB allowed and unallowed device rules	<p>Specifies the USB devices that are authorized and not authorized for PCoIP sessions that use a zero client that runs Teradici firmware. USB devices that are used in PCoIP sessions must appear in the USB authorization table. USB devices that appear in the USB unauthorization table cannot be used in PCoIP sessions.</p> <p>You can define a maximum of 10 USB authorization rules and a maximum of 10 USB unauthorization rules. Separate multiple rules with the vertical bar () character.</p> <p>Each rule can be a combination of a Vendor ID (VID) and a Product ID (PID), or a rule can describe a class of USB devices. A class rule can allow or disallow an entire device class, a single subclass, or a protocol within a subclass.</p> <p>The format of a combination VID/PID rule is 1xxxxyyyy, where xxxx is the VID in hexadecimal format and yyyy is the PID in hexadecimal format. For example, the rule to authorize or block a device with VID 0x1a2b and PID 0x3c4d is 11a2b3c4d.</p> <p>For class rules, use one of the following formats:</p> <table border="0" data-bbox="735 751 1321 1108"> <tr> <td data-bbox="735 751 874 800">Allow all USB devices</td> <td data-bbox="940 751 1129 814">Format: 23XXXXXX Example: 23XXXXXX</td> </tr> <tr> <td data-bbox="735 835 874 940">Allow USB devices with a specific class ID</td> <td data-bbox="940 835 1153 898">Format: 22classXXXX Example: 22aaXXXX</td> </tr> <tr> <td data-bbox="735 961 895 1010">Allow a specific subclass</td> <td data-bbox="940 961 1238 1024">Format: 21class-subclassXX Example: 21aabbXX</td> </tr> <tr> <td data-bbox="735 1045 895 1094">Allow a specific protocol</td> <td data-bbox="940 1045 1321 1108">Format: 20class-subclass-protocol Example: 20aabbcc</td> </tr> </table> <p>For example, the USB authorization string to allow USB HID (mouse and keyboard) devices (class ID 0x03) and webcams (class ID 0x0e) is 2203XXXX 220eXXXX. The USB unauthorization string to disallow USB Mass Storage devices (class ID 0x08) is 2208XXXX.</p> <p>An empty USB authorization string means that no USB devices are authorized. An empty USB unauthorization string means that no USB devices are banned.</p> <p>This setting applies to Horizon Agent only and only when the remote desktop is in a session with a zero client that runs Teradici firmware. Device use is negotiated between the endpoints.</p> <p>By default, all devices are allowed and none are disallowed.</p>	Allow all USB devices	Format: 23XXXXXX Example: 23XXXXXX	Allow USB devices with a specific class ID	Format: 22classXXXX Example: 22aaXXXX	Allow a specific subclass	Format: 21class-subclassXX Example: 21aabbXX	Allow a specific protocol	Format: 20class-subclass-protocol Example: 20aabbcc
Allow all USB devices	Format: 23XXXXXX Example: 23XXXXXX								
Allow USB devices with a specific class ID	Format: 22classXXXX Example: 22aaXXXX								
Allow a specific subclass	Format: 21class-subclassXX Example: 21aabbXX								
Allow a specific protocol	Format: 20class-subclass-protocol Example: 20aabbcc								

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description
Configure PCoIP virtual channels	<p>Specifies the virtual channels that can and cannot operate over PCoIP sessions. This setting also determines whether to disable clipboard processing on the PCoIP host.</p> <p>Virtual channels that are used in PCoIP sessions must appear on the virtual channel authorization list. Virtual channels that appear in the unauthorized virtual channel list cannot be used in PCoIP sessions.</p> <p>You can specify a maximum of 15 virtual channels for use in PCoIP sessions.</p> <p>Separate multiple channel names with the vertical bar () character. For example, the virtual channel authorization string to allow the <code>mksvchan</code> and <code>vdp_rdpvbridge</code> virtual channels is <code>mksvchan vdp_vdpvbridge</code>.</p> <p>If a channel name contains the vertical bar or backslash (\) character, insert a backslash character before it. For example, type the channel name <code>awk ward\channel</code> as <code>awk\ ward\channel</code>.</p> <p>When the authorized virtual channel list is empty, all virtual channels are disallowed. When the unauthorized virtual channel list is empty, all virtual channels are allowed.</p> <p>The virtual channels setting applies to both agent and client. Virtual channels must be enabled on both agent and client for virtual channels to be used.</p> <p>The virtual channels setting provides a separate check box that allows you to disable remote clipboard processing on the PCoIP host. This value applies to the agent only.</p> <p>By default, all virtual channels are enabled, including clipboard processing.</p>
Configure the PCoIP transport header	<p>Configures the PCoIP transport header and sets the transport session priority.</p> <p>The PCoIP transport header is a 32-bit header that is added to all PCoIP UDP packets (only if the transport header is enabled and supported by both sides). The PCoIP transport header allows network devices to make better prioritization/QoS decisions when dealing with network congestion. The transport header is enabled by default.</p> <p>The transport session priority determines the PCoIP session priority reported in the PCoIP transport header. Network devices make better prioritization/QoS decisions based on the specified transport session priority.</p> <p>When the <code>Configure the PCoIP transport header</code> setting is enabled, the following transport session priorities are available:</p> <ul style="list-style-type: none"> ■ High ■ Medium (default value) ■ Low ■ Undefined <p>The transport session priority value is negotiated by the PCoIP agent and client. If the PCoIP agent specifies a transport session priority value, the session uses the agent-specified session priority. If only the client has specified a transport session priority, the session uses the client-specified session priority. If neither agent nor client has specified a transport session priority, or Undefined Priority is specified, the session uses the default value, Medium priority.</p>

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description
Configure the TCP port to which the PCoIP host binds and listens	<p>Specifies the TCP agent port bound to by software PCoIP hosts.</p> <p>The TCP port value specifies the base TCP port that the agent attempts to bind to. The TCP port range value determines how many additional ports to try if the base port is not available. The port range must be between 1 and 10.</p> <p>The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182.</p> <p>Do not set the size of the retry port range to 0. Setting this value to 0 causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message, <code>The Display protocol for this desktop is currently not available. Please contact your system administrator.</code></p> <p>This setting applies to Horizon Agent only.</p> <p>On single-user machines, the default base TCP port is 4172 in View 4.5 and later. The default base port is 50002 in View 4.0.x and earlier. By default, the port range is 1.</p> <p>On RDS hosts, the default base TCP port is 4173. When PCoIP is used with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections.</p> <p>IMPORTANT As a best practice, do not use this policy setting to change the default port range on RDS hosts, or change the TCP port value from the default of 4173. Most important, do not set the TCP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.</p>
Configure the UDP port to which the PCoIP host binds and listens	<p>Specifies the UDP agent port bound to by software PCoIP hosts.</p> <p>The UDP port value specifies the base UDP port that the agent attempts to bind to. The UDP port range value determines how many additional ports to try if the base port is not available. The port range must be between 1 and 10.</p> <p>Do not set the size of the retry port range to 0. Setting this value to 0 causes a connection failure when users log in to the desktop with the PCoIP display protocol. Horizon Client returns the error message, <code>The Display protocol for this desktop is currently not available. Please contact your system administrator.</code></p> <p>The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182.</p> <p>This setting applies to Horizon Agent only.</p> <p>On single-user machines, the default base UDP port is 4172 for View 4.5 and later and 50002 for View 4.0.x and earlier. By default, the port range is 10.</p> <p>On RDS hosts, the default base UDP port is 4173. When PCoIP is used with RDS hosts, a separate PCoIP port is used for each user connection. The default port range that is set by the Remote Desktop Service is large enough to accommodate the expected maximum of concurrent user connections.</p> <p>IMPORTANT As a best practice, do not use this policy setting to change the default port range on RDS hosts, or change the UDP port value from the default of 4173. Most important, do not set the UDP port value to 4172. Resetting this value to 4172 will adversely affect PCoIP performance in RDS sessions.</p>

Table 17-8. PCoIP General Policy Settings (Continued)

Setting	Description
Enable access to a PCoIP session from a vSphere console	<p>Determines whether to allow a vSphere Client console to display an active PCoIP session and send input to the desktop.</p> <p>By default, when a client is attached through PCoIP, the vSphere Client console screen is blank and the console cannot send input. The default setting ensures that a malicious user cannot view the user's desktop or provide input to the host locally when a PCoIP remote session is active. This setting applies to Horizon Agent only.</p> <p>When this setting is disabled or not configured, console access is not allowed. When this setting is enabled, the console displays the PCoIP session and console input is allowed.</p> <p>When this setting is enabled, the console can display a PCoIP session that is running on a Windows 7 system only when the Windows 7 virtual machine is hardware v8. Hardware v8 is available only on ESXi 5.0 and later. By contrast, console input to a Windows 7 system is allowed when the virtual machine is any hardware version.</p>
Enable the FIPS 140-2 approved mode of operation	<p>Determines whether to use only FIPS 140-2 approved cryptographic algorithms and protocols to establish a remote PCoIP connection. Enabling this setting overrides the disabling of AES128-GCM encryption.</p> <p>This setting applies to both agent and client. You can configure either endpoint or both endpoints to operate in FIPS mode. Configuring a single endpoint to operate in FIPS mode limits the encryption algorithms that are available for session negotiation.</p> <p>FIPS mode is available for View 4.5 and later. For View 4.0.x and earlier, FIPS mode is not available, and configuring this setting has no effect. When this setting is disabled or not configured, FIPS mode is not used.</p>
Enable/disable audio in the PCoIP session	<p>Determines whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. When this setting is enabled, PCoIP audio is allowed. When it is disabled, PCoIP audio is disabled. When this setting is not configured, audio is enabled by default.</p>
Enable/disable microphone noise and DC offset filter in PCoIP session	<p>Determines whether to enable the microphone noise and DC offset filter for microphone input during PCoIP sessions.</p> <p>This setting applies to Horizon Agent and Teradici audio driver only. When this setting is not configured, the Teradici audio driver uses the microphone noise and DC offset filter by default.</p>
Turn on PCoIP user default input language synchronization	<p>Determines whether the default input language for the user in the PCoIP session is synchronized with the default input language of the PCoIP client endpoint. When this setting is enabled, synchronization is allowed. When this setting is disabled or not configured, synchronization is disallowed.</p> <p>This setting applies to Horizon Agent only.</p>

PCoIP Bandwidth Settings

The View PCoIP ADM template file contains group policy settings that configure PCoIP bandwidth characteristics.

Table 17-9. View PCoIP Session Bandwidth Variables

Setting	Description
Configure the maximum PCoIP session bandwidth	<p>Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic.</p> <p>Set this value to the overall capacity of the link to which your endpoint is connected, taking into consideration the number of expected concurrent PCoIP sessions. For example, with a single-user VDI configuration (a single PCoIP session) that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value to leave some allowance for other network traffic. When you expect multiple concurrent PCoIP sessions to share a link, comprising either multiple VDI users or an RDS configuration, you might want to adjust the setting accordingly. However, lowering this value will restrict the maximum bandwidth for each active session.</p> <p>Setting this value prevents the agent from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and agent to use the lower of the two values that are set on the client and agent side. For example, setting a 4Mbit/s maximum bandwidth forces the agent to transmit at a lower rate, even though the setting is configured on the client.</p> <p>When this setting is disabled or not configured on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is configured, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second.</p> <p>The default value when this setting is not configured is 900000 kilobits per second.</p> <p>This setting applies to Horizon Agent and the client. If the two endpoints have different settings, the lower value is used.</p>
Configure the PCoIP session bandwidth floor	<p>Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session.</p> <p>This setting configures the minimum expected bandwidth transmission rate for the endpoint. When you use this setting to reserve bandwidth for an endpoint, the user does not have to wait for bandwidth to become available, which improves session responsiveness.</p> <p>Make sure that you do not over-subscribe the total reserved bandwidth for all endpoints. Make sure that the sum of bandwidth floors for all connections in your configuration does not exceed the network capability.</p> <p>The default value is 0, which means that no minimum bandwidth is reserved. When this setting is disabled or not configured, no minimum bandwidth is reserved.</p> <p>This setting applies to Horizon Agent and the client, but the setting only affects the endpoint on which it is configured.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p>

Table 17-9. View PCoIP Session Bandwidth Variables (Continued)

Setting	Description
Configure the PCoIP session MTU	<p>Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session.</p> <p>The MTU size includes IP and UDP packet headers. TCP uses the standard MTU discovery mechanism to set MTU and is not affected by this setting.</p> <p>The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes.</p> <p>Typically, you do not have to change the MTU size. Change this value if you have an unusual network setup that causes PCoIP packet fragmentation.</p> <p>This setting applies to Horizon Agent and the client. If the two endpoints have different MTU size settings, the lowest size is used.</p> <p>If this setting is disabled or not configured, the client uses the default value in the negotiation with Horizon Agent.</p>
Configure the PCoIP session audio bandwidth limit	<p>Specifies the maximum bandwidth that can be used for audio (sound playback) in a PCoIP session.</p> <p>The audio processing monitors the bandwidth used for audio. The processing selects the audio compression algorithm that provides the best audio possible, given the current bandwidth utilization. If a bandwidth limit is set, the processing reduces quality by changing the compression algorithm selection until the bandwidth limit is reached. If minimum quality audio cannot be provided within the bandwidth limit specified, audio is disabled.</p> <p>To allow for uncompressed high quality stereo audio, set this value to higher than 1600 kbit/s. A value of 450 kbit/s and higher allows for stereo, high-quality, compressed audio. A value between 50 kbit/s and 450 kbit/s results in audio that ranges between FM radio and phone call quality. A value below 50 kbit/s might result in no audio playback.</p> <p>This setting applies to Horizon Agent only. You must enable audio on both endpoints before this setting has any effect.</p> <p>In addition, this setting has no effect on USB audio.</p> <p>If this setting is disabled or not configured, a default audio bandwidth limit of 500 kilobits per second is configured to constrain the audio compression algorithm selected. If the setting is configured, the value is measured in kilobits per second, with a default audio bandwidth limit of 500 kilobits per second.</p> <p>This setting applies to View 4.6 and later. It has no effect on earlier versions of View.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p>
Turn off Build-to-Lossless feature	<p>Specifies whether to turn the build-to-lossless feature of the PCoIP protocol off or on. This feature is turned off by default.</p> <p>If this setting is enabled or not configured, the build-to-lossless feature is turned off, and images and other desktop and application content are never built to a lossless state. In network environments with constrained bandwidth, turning off the build-to-lossless feature can provide bandwidth savings.</p> <p>If this setting is disabled, the build-to-lossless feature is turned on. Turning on the build-to-lossless feature is recommended in environments that require images and other desktop and application content to be built to a lossless state.</p> <p>When this setting is modified during an active PCoIP session, the change takes effect immediately.</p> <p>For more information about the PCoIP build-to-lossless feature, see “PCoIP Build-to-Lossless Feature,” on page 281.</p>

PCoIP Keyboard Settings

The View PCoIP ADM template file contains group policy settings that configure PCoIP settings that affect the use of the keyboard.

Table 17-10. View PCoIP Session Variables for the Keyboard

Setting	Description
Disable sending CAD when users press Ctrl+Alt+Del	<p>When this policy is enabled, users must press Ctrl+Alt+Insert instead of Ctrl+Alt+Del to send a Secure Attention Sequence (SAS) to the remote desktop during a PCoIP session.</p> <p>You might want to enable this setting if users become confused when they press Ctrl+Alt+Del to lock the client endpoint and an SAS is sent to both the host and the guest.</p> <p>This setting applies to Horizon Agent only and has no effect on a client.</p> <p>When this policy is not configured or is disabled, users can press Ctrl +Alt+Del or Ctrl+Alt+Insert to send an SAS to the remote desktop.</p>
Use alternate key for sending Secure Attention Sequence	<p>Specifies an alternate key, instead of the Insert key, for sending a Secure Attention Sequence (SAS).</p> <p>You can use this setting to preserve the Ctrl+Alt+Ins key sequence in virtual machines that are launched from inside a remote desktop during a PCoIP session.</p> <p>For example, a user can launch a vSphere Client from inside a PCoIP desktop and open a console on a virtual machine in vCenter Server. If the Ctrl+Alt+Ins sequence is used inside the guest operating system on the vCenter Server virtual machine, a Ctrl+Alt+Del SAS is sent to the virtual machine. This setting allows the Ctrl+Alt+<i>Alternate Key</i> sequence to send a Ctrl+Alt+Del SAS to the PCoIP desktop.</p> <p>When this setting is enabled, you must select an alternate key from a drop-down menu. You cannot enable the setting and leave the value unspecified.</p> <p>When this setting is disabled or not configured, the Ctrl+Alt+Ins key sequence is used as the SAS.</p> <p>This setting applies to Horizon Agent only and has no effect on a client.</p>

PCoIP Build-to-Lossless Feature

You can configure the PCoIP display protocol to use an encoding approach called progressive build, or build-to-lossless, which works to provide the optimal overall user experience even under constrained network conditions. This feature is turned off by default.

The build-to-lossless feature provides a highly compressed initial image, called a lossy image, that is then progressively built to a full lossless state. A lossless state means that the image appears with the full fidelity intended.

On a LAN, PCoIP always displays text using lossless compression. If the build-to-lossless feature is turned on, and if available bandwidth per session drops below 1Mbps, PCoIP initially displays a lossy text image and rapidly builds the image to a lossless state. This approach allows the desktop to remain responsive and display the best possible image during varying network conditions, providing an optimal experience for users.

The build-to-lossless feature provides the following characteristics:

- Dynamically adjusts image quality
- Reduces image quality on congested networks
- Maintains responsiveness by reducing screen update latency
- Resumes maximum image quality when the network is no longer congested

You can turn on the build-to-lossless feature by disabling the Turn off Build-to-Lossless feature group policy setting. See “PCoIP Bandwidth Settings,” on page 279.

VMware Blast Policy Settings

The VMware Blast group policy template file `vdm_blast.adm` contains policy settings for the VMware Blast display protocol. After the policy is applied, the settings are stored in the registry key

`HKLM\Software\Policies\VMware, Inc.\VMware Blast\config`.

These settings apply to HTML Access and all Horizon Clients.

Table 17-11. VMware Blast Policy Settings

Setting	Description
Max Session Bandwidth	Specifies the maximum bandwidth, in kilobits per second (kbps), for a VMware Blast session. The bandwidth includes all imaging, audio, virtual channel, USB, and VMware Blast control traffic. The default is 1 Gbps.
Min Session Bandwidth	Specifies the minimum bandwidth, in kilobits per second (kbps), that is reserved for a VMware Blast session. The default is 128 kbps.
Max Frame Rate	Specifies the maximum rate of screen updates. Use this setting to manage the average bandwidth that users consume. The default is 30 updates per second.
UDP Protocol	Specifies whether to use the UDP or the TCP protocol. The default is not to use the UDP protocol, that is, to use the TCP protocol. Enable this setting to use the UDP protocol. This setting does not apply to HTML Access, which always uses the TCP protocol.
H264	Specifies whether to use H.264 encoding or JPEG/PNG encoding. The default is to use H.264 encoding.
Screen Blanking	Specifies whether to have the desktop VM's console show the actual desktop that the user sees or to show a blank screen when the desktop has an active session. The default is to show a blank screen.
Session Garbage Collection	Specifies how garbage collection of abandoned remoting sessions runs. You specify two values: <ul style="list-style-type: none"> ■ Interval (ms) determines how often, in milliseconds, the garbage collector runs. The default is 100 ms. ■ Threshold (s) determines how old, in seconds, an abandoned session must be before it is a candidate for deletion. The default is 1 second.
Image Quality	Specifies the image quality of the desktop display. You can specify two low-quality settings, two high-quality settings, and a mid-quality setting. The low-quality settings are for areas of the screen that change often, for example, when scrolling occurs. The high-quality settings are for areas of the screen that are more static, resulting in a better image quality. You can specify the following settings: <ul style="list-style-type: none"> ■ Low JPEG Quality (available range of values: 1 - 100, default: 25) ■ Low JPEG Chroma Subsampling (available range of values: 4:1:0 (lowest), 4:1:1, 4:2:0, 4:2:2, and 4:4:4 (highest), default: 4:1:0) ■ Mid JPEG Quality (available range of values: 1 - 100, default: 35) ■ High JPEG Quality (available range of values: 1 - 100, default: 90) ■ High JPEG Chroma Subsampling (available range of values: 4:1:0 (lowest), 4:1:1, 4:2:0, 4:2:2, and 4:4:4 (highest), default: 4:4:4)
HTTP Service	Specifies the port that is used for secure communication (HTTPS) between the security server or Access Point appliance and a desktop. The firewall must be configured to have this port open. The default is 22443.

Table 17-11. VMware Blast Policy Settings (Continued)

Setting	Description
Audio Playback	Specifies whether audio playback is enabled for remote desktops. This setting is to enable audio playback.
Configure Clipboard Redirection	Specifies the permissible behavior for clipboard redirection. The options are: <ul style="list-style-type: none"> ■ Enabled in both directions ■ Disabled in both directions ■ Enabled client to server only (Users can copy/paste from the client to the desktop only.) ■ Enabled server to client only (Users can copy/paste from the desktop to the client only.) The default is Enabled client to server only .

Using Remote Desktop Services Group Policies

You can use Remote Desktop Services (RDS) group policies to control the configuration and performance of RDS hosts and RDS desktop and application sessions. View provides ADMX files that contain the Microsoft RDS group policies that are supported in View.

As a best practice, configure the group policies that are provided in the View ADMX files rather than the corresponding Microsoft group policies. The View group policies are certified to support your View deployment.

Configure the RDS Per Device CAL Storage

You can configure the RDS Per Device CAL storage options to specify the location of the CALs to be stored. This feature lets you decide whether you want to store the CALs or not.

Sometimes, there might be potential over usage of Per Device CALs, such as View RDS Deployments might have both Windows Server 2008 and Windows Server 2012 systems. Enabling this feature makes the CAL usage efficient in View RDS deployments. This is achieved by storing the issued license, supplying the license when the client is trying to connect to the RDS host, and storing the license again if there is any license upgrade.

You can configure the RDS Per Device CAL in the View Administrator or manually in View LDAP database.

Procedure

- 1 In the View Administrator, click **View Configuration > Global Settings**.
- 2 In the General pane, click **Edit**.
- 3 Select one of the following configurations from the **RDS Per Device CAL Storage Options** drop-down menu.

Option	Description
Save only on Broker	The Per Device CALs are saved only on Broker. NOTE The LDAP entry, <code>cs-enablerdslicensing=true</code> and <code>sendRdsLicense=false</code> .
Save on both Clients and Broker	The Per Device CALs are stored on both Clients and Broker. NOTE The LDAP entries <code>cs-enablerdslicensing=true</code> and <code>sendRdsLicense=true</code> .
Don't save the Per Device CAL	The Per Device CALs are not stored at any location. NOTE The LDAP entries, <code>cs-enablerdslicensing=false</code> and <code>sendRdsLicense=false</code> .

- 4 Click **OK**.

Add the Remote Desktop Services ADMX Files to Active Directory

You can add the policy settings in the View RDS ADMX files to group policy objects (GPOs) in Active Directory. You can also install the RDS ADMX files on individual RDS hosts.

Prerequisites

- Create GPOs for the RDS group policy settings and link them to the OU that contains your RDS hosts.
- Verify that the Group Policy Management feature is available on your Active Directory server.

The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See [“Create GPOs for View Group Policies,”](#) on page 298.

Procedure

- 1 Download the View 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 View are available in this file.

- 2 Unzip the `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` file and copy the RDS ADMX files to your Active Directory or RDS host.
 - a Copy the `vmware_rdsh.admx` and `vmware_rdsh_server.admx` files and the `en-US` folder to the `C:\Windows\PolicyDefinitions` folder on your Active Directory or RDS host.
 - b (Optional) Copy the language resource files `vmware_rdsh.adml` and `vmware_rdsh_server.adml` to the appropriate subfolder in `C:\Windows\PolicyDefinitions\` on your Active Directory or RDS host.
- 3 On the Active Directory host, open the Group Policy Management Editor.

On an individual RDS host, you can open the Local Group Policy Editor with the `gpedit.msc` utility.

The View RDS group policy settings are installed in the **Computer Configuration > Policies > Administrative Templates > Windows Components > Horizon View RDSH Services > Remote Desktop Session Host** folder.

- 4 (Optional) Configure the group policy settings in the **Horizon View RDSH Services > Remote Desktop Session Host** folder.

RDS Application Compatibility Settings

The RDS Application Compatibility group policy settings control Windows installer compatibility, remote desktop IP virtualization, network adapter selection, and the use of the RDS host IP address.

Table 17-12. RDS Application Compatibility Group Policy Settings

Setting	Description
Turn off Windows Installer RDS Compatibility	<p>This policy setting specifies whether Windows Installer RDS Compatibility runs on a per user basis for fully installed applications. Windows Installer allows one instance of the <code>msiexec</code> process to run at a time. By default, Windows Installer RDS Compatibility is turned on.</p> <p>If you enable this policy setting, Windows Installer RDS Compatibility is turned off, and only one instance of the <code>msiexec</code> process can run at a time.</p> <p>If you disable or do not configure this policy setting, Windows Installer RDS Compatibility is turned on, and multiple per user application installation requests are queued and handled by the <code>msiexec</code> process in the order in which they are received.</p>
Turn on Remote Desktop IP Virtualization	<p>This policy setting specifies whether Remote Desktop IP Virtualization is turned on.</p> <p>By default, Remote Desktop IP Virtualization is turned off.</p> <p>If you enable this policy setting, Remote Desktop IP Virtualization is turned on. You can select the mode in which this setting is applied. If you are using Per Program mode, you must enter a list of programs to use virtual IP addresses. List each program on a separate line (do not enter any blank lines between programs). For example:</p> <pre>explorer.exe mstsc.exe</pre> <p>If you disable or do not configure this policy setting, Remote Desktop IP Virtualization is turned off.</p>
Select the network adapter to be used for Remote Desktop IP Virtualization	<p>This policy setting specifies the IP address and network mask that corresponds to the network adapter used for virtual IP addresses. The IP address and network mask should be entered in Classless Inter-Domain Routing notation. For example: <code>192.0.2.96/24</code>.</p> <p>If you enable this policy setting, the specified IP address and network mask are used to select the network adapter used for the virtual IP addresses.</p> <p>If you disable or do not configure this policy setting, Remote Desktop IP Virtualization is turned off. A network adapter must be configured for Remote Desktop IP Virtualization to work.</p>
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	<p>This policy setting specifies whether a session uses the IP address of the Remote Desktop Session Host server if a virtual IP address is not available.</p> <p>If you enable this policy setting, the IP address of the RD Session Host server is not used if a virtual IP is not available. The session will not have network connectivity.</p> <p>If you disable or do not configure this policy setting, the IP address of the RD Session Host server is used if a virtual IP is not available.</p>

RDS Connections Settings

The RDS Connections group policy setting lets you disable Fair Share CPU Scheduling.

Table 17-13. RDS Connections Group Policy Settings

Setting	Description
Turn off Fair Share CPU Scheduling	<p>Fair Share CPU Scheduling dynamically distributes processor time across all Remote Desktop Services sessions on the same RD Session Host server, based on the number of sessions and the demand for processor time within each session.</p> <p>If you enable this policy setting, Fair Share CPU Scheduling is turned off.</p> <p>If you disable or do not configure this policy setting, Fair Share CPU Scheduling is turned on.</p>

RDS Device and Resource Redirection Settings

The RDS device and resource redirection group policy settings control access to devices and resources on a client computer in Remote Desktop Services sessions.

Table 17-14. RDS Device and Resource Redirection Group Policy Settings

Setting	Description
Allow time zone redirection	<p>This policy setting determines whether the client computer redirects its time zone settings to the Remote Desktop Services session.</p> <p>If you enable this policy setting, clients that are capable of time zone redirection send their time zone information to the server. The server base time is then used to calculate the current session time (current session time = server base time + client time zone).</p> <p>If you disable or do not configure this policy setting, the client computer does not redirect its time zone information and the session time zone is the same as the server time zone.</p>

RDS Licensing Settings

The RDS Licensing group policy settings control the order in which RDS license servers are located, whether problem notifications are displayed, and whether Per User or Per Device licensing is used for RDS Client Access Licenses (CALs).

Table 17-15. RDS Licensing Group Policy Settings

Setting	Description
Use the specified Remote Desktop license servers	<p>This policy setting allows you to specify the order in which an RD Session Host server attempts to locate Remote Desktop license servers.</p> <p>If you enable this policy setting, an RD Session Host server first attempts to locate the license servers that you specify. If the specified license servers cannot be located, the RD Session Host server will attempt automatic license server discovery.</p> <p>In the automatic license server discovery process, an RD Session Host server in a Windows Server-based domain attempts to contact a license server in the following order:</p> <ol style="list-style-type: none"> 1 License servers that are specified in the Remote Desktop Session Host Configuration tool 2 License servers that are published in Active Directory Domain Services 3 License servers that are installed on domain controllers in the same domain as the RD Session Host server <p>If you disable or do not configure this policy setting, the RD Session Host server uses the license server discovery mode specified in the Remote Desktop Session Host Configuration tool.</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>This policy setting determines whether notifications are displayed on an RD Session Host server when there are problems with RD Licensing that affect the RD Session Host server.</p> <p>By default, notifications are displayed on an RD Session Host server after you log on as a local administrator, if there are problems with RD Licensing that affect the RD Session Host server. If applicable, a notification will also be displayed that notes the number of days until the licensing grace period for the RD Session Host server will expire.</p> <p>If you enable this policy setting, these notifications will not be displayed on the RD Session Host server.</p> <p>If you disable or do not configure this policy setting, these notifications will be displayed on the RD Session Host server after you log on as a local administrator.</p>
Set the Remote Desktop licensing mode	<p>This policy setting allows you to specify the type of Remote Desktop Services client access license (RDS CAL) that is required to connect to this RD Session Host server.</p> <p>You can use this policy setting to select one of two licensing modes: Per User or Per Device.</p> <p>Per User licensing mode requires that each user account connecting to this RD Session Host server have an RDS Per User CAL.</p> <p>Per Device licensing mode requires that each device connecting to this RD Session Host server have an RDS Per Device CAL.</p> <p>If you enable this policy setting, the licensing mode that you specify takes precedence over the licensing mode that is specified during the installation of Remote Desktop Session Host or specified in the Remote Desktop Session Host Configuration tool.</p>

Table 17-15. RDS Licensing Group Policy Settings (Continued)

Setting	Description
	If you disable or do not configure this policy setting, the licensing mode that is specified during the installation of Remote Desktop Session Host role service or specified in the Remote Desktop Session Host Configuration tool is used.

RDS Profiles Settings

The RDS Profiles group policy settings control roaming profile and home directory settings for Remote Desktop Services sessions.

Table 17-16. RDS Profiles Group Policy Settings

Setting	Description
Limit the size of the entire roaming user profile cache	<p>This policy setting allows you to limit the size of the entire roaming user profile cache on the local drive. This policy setting only applies to a computer on which the Remote Desktop Session Host role service is installed.</p> <p>NOTE If you want to limit the size of an individual user profile, use the <code>Limit profile size</code> policy setting located in <code>User Configuration\Policies\Administrative Templates\System\User Profiles</code>.</p> <p>If you enable this policy setting, you must specify a monitoring interval (in minutes) and a maximum size (in gigabytes) for the entire roaming user profile cache. The monitoring interval determines how often the size of the entire roaming user profile cache is checked. When the size of the entire roaming user profile cache exceeds the maximum size that you have specified, the oldest (least recently used) roaming user profiles will be deleted until the size of the entire roaming user profile cache is less than the maximum size specified.</p> <p>If you disable or do not configure this policy setting, no restriction is placed on the size of the entire roaming user profile cache on the local drive.</p> <p>Note: This policy setting is ignored if the <code>Prevent Roaming Profile changes from propagating</code> to the server policy setting located in <code>Computer Configuration\Policies\Administrative Templates\System\User Profiles</code> is enabled.</p>
Set Remote Desktop Services User Home Directory	<p>Specifies whether Remote Desktop Services uses the specified network share or local directory path as the root of the user's home directory for a Remote Desktop Services session.</p> <p>To use this setting, select the location for the home directory (network or local) from the Location drop-down list. If you choose to place the directory on a network share, type the Home Dir Root Path in the form <code>\\Computername\Sharename</code>, and then select the drive letter to which you want the network share to be mapped.</p> <p>If you choose to keep the home directory on the local computer, type the Home Dir Root Path in the form <code>Drive:\Path</code>, without environment variables or ellipses. Do not specify a placeholder for user alias, because Remote Desktop Services automatically appends this at logon.</p> <p>NOTE The Drive Letter field is ignored if you choose to specify a local path. If you choose to specify a local path but then type the name of a network share in Home Dir Root Path, Remote Desktop Services places user home directories in the network location.</p> <p>If the status is set to Enabled, Remote Desktop Services creates the user's home directory in the specified location on the local computer or the network. The home directory path for each user is the specified Home Dir Root Path and the user's alias.</p> <p>If the status is set to Disabled or Not Configured, the user's home directory is as specified at the server.</p>

Table 17-16. RDS Profiles Group Policy Settings (Continued)

Setting	Description
Use mandatory profiles on the RD Session Host server	<p>This policy setting allows you to specify whether Remote Desktop Services uses a mandatory profile for all users connecting remotely to the RD Session Host server.</p> <p>If you enable this policy setting, Remote Desktop Services uses the path specified in the Set path for Remote Desktop Services Roaming User Profile policy setting as the root folder for the mandatory user profile. All users connecting remotely to the RD Session Host server use the same user profile.</p> <p>If you disable or do not configure this policy setting, mandatory user profiles are not used by users connecting remotely to the RD Session Host server.</p> <p>NOTE For this policy setting to take effect, you must also enable and configure the Set path for Remote Desktop Services Roaming User Profile policy setting.</p>
Set path for Remote Desktop Services Roaming User Profile	<p>This policy setting allows you to specify the network path that Remote Desktop Services uses for roaming user profiles.</p> <p>By default, Remote Desktop Services stores all user profiles locally on the RD Session Host server. You can use this policy setting to specify a network share where user profiles can be centrally stored, allowing a user to access the same profile for sessions on all RD Session Host servers that are configured to use the network share for user profiles.</p> <p>If you enable this policy setting, Remote Desktop Services uses the specified path as the root directory for all user profiles. The profiles are contained in subfolders named for the account name of each user.</p> <p>To configure this policy setting, type the path to the network share in the form of <code>\\Computername\Sharename</code>. Do not specify a placeholder for the user account name, because Remote Desktop Services automatically adds this when the user logs on and the profile is created. If the specified network share does not exist, Remote Desktop Services displays an error message on the RD Session Host server and will store the user profiles locally on the RD Session Host server.</p> <p>If you disable or do not configure this policy setting, user profiles are stored locally on the RD Session Host server. You can configure a user's profile path on the Remote Desktop Services Profile tab on the user's account Properties dialog box.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li data-bbox="831 1415 1398 1566">1 The roaming user profiles enabled by the policy setting apply only to Remote Desktop Services connections. A user might also have a Windows roaming user profile configured. The Remote Desktop Services roaming user profile always takes precedence in a Remote Desktop Services session. <li data-bbox="831 1577 1426 1873">2 To configure a mandatory Remote Desktop Services roaming user profile for all users connecting remotely to the RD Session Host server, use this policy setting together with the Use mandatory profiles on the RD Session Host server policy setting located in Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\RD Session Host\Profiles. The path set in the Set path for Remote Desktop Services Roaming User Profile policy setting should contain the mandatory profile.

RDS Remote Session Environment Settings

The RDS Remote Session Environment group policy settings control configuration of the user interface in Remote Desktop Services sessions.

Table 17-17. RDS Remote Session Environment Group Policy Settings

Setting	Description
Remove Windows Security item from Start menu	<p>Specifies whether to remove the Windows Security item from the Settings menu on Remote Desktop clients. You can use this setting to prevent inexperienced users from logging off from Remote Desktop Services inadvertently.</p> <p>If the status is set to Enabled, Windows Security does not appear in Settings on the Start menu. As a result, users must type a security attention sequence, such as CTRL+ALT+END, to open the Windows Security dialog box on the client computer.</p> <p>If the status is set to Disabled or Not Configured, Windows Security remains in the Settings menu.</p>

RDS Security Settings

The RDS Security group policy setting controls whether to let local administrators customize permissions.

Table 17-18. RDS Security Group Policy Settings

Setting	Description
Do not allow local administrators to customize permissions	<p>Specifies whether to disable the administrator rights to customize security permissions in the Remote Desktop Session Host Configuration tool.</p> <p>You can use this setting to prevent administrators from making changes to the user groups on the Permissions tab in the Remote Desktop Session Host Configuration tool. By default, administrators are able to make such changes.</p> <p>If the status is set to Enabled, the Permissions tab in the Remote Desktop Session Host Configuration tool cannot be used to customize per-connection security descriptors or to change the default security descriptors for an existing group. All of the security descriptors are Read Only.</p> <p>If the status is set to Disabled or Not Configured, server administrators have full Read/Write privileges to the user security descriptors on the Permissions tab in the Remote Desktop Session Host Configuration tool.</p> <p>NOTE The preferred method of managing user access is by adding a user to the Remote Desktop Users group.</p>

RDS Temporary Folders Settings

The RDS Connections group policy settings control the creation and deletion of temporary folders for Remote Desktop Services sessions.

Table 17-19. RDS Temporary Folders Group Policy Settings

Setting	Description
Do not delete temp folder upon exit	<p>Specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff.</p> <p>You can use this setting to maintain a user's session-specific temporary folders on a remote computer, even if the user logs off from a session. By default, Remote Desktop Services deletes a user's temporary folders when the user logs off.</p> <p>If the status is set to Enabled, users' per-session temporary folders are retained when the user logs off from a session.</p> <p>If the status is set to Disabled, temporary folders are deleted when a user logs off, even if the administrator specifies otherwise in the Remote Desktop Session Host Configuration tool.</p> <p>If the status is set to Not Configured, Remote Desktop Services deletes the temporary folders from the remote computer at logoff, unless specified otherwise by the server administrator.</p> <p>NOTE This setting only takes effect if per-session temporary folders are in use on the server. That is, if you enable the "Do not use temporary folders per session" setting, this setting has no effect.</p>
Do not use temporary folders per session	<p>This policy setting allows you to prevent Remote Desktop Services from creating session-specific temporary folders.</p> <p>You can use this policy setting to disable the creation of separate temporary folders on a remote computer for each session. By default, Remote Desktop Services creates a separate temporary folder for each active session that a user maintains on a remote computer. These temporary folders are created on the remote computer in a Temp folder under the user's profile folder and are named with the <code>sessionid</code>.</p> <p>If you enable this policy setting, per-session temporary folders are not created. Instead, a user's temporary files for all sessions on the remote computer are stored in a common Temp folder under the user's profile folder on the remote computer.</p> <p>If you disable this policy setting, per-session temporary folders are always created, even if you specify otherwise in the Remote Desktop Session Host Configuration tool.</p> <p>If you do not configure this policy setting, per-session temporary folders are created unless you specify otherwise in the Remote Desktop Session Host Configuration tool.</p>

Setting Up Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to View desktops, enabling users to print to their local and network printers from their View desktops.

Location-based printing allows IT organizations to map View desktops to the printer that is closest to the endpoint client device. For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer.

The location-based printing feature is available for Windows, Mac OS X, Linux, and mobile client devices.

In Horizon 6.0.1 and later, location-based 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
- Hosted Apps
- Hosted Apps that are launched from Horizon Client inside remote desktops

In Horizon 6.0 and earlier, location-based printing is supported on desktops that are deployed on single-user, Windows Desktop machines.

To use the location-based printing feature, you must install the Virtual Printing setup option with Horizon Agent and install the correct printer drivers on the desktop.

You set up location-based printing by configuring the Active Directory group policy setting `AutoConnect Map Additional Printers for VMware View`, which is located in the Microsoft Group Policy Object Editor in the **Software Settings** folder under **Computer Configuration**.

NOTE `AutoConnect Map Additional Printers for VMware View` is a computer-specific policy. Computer-specific policies apply to all View desktops, regardless of who connects to the desktop.

`AutoConnect Map Additional Printers for VMware View` is implemented as a name translation table. You use each row in the table to identify a specific printer and define a set of translation rules for that printer. The translation rules determine whether the printer is mapped to the View desktop for a particular client system.

When a user connects to a View desktop, View compares the client system to the translation rules associated with each printer in the table. If the client system meets all of the translation rules set for a printer, or if a printer has no associated translation rules, View maps the printer to the View desktop during the user's session.

You can define translation rules based on the client system's IP address, name, and MAC address, and on the user's name and group. You can specify one translation rule, or a combination of several translation rules, for a specific printer.

The information used to map the printer to the View desktop is stored in a registry entry on the View desktop in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

Printer Settings for Location-Based Printing

In Horizon 6.0.2 and later, printer settings for location-based printers are retained after a user logs out or disconnects from the desktop. For example, a user might set a location-based printer to use black and white mode. After the user logs out and logs in to the desktop again, the location-based printer continues to use black and white mode.

To save printer settings across sessions in a Hosted App, the user must select a location-based printer from the application's print dialog box, right-click the selected printer, and select **Printing Preferences**. Printer settings are not saved if the user selects a printer and clicks the **Preferences** button in the application's print dialog box.

Persistent settings for location-based printers are not supported if the settings are saved in the printer driver's private space and not in the DEVMODE extended part of the printer driver, as recommended by Microsoft. To support persistent settings, deploy printers that have the settings saved in the DEVMODE part of the printer driver.

Register the Location-Based Printing Group Policy DLL File

Before you can configure the group policy setting for location-based printing, you must register the DLL file `TPVMGPOACmap.dll`.

The 32-bit and 64-bit versions of `TPVMGPOACmap.dll` are available in a bundled .zip file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. You can download the file from the VMware Horizon 6 download site at <http://www.vmware.com/go/downloadview>.

Earlier View releases provide 32-bit and 64-bit versions of `TPVMGPOACmap.dll` in the directory `install_directory\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` on your View Connection Server host.

Procedure

- 1 Copy the appropriate version of `TPVMGPOACmap.dll` to your Active Directory server or to the domain computer that you use to configure group policies.
- 2 Use the `regsvr32` utility to register the `TPVMGPOACmap.dll` file.

For example: `regsvr32 "C:\TPVMGPOACmap.dll"`

What to do next

Configure the group policy setting for location-based printing.

Configure the Location-Based Printing Group Policy

To set up location-based printing, you configure the `AutoConnect Map Additional Printers for VMware View` group policy setting. The group policy setting is a name translation table that maps printers to View desktops.

Prerequisites

- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server or on the domain computer that you use to configure group policies.
- Register the DLL file `TPVMGPOACmap.dll` on your Active Directory server or on the domain computer that you use to configure group policies. See [“Register the Location-Based Printing Group Policy DLL File,”](#) on page 294.
- Familiarize yourself with syntax of the `AutoConnect Map Additional Printers for VMware View` group policy setting. See [“Location-Based Printing Group Policy Setting Syntax,”](#) on page 295.
- Create a GPO for the location-based group policy setting and link it to the OU that contains your View desktops. See [“Create GPOs for View Group Policies,”](#) on page 298 for an example of how to create GPOs for View group policies.
- Verify that the Virtual Printing setup option was installed with Horizon Agent on your desktops. To verify, check if the TP AutoConnect Service and TP VC Gateway Service are installed in the desktop operating system.
- Because print jobs are sent directly from the View desktop to the printer, verify that the required printer drivers are installed on your desktops.

Procedure

- 1 On the Active Directory server, edit the GPO.

AD Version	Navigation Path
Windows 2003	<ol style="list-style-type: none"> a Select Start > All Programs > Administrative Tools > Active Directory Users and Computers. b Right-click the OU that contains your View desktops and select Properties. c On the Group Policy tab, click Open to open the Group Policy Management plug-in. d In the right pane, right-click the GPO that you created for the location-based printing group policy setting and select Edit.
Windows 2008	<ol style="list-style-type: none"> a Select Start > Administrative Tools > Group Policy Management. b Expand your domain, right-click the GPO that you created for the location-based printing group policy setting and select Edit.

The Group Policy Object Editor window appears.

- 2 Expand **Computer Configuration**, open the **Software Settings** folder, and select **AutoConnect Map Additional Printers for VMware View**.
- 3 In the Policy pane, double-click **Configure AutoConnect Map Additional Printers**.

The AutoConnect Map Additional Printers for VMware View window appears.

- 4 Select **Enabled** to enable the group policy setting.

The translation table headings and buttons appear in the group policy window.

IMPORTANT Clicking **Disabled** deletes all table entries. As a precaution, save your configuration so that you can import it later.

- 5 Add the printers that you want to map to View desktops and define their associated translation rules.
- 6 Click **OK** to save your changes.

Location-Based Printing Group Policy Setting Syntax

You use the `AutoConnect Map Additional Printers for VMware View` group policy setting to map printers to remote desktops.

`AutoConnect Map Additional Printers for VMware View` is a name translation table that identifies printers and defines associated translation rules. [Table 17-20](#) describes the syntax of the translation table.

Location-based printing maps local printers to remote desktops but does not support mapping network printers that are configured by using UNC paths.

Table 17-20. Translation Table Columns and Values

Column	Description
IP Range	<p>A translation rule that specifies a range of IP addresses for client systems.</p> <p>To specify IP addresses in a specific range, use the following notation: <i>ip_address-ip_address</i></p> <p>For example: 10.112.116.0-10.112.119.255</p> <p>To specify all of the IP addresses in a specific subnet, use the following notation: <i>ip_address/subnet_mask_bits</i></p> <p>For example: 10.112.4.0/22</p> <p>This notation specifies the usable IPv4 addresses from 10.112.4.1 to 10.112.7.254.</p> <p>Type an asterisk to match any IP address.</p>
Client Name	<p>A translation rule that specifies a computer name.</p> <p>For example: Mary's Computer</p> <p>Type an asterisk to match any computer name.</p>
Mac Address	<p>A translation rule that specifies a MAC address. In the GPO editor, you must use the same format that the client system uses. For example:</p> <ul style="list-style-type: none"> ■ Windows clients use hyphens: 01-23-45-67-89-ab ■ Linux clients use colons: 01:23:45:67:89:ab <p>Type an asterisk to match any MAC address.</p>
User/Group	<p>A translation rule that specifies a user or group name.</p> <p>To specify a particular user or group, use the following notation: <i>\\domain\user_or_group</i></p> <p>For example: \\mydomain\Mary</p> <p>The Fully Qualified Domain Name (FQDN) is not supported notation for the domain name. Type an asterisk to match any user or group name.</p>
Printer Name	<p>The name of the printer when it is mapped to the remote desktop.</p> <p>For example: PRINTER-2-CLR</p> <p>The mapped name does not have to match the printer name on the client system.</p> <p>The printer must be local to the client device. Mapping a network printer in a UNC path is not supported.</p>
Printer Driver	<p>The name of the driver that the printer uses.</p> <p>For example: HP Color LaserJet 4700 PS</p> <p>IMPORTANT Because print jobs are sent directly from the desktop to the printer, the printer driver must be installed on the desktop.</p>
IP Port/ThinPrint Port	<p>For network printers, the IP address of the printer prepended with IP_.</p> <p>For example: IP_10.114.24.1</p> <p>The default port is 9100. You can specify a non-default port by appending the port number to the IP address.</p> <p>For example: IP_10.114.24.1:9104</p>
Default	<p>Indicates whether the printer is the default printer.</p>

You use the buttons that appear above the column headings to add, delete, and move rows and save and import table entries. Each button has an equivalent keyboard shortcut. Mouse over each button to see a description of the button and its equivalent keyboard shortcut. For example, to insert a row at the end of the table, click the first table button or press Alt+A. Click the last two buttons to import and save table entries.

Table 17-21 shows an example of two translation table rows.

Table 17-21. Location-Based Printing Group Policy Setting Example

IP Range	Client Name	Mac Address	User/ Group	Printer Name	Printer Driver	IP Port/ThinPrint Port	Default
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

The network printer specified in the first row will be mapped to a remote desktop for any client system because asterisks appear in all of the translation rule columns. The network printer specified in the second row will be mapped to a remote desktop only if the client system has an IP address in the range 10.112.116.140 through 10.112.116.145.

Active Directory Group Policy Example

One way to implement Active Directory group policies in View is to create an OU for the View machines that deliver remote desktop sessions and link one or more GPOs to that OU. You can use these GPOs to apply group policy settings to your View machines.

You can link GPOs directly to a domain if the policy settings apply to all computers in the domain. As a best practice, however, most deployments should link GPOs to individual OUs to avoid policy processing on all computers in the domain.

You can configure policies on your Active Directory Server or on any computer in your domain. This example shows how to configure policies directly on your Active Directory server.

NOTE Because every View environment is different, you might need to perform different steps to meet your organization's specific needs.

Create an OU for View Machines

To apply group policies to the View machines that deliver remote desktop sessions without affecting other Windows computers in the same Active Directory domain, create an OU specifically for your View machines. You might create one OU for your entire View deployment or separate OUs for single-user machines and RDS hosts.

Procedure

- 1 On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
- 2 Right-click the domain that contains your View machines and select **New > Organizational Unit**.
- 3 Type a name for the OU and click **OK**.
The new OU appears in the left pane.
- 4 To add View machines to the new OU:
 - a Click **Computers** in the left pane.
All the computer objects in the domain appear in the right pane.
 - b Right-click the name of the computer object that represents the View machine in the right panel and select **Move**.
 - c Select the OU and click **OK**.
The View machine appears in the right pane when you select the OU.

What to do next

Create GPOs for View group policies.

Create GPOs for View Group Policies

Create GPOs to contain group policies for View components and location-based printing and link them to the OU for your View machines.

Prerequisites

- Create an OU for your View machines.
- Verify that the Group Policy Management feature is available on your Active Directory server.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.

AD Version	Navigation Path
Windows 2012	Select Server Manager > Tools > Group Policy Management .
Windows 2008	Select Start > Administrative Tools > Group Policy Management .
Windows 2003	<ol style="list-style-type: none"> a Select Start > All Programs > Administrative Tools > Active Directory Users and Computers. b Right-click the OU that contains your View machines and select Properties. c On the Group Policy tab, click Open to open the Group Policy Management plug-in.

- 2 Expand your domain, right-click the OU that contains your View machines, and select **Create a GPO in this domain, and Link it here**.

On Windows 2003 Active Directory, this option is named **Create and Link a GPO Here**.

- 3 Type a name for the GPO and click **OK**.

The new GPO appears under the OU in the left pane.

- 4 (Optional) To apply the GPO only to specific View machines in the OU:

- a Select the GPO in the left pane.
- b Select **Security Filtering > Add**.
- c Type the computer names of the View machines and click **OK**.

The View machines appear in the Security Filtering pane. The settings in the GPO apply only to these machines.

What to do next

Add the View ADM templates to the GPO for group policies.

Add View ADM Templates to a GPO

To apply View component group policy settings to your remote desktops and applications, add their ADM template files to GPOs.

Prerequisites

- Create GPOs for the View component group policy settings and link them to the OU that contains your View machines.
- Verify that the Group Policy Management feature is available on your Active Directory server.

The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See “[Create GPOs for View Group Policies](#),” on page 298.

Procedure

- 1 Download the View 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 View are available in this file.
- 2 Copy the file to your Active Directory server and unzip the file.
- 3 On the Active Directory server, open the Group Policy Management Console.
- 4 Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.
- 5 In the Group Policy Management Editor, right-click the **Computer Configuration > Policies > Administrative Templates: Policy definitions** folder and select **Add/Remove Templates**.
- 6 Click **Add**, browse to the ADM Template file, and click **Open**.
- 7 Click **Close** to apply the policy settings in the ADM Template file to the GPO.
In Windows Server 2012 or 2008 Active Directory, the template name appears in the left pane under **Administrative Templates > Classic Administrative Templates (ADM)**. In Windows Server 2003 Active Directory, the template appears under **Administrative Templates**.
- 8 Configure the group policy settings.

What to do next

Enable loopback processing for your View machines.

Enable Loopback Processing for Remote Desktops

To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, enable loopback processing.

Prerequisites

- Create GPOs for the View component group policy settings and link them to the OU that contains your View machines.
- Verify that the Group Policy Management feature is available on your Active Directory server.

The steps for opening the Group Policy Management Console differ in the Windows 2012, Windows 2008, and Windows 2003 Active Directory versions. See “[Create GPOs for View Group Policies](#),” on page 298.

Procedure

- 1 On the Active Directory server, open the Group Policy Management Console.
- 2 Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.
- 3 In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates: Policy definitions > System > Group Policy**.
- 4 In the right pane, double-click **User Group Policy loopback processing mode**.

- 5 Select **Enabled** and then select a loopback processing mode from the **Mode** drop-down menu.

Option	Action
Merge	The user policy settings applied are the combination of those included in both the computer and user GPOs. Where conflicts exist, the computer GPOs take precedence.
Replace	The user policy is defined entirely from the GPOs associated with the computer. Any GPOs associated with the user are ignored.

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

Configuring User Profiles with View Persona Management

18

With View 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. View 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 View Persona Management and control various aspects of your View Persona Management deployment.

To enable and use View 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 View,”](#) on page 301
- [“Using View Persona Management with Standalone Systems,”](#) on page 302
- [“Migrating User Profiles with View Persona Management,”](#) on page 303
- [“Persona Management and Windows Roaming Profiles,”](#) on page 306
- [“Configuring a View Persona Management Deployment,”](#) on page 306
- [“Best Practices for Configuring a View Persona Management Deployment,”](#) on page 315
- [“View Persona Management Group Policy Settings,”](#) on page 318

Providing User Personas in View

With the View Persona Management feature, a user's remote profile is dynamically downloaded when the user logs in to a View desktop. You can configure View to store user profiles in a secure, centralized repository. View downloads persona information as the user needs it.

View Persona Management is an alternative to Windows roaming profiles. View Persona Management expands functionality and improves performance compared to Windows roaming profiles.

You can configure and manage personas entirely within View. 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 View.

A user profile is independent of the View 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.

View 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, View 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.
- View 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 View Persona Management with Standalone Systems

You can install a standalone version of View Persona Management on physical computers and virtual machines that are not managed by View. With this software, you can manage user profiles across View desktops and standalone systems.

The standalone View 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 View Persona Management software to accomplish these goals:

- Share user profiles across standalone systems and View desktops.

Your users can continue to use standalone systems as well as View desktops with View Persona Management. If you use the same View Persona Management group policy settings to control View desktops and physical systems, users can receive their up-to-date profiles each time they log in, whether they use their legacy computers or View desktops.

NOTE View 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 View desktops

If you intend to re-purpose legacy physical computers for use in a View deployment, you can install standalone View Persona Management on the legacy systems before you roll out View desktops to your users. When users log in to their legacy systems, their profiles are stored on the View remote profile repository. When users log in to their View desktops for the first time, their existing profiles are downloaded to their View desktops.

- Perform a staged migration from physical systems to View desktops

If you migrate your deployment in stages, users who do not yet have access to View desktops can use standalone View Persona Management. As each set of View desktops is deployed, users can access their profiles on their View 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, View 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 View Persona Management

With View Persona Management, you can migrate existing user profiles in a variety of settings to View desktops. When users log in to their View 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 View desktops to Windows 10 View 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 View for the first time.
- You can upgrade legacy Windows XP View desktops to Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops.
- You can migrate from physical computers to View desktops without upgrading the operating systems.

To support these scenarios, View Persona Management provides a profile migration utility and a standalone View 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 View 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 View Connection Server 6.1.

With the View 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 View releases.

[Table 18-1](#) shows various migration scenarios and outlines the tasks you should perform in each scenario.

Table 18-1. 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 View desktops	Windows 10 View desktops	<ol style="list-style-type: none"> 1 Configure the Windows 10 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 306. NOTE Do not roll out the Windows 10 View desktops to your users until you complete step 2. 2 Run the View V2 to V5 profile migration utility. <ul style="list-style-type: none"> ■ For the source profiles, specify the remote profile repository for existing Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops. ■ For the destination profiles, specify the remote profile repository that you configured for the Windows 10 View desktops. <p>For details, see the <i>View User Profile Migration</i> document.</p> 3 Allow your users to log in to their Windows 10 View desktops.
Windows XP physical computers	Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops	<ol style="list-style-type: none"> 1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 306. NOTE Do not roll out the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops to your users until you complete step 2. 2 Run the View V1 to V2 profile migration utility. <ul style="list-style-type: none"> ■ 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 View deployment. <p>For details, see the <i>View User Profile Migration</i> document.</p> 3 Allow your users to log in to their Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops.

Table 18-1. User Profile Migration Scenarios (Continued)

If This Is Your Original Deployment...	And This Is Your Destination Deployment...	Perform These Tasks:
<p>Windows XP physical computers or virtual machines that use a roaming user profile solution. For example, your deployment might use one of these solutions:</p> <ul style="list-style-type: none"> ■ View Persona Management ■ RTO Virtual Profiles ■ Windows roaming profiles <p>In this scenario, the original user profiles must be maintained in a remote profile repository.</p>	<p>Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops</p>	<ol style="list-style-type: none"> 1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 306. <p>NOTE Do not roll out the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops to your users until you complete step 2.</p> 2 Run the View V1 to V2 profile migration utility. <ul style="list-style-type: none"> ■ 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 View deployment. <p>For details, see the <i>View User Profile Migration</i> document.</p> 3 Allow your users to log in to their Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops.
<p>Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 physical computers or virtual machines.</p> <p>The legacy systems cannot have View Agent 5.x installed.</p>	<p>Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops</p>	<ol style="list-style-type: none"> 1 Configure Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 306. 2 Install the standalone View Persona Management software on the Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 systems. See “Install Standalone View Persona Management,” on page 309. 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 View desktops. See “Configure a User Profile Repository,” on page 307. <p>The easiest approach is to use the same View Persona Management group policy settings in Active Directory to control both the legacy systems and the View desktops. See “Add the View Persona Management ADM Template File,” on page 310.</p> 4 Roll out your Windows 7, Windows 8, Windows Server 2008 R2, or Windows Server 2012 R2 View desktops to your users.

Persona Management and Windows Roaming Profiles

When Persona Management is enabled, you cannot manage View 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**, View 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 View Persona Management. You use the **Windows Roaming Profiles Synchronization** policy to specify these files and folders.

Configuring a View Persona Management Deployment

To configure View Persona Management, you set up a remote repository that stores user profiles, install Horizon Agent with the **View Persona Management** setup option on virtual machines that deliver remote desktop sessions, add and configure View Persona Management group policy settings, and deploy desktop pools.

You can also configure View Persona Management for a non-View deployment. You install the standalone version of View Persona Management on your users' non-View laptops, desktops, or virtual machines. You must also set up a remote repository and configure View Persona Management group policy settings.

Overview of Setting Up a View Persona Management Deployment

To set up a View desktop deployment or standalone computers with View 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 **View Persona Management** setup option on the virtual machines that you use to create desktop pools.

To configure View Persona Management for non-View laptops, desktops, or virtual machines, install the standalone View Persona Management software on each computer in your targeted deployment.

- 3 Add the View Persona Management Administrative (ADM) Template file to your Active Directory server or the Local Computer Policy configuration on the parent virtual machine.

To configure View Persona Management for your whole View or non-View deployment, add the ADM Template file to Active Directory.

To configure View Persona Management for one desktop pool, you can take these approaches:

- Add the ADM Template file to the virtual machine that you use to create the pool.
- Add the ADM Template file to Active Directory and apply the group policy settings to the OU that contains the machines in the pool.

- 4 Enable View 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 **View 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 View 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 View Persona Management,”](#) on page 307.
- Familiarize yourself with the guidelines for creating a user profile repository. See [“Creating a Network Share for View Persona Management,”](#) on page 308

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, View 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 View Persona Management.

Setting Access Permissions on Shared Folders for View Persona Management

View Persona Management and Windows roaming profiles require a specific minimum level of permissions on the user profile repository. View 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 18-2. 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 18-3. 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](http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx)

Creating a Network Share for View 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 View 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 View 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 View 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 View Persona Management Option

To use View Persona Management with View desktops, you must install Horizon Agent with the **View 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 **View 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 View Persona Management software is deployed on your View desktops.

For a manual pool, you must install Horizon Agent with the **View Persona Management** setup option on each virtual machine that is used as a desktop in the pool. Use Active Directory to configure View Persona Management group policies for a manual pool. The alternative is to add the ADM 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. View Persona Management does not operate on Microsoft RDS hosts.

Installing Horizon Agent with the **View Persona Management** setup option does not work on physical computers. You can install the standalone View Persona Management software on physical computers. See [“Install Standalone View Persona Management,”](#) on page 309.

- 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 **View Persona Management** setup option.
- Familiarize yourself with installing Horizon Agent. See [“Install Horizon Agent on a Virtual Machine,”](#) on page 26 or [“Install Horizon Agent on an Unmanaged Machine,”](#) on page 16.

Procedure

- ◆ When you install Horizon Agent on a virtual machine, select the **View Persona Management** setup option.

What to do next

Add the View Persona Management ADM Template file to your Active Directory server or the Local Computer Policy configuration on the virtual machine itself. See [“Add the View Persona Management ADM Template File,”](#) on page 310.

Install Standalone View Persona Management

To use View Persona Management with non-View physical computers or virtual machines, install the standalone version of View Persona Management. You can run an interactive installation or a silent installation at the command line.

Install the standalone View 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. View 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 View 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 View 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	<ol style="list-style-type: none"> a To start the installation program, double-click the installer file. b Accept the VMware license terms. c Click Install. <p>By default, View Persona Management is installed in the C:\Program Files\VMware\VMware View Persona Management directory.</p> <ol style="list-style-type: none"> d Click Finish.
Silent installation	<p>Open a Windows command prompt on the machine and type the installation command on one line.</p> <p>For example: VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"</p> <p>IMPORTANT You must include the ALLUSERS=1 property in the command line.</p>

- 3 Restart your system to allow the installation changes to take effect.

What to do next

Add the View Persona Management ADM Template file to your Active Directory or local group policy configuration.

Add the View Persona Management ADM Template File

The View Persona Management Administrative (ADM) Template file contains group policy settings that allow you to configure View Persona Management. Before you can configure the policies, you must add the ADM Template file to the local systems or Active Directory server.

To configure View 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 View 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 View Persona Management at the domain-wide level and apply the configuration to many View 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 View machines that use View Persona Management, create one or more GPOs, and link the GPOs to the OU. To configure separate View Persona Management policies for different types of users, you can create OUs for particular sets of View machines and apply different GPOs to the OUs.

For example, you might create one OU for View machines with View Persona Management and another OU for physical computers on which the standalone View Persona Management software is installed.

For an example of implementing Active Directory group policies in View, see “[Active Directory Group Policy Example](#),” on page 297.

Add the Persona Management ADM Template to a Single System

To configure View Persona Management for a single desktop pool, you must add the Persona Management ADM Template file to the Local Computer Policy on the virtual machine that you use to create the pool. To configure View Persona Management on a single system, you must add the Persona Management ADM Template file to that system.

Prerequisites

- Verify that Horizon Agent is installed with the View Persona Management setup option on the system. See “[Install Horizon Agent with the View Persona Management Option](#),” on page 309.
- Verify that you can log in as an administrator on the system.

Procedure

- 1 Download the View 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-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.

- 2 Unzip the file and copy the 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` file and click **Add**.
- 9 Close the Add/Remove Templates window.

The View 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 View Persona Management group policy settings on the local system. See “[Configure View Persona Management Policies](#),” on page 312.

Add the Persona Management ADM Template to Active Directory

To configure View 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 View Persona Management deployment and link them to the OU that contains the View machines that use View Persona Management. See “[Active Directory Group Policy Example](#),” on page 297.
- 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 View Persona Management setup option on a system that is accessible to your Active Directory server. See “[Install Horizon Agent with the View Persona Management Option](#),” on page 309.

Procedure

- 1 Download the View 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-yyyyyy.zip`, where `x.x.x` is the version and `yyyyyy` is the build number. All ADM and ADMX files that provide group policy settings for View are available in this file.
- 2 Unzip the file and copy the View Persona Management ADM Template 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 View 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` file, 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 View Persona Management group policy settings on your Active Directory server.

Configure View Persona Management Policies

To use View Persona Management, you must enable the **Manage user persona** group policy setting, which activates the View 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 View 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 319.
- 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 Persona Management ADM Template to a Single System,”](#) on page 311.
- 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 Persona Management ADM Template to Active Directory,”](#) on page 312.

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 View Persona Management. When this setting is disabled or not configured, View Persona Management does not function.

- 5 Type the profile upload interval, in minutes, and click **OK**.

The profile upload interval determines how often View 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 View Persona Management group policy settings.

Create Desktop Pools That Use Persona Management

To use View Persona Management with View desktops, you must create desktop pools with a View Persona Management agent installed on each machine.

You cannot use View Persona Management on RDS desktop pools, which run on Remote Desktop Services (RDS) hosts.

Prerequisites

- Verify that Horizon Agent with the **View Persona Management** setup option is installed on the virtual machine that you use to create the desktop pool. See [“Install Horizon Agent with the View Persona Management Option,”](#) on page 309.
- If you intend to configure View Persona Management policies for this desktop pool only, verify that you added the View Persona Management ADM Template file to the virtual machine and configured group policy settings in the Local Computer Policy configuration. See [“Add the Persona Management ADM Template to a Single System,”](#) on page 311 and [“Configure View Persona Management Policies,”](#) on page 312.

Procedure

- Generate a snapshot or template from the virtual machine and create an automated desktop pool.

You can configure View Persona Management with pools that contain full virtual machines or linked clones. The pools can use dedicated or floating assignments.

- (Optional) To use View Persona Management with manual desktop pools, select machines on which Horizon Agent with the **View Persona Management** option is installed.

NOTE After you deploy View Persona Management on your View desktop pools, if you remove the **View Persona Management** setup option on the View 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 View Persona Management Deployment

You should follow best practices for configuring View Persona Management to enhance your users' desktop experience, improve desktop performance, and ensure that View Persona Management operates efficiently with other View features.

Determining Whether to Remove Local User Profiles at Logoff

By default, View 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, View 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 View Persona Management and Windows Roaming Profiles

In deployments in which Windows roaming profiles are configured, and users access View desktops with View Persona Management and standard desktops with Windows roaming profiles, the best practice is to use different profiles for the two desktop environments. If a View 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 View 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 View Persona Management profile when the user logs off from the client computer.

If users intend to share data between existing Windows roaming profiles and View 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 View Persona Management Deployment

To help you manage your deployment, View Persona Management provides improved log messages and profile size and file and folder count tracking. View 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 View Persona Management stores the profile repository.

NOTE Do not use backup software such as MozyPro or Windows Volume backup services with View Persona Management to back up user profiles on View desktops.

View 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 View Persona Management and cause data loss or corruption.

- You can set View Persona Management policies to enhance performance when users start ThinApp applications. See [“Configuring User Profiles to Include ThinApp Sandbox Folders,”](#) on page 317.
- 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 View Persona Management. See [“Configuring View Composer Persistent Disks with View Persona Management,”](#) on page 317.
- If you configure View 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 317.
- Do not use Windows Client-Side Caching with View 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, View 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 View Persona Management. If you encounter issues with View 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

View Persona Management maintains user settings that are associated with ThinApp applications by including ThinApp sandbox folders in user profiles. You can set View Persona Management policies to enhance performance when users start ThinApp applications.

View 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, View 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 319.

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 View 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 View Persona Management when users generate a large amount of persona information. You can configure persistent disks only with dedicated-assignment, linked-clone desktops.

View 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 View 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, View 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 View Persona Management on standalone (non-View) 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 View 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 View 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 View Persona Management is configured for your users' standalone laptops. See [“Configuring a View Persona Management Deployment,”](#) on page 306.

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-View 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.

View Persona Management Group Policy Settings

The View Persona Management ADM Template file contains 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 View Persona Management.

The ADM Template file is named `ViewPM.adm`.

This ADM file is available in a bundled `.zip` file named `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.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.adm` file to your Group Policy configuration, the policy settings are located in the **Persona Management** folder in the Group Policy window.

Table 18-4. Location of View 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 View 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	<p>Determines whether to manage user profiles dynamically with View Persona Management or with Windows roaming profiles. This setting turns View Persona Management on and off.</p> <p>When this setting is enabled, View Persona Management manages user profiles.</p> <p>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.</p> <p>When this setting is disabled or not configured, user profiles are managed by Windows.</p>
Persona repository location	<p>Specifies the location of the user profile repository. This setting also determines whether to use a network share that is specified in View Persona Management or a path that is configured in Active Directory to support Windows roaming profiles.</p> <p>When this setting is enabled, you can use the Share path to determine the location of the user profile repository.</p> <p>In the Share path text box, you specify a UNC path to a network share that is accessible to View Persona Management desktops. This setting lets View Persona Management control the location of the user profile repository.</p> <p>For example: <code>\\server.domain.com\VPRepository</code></p> <p>If <code>%username%</code> is not part of the folder path that you configure, View Persona Management appends <code>%username%.%userdomain%</code> to the path.</p> <p>For example: <code>\\server.domain.com\VPRepository\%username%.%userdomain%</code></p> <p>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.</p> <p>For details about configuring a UNC network share for View Persona Management, see “Configure a User Profile Repository,” on page 307.</p> <p>By default, the Active Directory user profile path is used.</p> <p>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.</p> <p>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 View Persona Management uses the path specified in the Share path. By default, this check box is unchecked, and View Persona Management uses the Active Directory user profile path when both locations are configured.</p>
Remove local persona at log off	<p>Deletes each user's locally stored profile from the View machine when the user logs off.</p> <p>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 <code>AppData\Local</code> folder.</p> <p>For guidelines for using this setting, see “Best Practices for Configuring a View Persona Management Deployment,” on page 315.</p> <p>When this setting is disabled or not configured, the locally stored user profiles, including local settings folders, are not deleted when users log off.</p>
Roam local settings folders	<p>Roams the local settings folders with the rest of each user profile.</p> <p>This policy affects the <code>AppData\Local</code> folder.</p> <p>By default, local settings are not roamed.</p>

Group Policy Setting	Description
Files and folders to preload	<p>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.</p> <p>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.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname. For example: <code>Application Data\Microsoft\Certificates</code></p> <p>After the specified files and folders are preloaded, View 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, View Persona Management copies the updated data to the remote profile repository during the session, at the next profile upload interval.</p>
Files and folders to preload (exceptions)	<p>Prevents the specified files and folders from being preloaded.</p> <p>The selected folder paths must reside within the folders that you specify in the Files and folders to preload setting.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Windows roaming profiles synchronization	<p>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.</p> <p>For the specified files and folders, View Persona Management ignores the profile replication interval that is configured by the Profile upload interval in the Manage user persona setting.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Windows roaming profiles synchronization (exceptions)	<p>The selected files and folders are exceptions to the paths that are specified in the Windows roaming profiles synchronization setting.</p> <p>The selected folder paths must reside within the folders that you specify in the Windows roaming profiles synchronization setting.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Files and folders excluded from roaming	<p>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.</p> <p>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.</p> <p>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.</p>
Files and folders excluded from roaming (exceptions)	<p>The selected files and folders are exceptions to the paths that are specified in the Files and folders excluded from roaming setting.</p> <p>The selected folder paths must reside within the folders that you specify in the Files and folders excluded from roaming setting.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Enable background download for laptops	<p>Downloads all files in the user profile when a user logs in to a laptop on which the View Persona Management software is installed. Files are downloaded in the background.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>See “Manage User Profiles on Standalone Laptops,” on page 317.</p>

Group Policy Setting	Description
Folders to background download	<p>The selected folders are downloaded in the background after a user logs in to the desktop.</p> <p>In certain cases, you can optimize View 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.</p> <p>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.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Folders to background download (exceptions)	<p>The selected folders are exceptions to the paths that are specified in the Folders to background download setting.</p> <p>The selected folder paths must reside within the folders that you specify in the Folders to background download setting.</p> <p>Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.</p>
Excluded processes	<p>The I/O of the specified processes are ignored by View Persona Management.</p> <p>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, View Persona Management does replicate changes to files and settings in the users' profiles that are made by excluded processes.</p> <p>To add processes to the Excluded processes list, enable this setting, click Show, type the process name, and click OK. For example: process.exe.</p>
Cleanup CLFS files	<p>Deletes the files that are generated by Common Log File System (CLFS) for <code>ntuser.dat</code> and <code>usrclass.dat</code> from the roaming profile on logon.</p> <p>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.</p>

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. View 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, View 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 315.
- You configure a separate setting for each folder. You can select particular folders for redirection and leave others on the local View 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 View desktop and managed according to the View Persona Management group policy settings.
- If View Persona Management and Windows roaming profiles are configured to redirect the same folder, View 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 View 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, View 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 18-5](#).

For existing redirected folders, see [“Granting Domain Administrators Access to Existing Redirected Folders,”](#) on page 323.

You can specify folder paths that are excluded from folder redirection. See [Table 18-5](#).



CAUTION View does not support enabling folder redirection to a folder that is already in a profile managed by View Persona Management. This configuration can cause failures in View 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 View 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 18-5. 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 18-5](#).

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 View 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 View 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 View Persona Management log files.

View Persona Management logging configuration is simplified in Horizon 6 version 6.1 and later releases. To use the updated logging settings, you must upgrade the View Persona Management ADM file, `ViewPM.adm`, to the version that is provided with Horizon 6 version 6.1 with View or later.

Group Policy Setting	Description
Logging filename	Specifies the full pathname of the local View Persona Management log file. The default path is <code>ProgramData\VMware\VDM\logs\filename</code> . The default logging filename is <code>VMWVp.txt</code> .
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. <ul style="list-style-type: none"> ■ 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 View 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 View 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. View 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

19

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,”](#) on page 327
- [“Send Messages to Desktop Users,”](#) on page 328
- [“Problems Provisioning or Recreating a Desktop Pool,”](#) on page 328
- [“Troubleshooting Network Connection Problems,”](#) on page 339
- [“Troubleshooting USB Redirection Problems,”](#) on page 342
- [“Manage Machines and Policies for Unentitled Users,”](#) on page 344
- [“Resolving Database Inconsistencies with the ViewDbChk Command,”](#) on page 344
- [“Further Troubleshooting Information,”](#) on page 347

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 334.
- 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 332.
- 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 View Connection Server Instances,”](#) on page 339.
- 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.

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 Provisioning 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.

- 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
```

- Restart the View Composer service.
- (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 19-1](#) 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 19-1. 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 19-1. View Composer Provisioning Errors (Continued)

Error	Description
6	<p>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.</p> <p>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.</p> <p>PnP mounts up to three disks, depending on how the pool was configured:</p> <ul style="list-style-type: none"> ■ 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. <p>The timeout length is 10 minutes. If PnP does not finish mounting the disks within 10 minutes, View Composer fails with error code 6.</p>
7	<p>Too many View Composer persistent disks are attached to the linked clone. A clone can have at most three View Composer persistent disks.</p>
8	<p>A persistent disk could not be mounted on the datastore that was selected when the pool was created.</p>
9	<p>View Composer could not redirect disposable-data files to the nonpersistent disk. Either the paging file or the temp-files folders were not redirected.</p>
10	<p>View Composer cannot find the QuickPrep configuration policy file on the specified internal disk.</p>
12	<p>View Composer cannot find the internal disk that contains the QuickPrep configuration policy file and other OS-related data.</p>
13	<p>More than one persistent disk is configured to redirect the Windows user profile.</p>
14	<p>View Composer failed to unmount the internal disk.</p>
15	<p>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.</p>
16	<p>The View Composer agent did not start because the volume license for the guest OS was not activated.</p>
17	<p>The View Composer agent did not start. The agent timed out while waiting for Sysprep to start.</p>
18	<p>The View Composer agent failed to join the linked-clone virtual machine to a domain during customization.</p>
19	<p>The View Composer agent failed to execute a post-synchronization script.</p>
20	<p>The View Composer agent failed to handle a machine password synchronization event.</p> <p>This error might be transient. If the linked clone joins the domain, the password is fine.</p> <p>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.</p>
21	<p>The View Composer agent failed to mount the system disposable disk.</p>
22	<p>The View Composer agent failed to mount the View Composer persistent disk.</p>

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 View Connection Server Instances

You might experience connection problems between machines and View Connection Server instances.

Problem

If connectivity between a machine and a View 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 View Connection Server instance can occur for different reasons.

- Lookup failure on the machine for the DNS name of the View Connection Server host.
- The ports for JMS, RDP, or AJP13 communication being blocked by firewall rules.
- The failure of the JMS router on the View 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 View Connection Server host. If the command fails to return the IP address of the View 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 View 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 View 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 View 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 View desktops. The initial login to a security server or View Connection Server instance succeeds, but the connection fails when the user selects a View desktop. This issue occurs when the PCoIP Secure Gateway is configured on a security server or View 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 View Connection Server host, the PCoIP Secure Gateway can also be configured on View 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 View 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 View Connection Server host. When you configure these addresses on a security server or View 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 View 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 View 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 View Connection Server host.

Port	Description
TCP 4172	From Horizon Client to the security server or View Connection Server host.
UDP 4172	Between Horizon Client and the security server or View Connection Server host, in both directions.
TCP 4172	From the security server or View Connection Server host to the View desktop.
UDP 4172	Between the security server or View Connection Server host and the View desktop, in both directions.

- In View Administrator, make sure that the PCoIP Secure Gateway is enabled.
 - a Click **View Configuration > Servers**.
 - b Select the View 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 View 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 View 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 View 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 View Connection Server Settings dialog must allow client systems to reach this View Connection Server instance.
 - f Click **OK**.
Repeat these steps for each security server and View 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 View Connection Server Instances

You might experience connection problems between machines and View Connection Server instances.

Problem

If connectivity between a machine and a View 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 View Connection Server instance can occur for different reasons.

- Lookup failure on the machine for the DNS name of the View Connection Server host.

- The ports for JMS, RDP, or AJP13 communication being blocked by firewall rules.
- The failure of the JMS router on the View 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 View Connection Server host. If the command fails to return the IP address of the View 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 View 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 View 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](#),” on page 221.
- 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 HID devices 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 HID devices, 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,”](#) on page 219.
- 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
<code>--findDesktop</code>	Finds a desktop pool or farm.
<code>--enableDesktop</code>	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

Numerics

3D renderer, configuring **145, 148, 150**

A

access permissions, shared folders for Persona Management **307**

Active Directory, using existing computer accounts for linked clones **76**

ADM Template file

adding to a local system **311**

adding to Active Directory **312**

installing **310**

ADM template file

Real-Time Audio-Video **194**

scanner redirection **199**

serial port redirection **205**

ADM template files

Horizon Agent Configuration **266**

PCoIP Session Variables **271**

PCoIP session bandwidth settings **279**

View components **264**

VMware Blast **282**

where to find **264**

ADMX files, adding to Active Directory **284**

Adobe Flash

quality modes **139**

throttling modes **139**

Adobe Flash Throttling Throttling, RDS desktop pools **125**

Adobe Flash URL redirection, system requirements **169**

Always on policy **140**

AMD Multiuser GPU using vDGA **150, 154**

application compatibility, RDS group policy settings **285**

application pools

advantages **14**

creating **119, 120**

introduction **9**

worksheet for creating **120**

application sessions, time zone redirection **102**

applications, enable Windows basic theme **102**

automated desktop pools

adding machines manually **132**

assigning multiple network labels **158**

cloning **56, 69**

creating **51, 55**

customizing machines in maintenance mode **134**

deploying large pools **157**

desktop settings **57, 135**

machine-naming example **131**

maintenance mode **133, 134**

naming machines manually **128, 129**

power policies **142–144**

using a machine-naming pattern **128**

worksheet for creating **51**

automated farm creation, storing swap files **108**

automated farms, preparing a parent virtual machine **108**

automatic Windows updates, disabling **42**

B

bandwidth, Real-Time Audio-Video **196**

base image for virtual desktops **233, 240**

best practices, View Persona Management **315**

blackout times

for disk space reclamation **254**

for View Storage Accelerator **254**

C

CBRC, configuring for desktop pools **250**

client devices, setting up for Flash URL Redirection **171**

client drive redirection **211, 212**

client session policies

configuring global **256**

configuring pool-level **256**

configuring user-level **256**

defined **255**

general **257**

inheritance **255**

client systems, passing information to desktops **268**

ClonePrep, increasing timeout limit for customization scripts **49**

cloning, preparing a virtual machine for **19**

cluster, more than eight hosts **157**

COM ports, redirecting serial **202**

command scripts, running on desktops **271**

CommandsToRunOnConnect group policy setting **271**

composite USB devices **221**

configuring RDS per device CAL **283**

- connection issues
 - between Horizon Client and the PCoIP Secure Gateway **340**
 - between machines and View Connection Server **339, 341**
 - linked-clone machines with static IP addresses **342**
- connection ticket timeout **266**
- connections, troubleshooting **339**
- custom setup options
 - Horizon Agent **17, 28**
 - installing Horizon Agent on an RDS host **100**
- customization specifications
 - creating **50**
 - recomposing linked-clone machines **75**
- customization scripts
 - increasing ClonePrep and QuickPrep timeout limits **49**
 - using QuickPrep for linked-clone machines **73**
- customizing machines, maintenance mode **133**

D

- datastores
 - local storage **248**
 - sizing linked-clone pools **241**
 - storage sizing table **241**
 - storing linked clones and replicas **249**
- dedicated-assignment desktop pools **10, 240**
- dedicated-assignment pools
 - choosing a user assignment type **127**
 - maintenance mode **134**
- defragmentation, disabling on linked clones **41**
- delta disks, storage overcommit **245**
- Desktop Experience feature
 - install on Windows Server 2008 R2 **25, 98**
 - install on Windows Server 2012 or 2012 R2 **25, 98**
- desktop pool managementdesktop pool management, reclaiming disk space **251**
- desktop pool creation
 - choosing a user assignment type **127**
 - customizing in maintenance mode **134**
 - deploying large pools **157**
 - machine-naming example **131**
 - on more than 8 hosts **157**
 - provisioning options **127**
 - with Persona Management **314**
- desktop pool troubleshooting
 - cannot delete orphaned instant clones **329**
 - cloning failure **331**
 - creation problems **328**
 - customization failure **332**
 - endless error recovery during instant-clone provisioning **329**

- failure due to configuration problems **330**
- failure due to missing customization specifications **330**
- failure due to permissions problems **330**
- failure due to vCenter being overloaded **332**
- free disk space problems **331**
- inability to connect to vCenter **331**
- inability to log in to vCenter **331**
- instant clone image publish failure **329**
- instant-clone provisioning or push image failure **328**
- resource problems **331**
- timeout while customizing **332**
- vCenter status unknown **331**
- virtual machines stuck in Provisioning state **332**
- desktop pools, introduction **9**
- desktop settings
 - automated desktop pools **57, 135**
 - linked-clone desktops **70**
 - manual desktop pools **135**
 - RDS desktop pools **124, 135**
- desktop sources, preparing for desktop deployment **19**
- desktop UI, group policy settings **324**
- device families **226**
- Diagnostic Policy Service, disabling **42**
- disposable file redirection, paging-file size **48**
- disposable-data disks, linked-clone virtual machines **247**
- Do nothing policy **140**

E

- entitlements
 - adding to desktop pools **159**
 - adding to desktop or application pools **159**
 - removing from desktop or application pools **160**
 - restricting **160**
 - reviewing **160**
- esxcfg-module command **155**
- ESXi hosts, using more than eight in a cluster **157**

F

- farms
 - creating **107**
 - creating a manual farm **116**
 - creating an automated farm **117**
 - introduction **9**
 - worksheet for creating a manual farm **111**
 - worksheet for creating an automated farm **112**
- Favorite Applications, configuring **166**
- Fibre Channel SAN arrays **233**

- Flash Redirection **172–174, 176**
 - Flash URL Redirection
 - configuring **168**
 - disabling **172**
 - enabling **172**
 - setting up clients **171**
 - system requirements **169**
 - verifying installation **170**
 - floating-assignment desktop pools **10**
 - floating-assignment pools
 - choosing a user assignment type **127**
 - maintenance mode **134**
 - folder redirection
 - granting domain administrator rights **323**
 - group policy settings **321**
- G**
- global policies, configuring **256**
 - GPOs
 - creating for desktops **298**
 - creating for View component policies **263**
 - gpupvm utility, examining GPU resources **156**
 - graphics, 3D renderer **145, 148, 150**
 - GRID vGPU **148**
 - GRID vGPU, NVIDIA **145, 150, 153**
 - group policies
 - ADM template files **264**
 - applying to GPOs **298**
 - examples **297**
 - Horizon Agent configuration **266**
 - Remote Desktop Services **283**
 - URL Content Redirection **179, 180**
 - View components **264**
 - group policies for desktop pools **255**
 - group policy settings
 - adding RDS ADMX files **284**
 - adding to a local system **311**
 - adding to Active Directory **312**
 - desktop UI settings **324**
 - folder redirection **321**
 - logging **324**
 - manage user persona **319**
 - persona repository location **319**
 - Real-Time Audio-Video **195**
 - roaming and synchronization **319**
 - runonce.exe **103**
 - scanner redirection **200**
 - View Persona Management **318**
 - guest operating systems
 - installing **22**
 - optimizing performance **37**
 - paging-file size **48**
 - preparing for desktop deployment **22**
 - GUIDs, support in View Composer **71**
- H**
- Horizon agent, installing on a virtual machine **26**
 - Horizon Agent
 - configuring multiple NICs **36**
 - custom setup options on an RDS host **100**
 - custom setup options **17, 28**
 - installing silently **30**
 - installing on unmanaged machines **16**
 - silent installation properties **33**
 - with View Persona Management **309**
 - Horizon Client, connection problems to the
 - PCoIP Secure Gateway **340**
 - host caching, for desktop pools **250**
- I**
- IcMaint.cmd **87**
 - IcUnprotect.cmd **87**
 - individual desktops, creating **92**
 - installation
 - guest operating system **22**
 - Horizon agent **26**
 - Horizon Agent **16, 30**
 - silent **30**
 - silent installation options **31**
 - standalone View Persona Management **309**
 - instant clone Agent, Horizon Agent custom setup
 - option **28**
 - instant clones
 - domain administrator **81**
 - maintenance utilities **87**
 - instant-clone desktop pools
 - creating **79, 85**
 - understanding **79**
 - worksheet for creating **81**
 - Intel vDGA **150**
 - IOPS
 - benefits of disabling Windows 7 services **39**
 - benefits of disabling Windows 8 services **39**
 - IP addresses, troubleshooting for linked-cloned
 - machine connections **342**
 - iSCSI SAN arrays **233**
- K**
- keyboard settings, PCoIP session variables **281**
 - kiosk mode **13**
 - KMS license keys, volume action on linked
 - clones **47, 110**
 - Knowledge Base articles, where to find **347**
 - knowledge workers **12**

L

- laptops
 - installing View Persona Management **302**
 - Persona Management configuration **317**
- licensing, RDS group policy settings **287**
- linked clones **240**
- linked-clone desktop creation
 - cloning a pool **56, 69**
 - desktop settings **70**
 - storage sizing **241**
 - understanding **59**
 - using View Composer **67**
 - worksheet for creating **59**
- linked-clone desktop pools **59**
- linked-clone desktop pool creation, storing swap files **45**
- linked-clone machine creation
 - choosing a naming pattern **130**
 - choosing QuickPrep or Sysprep **72**
 - customizing **72**
 - data disk creation **247**
 - setting minimum ready machines **75**
 - setting the storage overcommit level **246**
 - storage overcommit feature **245**
 - storage sizing table **241, 243**
 - storing replicas and linked clones on separate datastores **249**
 - storing swap files **48**
 - support for unique SIDs **71**
 - using existing AD computer accounts **76**
 - using local datastores **248**
 - Windows 7 volume activation **47**
 - Windows 7 volume activation **47**
- linked-clone machine troubleshooting
 - connection problems **342**
 - deleting orphaned clones **333**
 - provisioning error codes **337**
 - repeated deletions **334**
- linked-clone RDS hosts creation, Windows Server volume activation **110**
- Linux Thin clients, setting up for Flash URL Redirection **171**
- local datastore, linked-clone swap files **45, 48, 108**
- location-based printing
 - configuring **292**
 - group policy **292, 294, 295**
 - registry key **292**
 - TPVMGPoACmap.dll file **294**
- logging, group policy settings **324**
- loopback processing
 - benefits **264**
 - enabling **299**
- LSI20320-R controllers, installing driver **22**

LUNs 240**M**

- machine recomposition, Sysprep **75**
 - machine settings, manual desktop pools **93**
 - machine troubleshooting
 - connection issues **339, 341**
 - displaying orphaned machines **344**
 - displaying problem machines **327**
 - repeated deletions **334**
 - maintenance mode
 - customizing machines **134**
 - starting machines **133, 134**
 - manage user persona
 - configuring **312**
 - group policy settings **319**
 - manual desktop pools
 - configuring a single machine **92**
 - creating **89, 91**
 - desktop settings **135**
 - machine settings **93**
 - worksheet for creating **89**
 - messages, sending to desktop users **328**
 - MHTML Web pages, setting up for multicast **171**
 - microphone **186, 187, 191**
 - microphones, selecting default **186**
 - Microsoft Feeds Synchronization
 - disabling on Windows 7 **44**
 - disabling on Windows 8 **44**
 - Microsoft Windows Defender
 - disabling in Windows 8 **44**
 - disabling in Windows 7 **44**
 - Microsoft Windows Installer, properties for Horizon Agent **33**
 - migrating, user profiles **303**
 - MMR, system requirements **209**
 - multicast redirection
 - configuring **168**
 - system requirements **169**
 - multimedia redirection
 - enabling **209**
 - managing across a network **209**
 - network latency **210**
 - override network latency trigger **210**
 - system requirements **209**
 - multiple NICs, configuring for Horizon Agent **36**
- N**
- naming desktop pools
 - example **131**
 - manually specifying names **129**
 - naming machines
 - manually specifying names **128**
 - providing a naming pattern **128**
 - naming patterns, linked-clone machines **130**
 - NAS arrays **233**

- NAS devices, native NFS snapshots **253**
- network connections, troubleshooting **339**
- network labels, configuring for a pool **158**
- network share
 - access permissions for Persona Management **307**
 - guidelines for creating **308**
- NFS datastores, clusters with more than eight hosts **157**
- NVIDIA GRID vGPU **145, 148, 150**
- O**
- orphaned machines, displaying **344**
- OS disks
 - disabling Windows 7 services **39**
 - disabling Windows 8 services **39**
 - growth caused by Windows 7 services **39**
 - growth caused by Windows 8 services **39**
 - linked-clone virtual machines **247**
 - storage overcommit **246**
 - storage sizing formulas for editing pools **243, 244**
- OS_DISKpolicy profile **237**
- OUs, creating for remote desktops **263, 297**
- P**
- paging-file size, parent virtual machine **48**
- parent virtual machines
 - disabling hibernation **47, 110**
 - disabling defragmentation on Windows 7 **41**
 - disabling defragmentation on Windows 8 **41**
 - disabling Windows 7 services **39**
 - preparing **45**
 - preparing for View Composer **45**
- parent virtual machine **240**
- PCoIP Agent, Horizon Agent feature **100**
- PCoIP Profile setting **259**
- PCoIP Secure Gateway, connection problems **340**
- PCoIP Server, Horizon Agent custom option **28**
- PCoIP session variables
 - build-to-lossless feature **281**
 - general session variables **272**
 - group policy settings **271**
 - keyboard settings **281**
 - session bandwidth settings **279**
- pcoip.adm, ADM template files **264**
- performance optimization, guest operating system **37**
- persistent disks
 - creating **59**
 - linked-clone desktops **247**
 - Persona Management **317**
 - storage sizing formulas for editing pools **243, 244**
- PERSISTENT_DISK policy profile **237**
- Persona Management
 - best practices **315**
 - configuration overview **306**
 - configuring a deployment **306**
 - configuring and managing **301**
 - creating desktop pools **314**
 - enabling **312**
 - Horizon Agent installation option **309**
 - migrating user profiles **303**
 - setting the repository location **312**
 - standalone installation **309**
 - standalone laptops **317**
 - standalone systems **302**
 - View Composer persistent disks **317**
 - Windows roaming profiles **306**
 - with View **301**
- persona repository location, group policy settings **319**
- physical computers
 - installing Horizon Agent **16**
 - preparing for desktop delivery **15**
- policies
 - Active Directory **263**
 - automated pools **142**
 - client session **255**
 - client session inheritance **255**
 - configuring persona management **301**
 - displaying unentitled **344**
 - general client session **257**
 - global **256**
 - pool-level **256**
 - power **140, 142**
 - user-level **256**
- pools
 - desktop **11, 240**
 - kiosk users **13**
 - knowledge workers **12**
 - task workers **11**
- pools, desktop **10**
- post-synchronization script, customizing linked-clone machines **73**
- Power Off VM policy **140**
- power policies
 - automated desktop pools **143, 144**
 - avoiding conflicts **144**
 - machines and pools **140**
- power-off script, customizing linked-clone machines **73**
- prefetch and superfetch, disabling **43**
- printing, location-based **292**
- problem machines, displaying **327**
- product ID **219**

Q

- QuickPrep
 - customization errors **337**
 - customization scripts **73**
 - increasing timeout limit for customization scripts **49**
 - troubleshooting customization failure **335**
 - View Composer **72, 73**

R

- RDP, disabling access to desktops **156**
- RDS hosts
 - configuring 3D graphics **104**
 - installing applications **95**
 - installing Horizon Agent **99**
 - installing Remote Desktop Services on Windows Server 2008 R2 **97**
 - installing Remote Desktop Services on Windows Server 2012 or 2012 R2 **97**
 - introduction **9**
 - performance options **103**
 - Restrict Users to a Single Desktop Session **99**
 - setting up **95**
- RDS desktop pools
 - Adobe Flash Throttling **125**
 - creating **123, 124**
 - desktop settings **124, 135**
- RDS desktop sessions, time zone redirection **102**
- RDS host parent virtual machines, preparing for View Composer **108**
- RDS hosts, add ADMX files **284**
- Real-Time Audio-Video
 - bandwidth **196**
 - configuring **183**
 - configuring group policy settings **194**
 - group policy settings **195**
 - preventing conflicts with USB redirection **185**
 - system requirements **184**
- Real-Time Audio-Video, adding the ADM template **194**
- Real-Time Audio-Video, configuration choices **184**
- rebalance feature **240**
- rebalancing linked-clone machines, setting minimum ready machines **75**
- recomposing machines, setting minimum ready machines **75**
- recomposing linked-clone machines, Sysprep **75**
- refresh, setting minimum ready machines **75**
- registry backup (RegIdleBackup), disabling **43**
- regulatory compliance **14**
- remote repository, configuring **307**

- Remote Desktop connections
 - disabling RDP **156**
 - enabling **22**
- Remote Desktop Services
 - adding ADMX files to Active Directory **284**
 - application compatibility group policies **285**
 - connections group policies **286**
 - device and resource redirection group policies **286**
 - licensing group policies **287**
 - profiles group policies **289**
 - remote session environment group policies **291**
 - security group policies **291**
 - temporary folders group policies **292**
- Remote Desktop Services (RDS) hosts
 - setting up **95**
 - See also* RDS hosts
- Remote Desktop Services group policies **283**
- Remote Desktop Users group **22**
- remote desktops, USB redirection problems **230, 342**
- remote desktops, configuring features **165**
- REPLICA_DISK policy profile **237**
- replicas **240**
- restricted entitlements
 - assigning tags to desktop pools **163**
 - configuring **163**
 - examples **161**
 - limitations **163**
 - tag matching **162**
 - understanding **160**
- roaming and synchronization, group policy settings **319**
- roaming profiles, *See* persona management

S

- SBPM (storage-based policy management) **235, 238**
- scanner redirection
 - ADM template file **199**
 - configuring **197**
 - group policy settings **199, 200**
 - system requirements **197**
 - user features **198**
- security **14**
- security server, connection problems to the PCoIP Secure Gateway **340**
- security servers, restricted entitlements limitations **163**
- sending messages to desktop users **328**
- serial port redirection
 - ADM template file **205**
 - configuring **202**

- configuring group policies **205**
- group policy settings **206**
- guidelines **204**
- user operation **203**
- shared folders, access permissions for Persona Management **307**
- shared storage **233**
- SIDs, support in View Composer **71**
- silent installation, Horizon Agent **30**
- silent installation options **31**
- single sign-on, group policy settings **266**
- Smart Policies **257, 258**
- Smartcard Redirection, Horizon Agent custom option **17, 28**
- solid-state disks, storing View Composer replicas **249**
- sparse disks, configuring for desktop pools **251**
- splitting composite USB devices **221**
- SSO, group policy settings **266**
- storage
 - reclaiming disk space **251**
 - reducing, with instant clones **239**
 - reducing, with instant clones or View Composer linked clones **233**
 - reducing, with View Composer **240**
- storage overcommit, linked clones **245, 246**
- storage-based policy management **235, 238**
- Suspend VM policy, on disconnect **142**
- swap files, linked-clone machines **45, 48, 108**
- Sysprep
 - linked-clone machines **72**
 - recomposing linked-clone machines **75**
- System Restore, disabling **44**
- system requirements, Unity Touch **166**

T

- task workers **11**
- terminal servers, preparing for desktop delivery **15**
- ThinApp applications, configuring user profiles **317**
- third-party applications, support in View Composer **71**
- time synchronization, guest OS and ESXi host **22**
- time zone redirection **102**
- timeout limit, ClonePrep and QuickPrep customization scripts **49**
- TPVMGPOACmap.dll file **294**
- troubleshooting machines and desktop pools **327**

U

- unentitled users, displaying **344**
- unicast redirection
 - configuring **168**
 - system requirements **169**
- Unity Touch
 - configuring **165**
 - system requirements **166**
- Unity Touch feature **166**
- unmanaged machines
 - defined **15**
 - installing Horizon Agent **16**
 - preparing for desktop delivery **15**
- Update Service, disabling **42**
- URL Content Redirection, installing **179**
- USB device families **226**
- USB device filtersUSB device filters **223**
- USB devices
 - support for **214**
 - using with View desktops **213, 215**
- USB redirection
 - automatic connections **216**
 - configuring in Horizon Agent **17, 28**
 - controlling using policies **220, 227**
 - deploying devices securely **217**
 - disabling all devices **217**
 - disabling specific devices **218**
 - ports for **216**
 - preventing conflicts with Real-Time Audio-Video **185**
 - troubleshooting failure **230, 342**
- USB to Serial adapters, configuring for redirection **208**
- User Environment Manager **258–260, 262**
- user persona, configuring policies **301**
- user profile path, configuring **307**
- user profile repository, guidelines for creating **308**
- user profiles
 - ThinApp sandbox folders **317**
 - See also* persona management
- users
 - displaying unentitled **344**
 - sending messages **328**

V

- VAAI, creating linked clones **253**
- vCenter Server **10**
- vDGA (Virtual Dedicated Graphics Acceleration) **145, 148, 150, 153**
- vdm_agent.adm **264, 266**
- vdm_blast.adm **282**
- vdm_client.adm **264**
- vdm_common.adm **264**

- vdm_server.adm **264**
- vendor ID **219**
- vid/pid **219**
- View Storage Accelerator, configuring for desktop pools **250**
- View Composer **240**
- View Composer Agent
 - Horizon Agent custom option **28**
 - Horizon Agent custom setup option **28**
- View Composer Array Integration, enabling for desktop pools **253**
- View Composer configuration
 - support for unique SIDs **71**
 - volume activation **47, 110**
- View Composer persistent disks
 - storage sizing formulas **243**
 - storage sizing formulas for editing pools **244**
- View Composer troubleshooting
 - finding unused replicas **336**
 - provisioning error codes **337**
 - QuickPrep script failure **335**
- View Composer use
 - choosing QuickPrep or Sysprep **72**
 - considerations for storing replicas on separate datastores **249**
 - creating data disks **247**
 - creating linked-clone pools **59, 67**
 - local datastores **248**
 - preparing a parent virtual machine **45**
 - preparing an RDS host parent virtual machine **108**
 - QuickPrep **73**
 - storing replicas and linked clones on separate datastores **249**
 - worksheet for creating linked-clone pools **59**
- View Connection Server
 - assigning tags for restricted entitlement **163**
 - troubleshooting connection issues **339, 341**
- ViewDbChk **344**
- ViewPM.adm, ADM template files **264**
- ViewPM.adm file
 - adding to Active Directory **312**
 - adding to a local system **311**
- virtual machines
 - creating templates **49**
 - creating in vSphere **20**
 - custom configuration parameters **21**
 - customization failures **332**
 - disabling Windows 7 services **39**
 - disabling Windows 8 services **39**
 - installing guest operating system **22**
 - preparing for desktop deployment **19**
 - stuck in Provisioning state **332**
- Virtual Printing, Horizon Agent custom option **28**

- virtual profiles, See persona management
- Virtual SAN **233, 235, 240**
- Virtual Volumes (VVols) **238, 240**
- VM_HOMEpolicy profile **237**
- VMFS datastores, clusters with more than eight hosts **157**
- VMware Tools, installing **22**
- VMware Blast, group policy settings **282**
- volume activation
 - linked-clone machines **47**
 - linked-clone RDS hosts **110**
- vSAN **233, 235, 240**
- vSGA (Virtual Shared Graphics Acceleration) **145, 148, 150**
- vSphere **233**

W

- Web pages, providing multicast streams **171**
- webcam **186, 189, 191**
- webcams, selecting preferred **186**
- Windows 8.1, restarting Windows Firewall **26**
- Windows 10
 - disabling services **39**
 - restarting Windows Firewall **26**
 - services that cause OS disk growth **39**
- Windows 7
 - 3D rendering **145, 148, 150**
 - benefits of disabling services **39**
 - disabling hibernation **47, 110**
 - disabling customer experience improvement program **38**
 - disabling defragmentation for linked clones **41**
 - disabling Microsoft Feeds Synchronization **44**
 - disabling prefetch and superfetch **43**
 - disabling registry backup **43**
 - disabling System Restore **44**
 - disabling Windows Defender **44**
 - disabling Windows Diagnostic Policy Service **42**
 - disabling Windows Update Service **42**
 - services that cause OS disk growth **39**
 - volume activation with linked clones **47**
- Windows 8
 - benefits of disabling services **39**
 - disabling hibernation **47, 110**
 - disabling services **39**
 - disabling customer experience improvement program **38**
 - disabling defragmentation for linked clones **41**
 - disabling Microsoft Feeds Synchronization **44**
 - disabling prefetch and superfetch **43**
 - disabling registry backup **43**
 - disabling System Restore **44**
 - disabling Windows Defender **44**

- disabling Windows Diagnostic Policy Service **42**
- disabling Windows Update Service **42**
- services that cause OS disk growth **39**
- volume activation with linked clones **47**
- Windows registry, disabling or enabling Flash URL Redirection **172**
- Windows roaming profiles, Persona Management **306**
- Windows Server 2008 R2 desktops **24**
- Windows Server 2012 R2 desktops, restarting Windows Firewall **26**
- worker types **11**

