View Upgrades

VMware Horizon 6.0

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-001476-01

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

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

Contents

View Upgrades

View Upgrades provides instructions for upgrading from Horizon View 5.x (which includes 5.0.1, 5.1.3, 5.2, 5.3, and 5.3.1) to VMware Horizon™ with View™ 6.0. You can also use this guide when you upgrade to View maintenance and patch releases.

If you are also upgrading your version of VMware vSphere®, this guide tells you which steps of that upgrade to do at various stages of the View upgrade.

For View patch releases, see Chapter 8, "Applying View Patches," on page 59.

Intended Audience

This guide is intended for anyone who needs to upgrade to this latest version of View. The information in this guide is written for experienced Microsoft Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

View Component Compatibility Matrix 1

Because large enterprises must often perform phased upgrades, View components are designed to be somewhat forward and backward compatible, at least during upgrades.

View Connection Server compatibility with View Agents is limited to interoperability during a View Connection Server upgrade. You must upgrade View Agents as soon as possible to match the version of the View Connection Server that manages them.

The following tables list the components of View and show whether they are compatible with other components whose version is different. For information about compatibility with vSphere, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Table 1-1. Compatibility Matrix for VMware Horizon with View 6.0 and Horizon View 5.3.x Components

	Connection Server 5.3.x	Security Server 5.3.x (PCoIP and RDP)	View Composer 5.3	View Agent 5.3.x	View Client (Windows) 5.x
Connection Server 6.0	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes
Security Server 6.0 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes
View Composer 6.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A
View Agent 6.0	Only during upgrade	No	No	N/A	Only during upgrade
Horizon Client 3.0	Yes	Yes	Yes	Yes	N/A

Table 1-2. Compatibility Matrix for VMware Horizon with View 6.0 and Horizon View 5.2.x Components

	Connection Server 5.2.x	Security Server 5.2.x (PCoIP and RDP)	View Composer 5.2	View Agent 5.2.x	View Client (Windows) 5.x
Connection Server 6.0	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes
Security Server 6.0 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes
View Composer 6.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A

Table 1-2. Compatibility Matrix for VMware Horizon with View 6.0 and Horizon View 5.2.x Components (Continued)

	Connection Server 5.2.x	Security Server 5.2.x (PCoIP and RDP)	View Composer 5.2	View Agent 5.2.x	View Client (Windows) 5.x
View Agent 6.0	Only during upgrade	No	No	N/A	Only during upgrade
Horizon Client 3.0	Yes	Yes	Yes	Yes	N/A

Table 1-3. Compatibility Matrix for VMware Horizon with View 6.0 and Horizon View 5.1.x Components

	Connection Server 5.1.3	Security Server 5.1.3 (PCoIP and RDP)	View Composer 3.0	View Agent 5.1.3	View Client (Windows) 5.1.x
Connection Server 6.0	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes
Security Server 6.0 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes
View Composer 6.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A
View Agent 6.0	Only during upgrade	No	No	N/A	Only during upgrade
Horizon Client 3.0	Yes	Yes	Yes	Yes	N/A

Table 1-4. Compatibility Matrix for VMware Horizon with View 6.0 and Horizon View 5.0.1 Components

	Connection Server 5.0.1	Security Server 5.0.1 (PCoIP and RDP)	View Composer 2.7	View Agent 5.0.1	View Client (Windows) 5.0.x
Connection Server 6.0	Only during upgrade	Only if paired before upgrade	No	Only during upgrade	Yes
Security Server 6.0 (PCoIP and RDP)	No	N/A	No	Only during upgrade	Yes
View Composer 6.0	Only during upgrade	Only during upgrade	N/A	Only during upgrade	N/A
View Agent 6.0	No	No	No	N/A	Only during upgrade
Horizon Client 3.0	5.0.1 Connection Server only	Yes	Yes	Yes	N/A

Although newer versions of View Client and Horizon Client can work with View Connection Server 5.0.0, the security enhancements and certificate checking that were introduced with View 5.1 are available only with View Connection Server 5.0.1 and later releases.

Caution During an upgrade, View does not support View Composer provisioning and maintenance operations. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server and View Composer have been upgraded to the latest version.

For details about which versions of View are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

View Upgrade Overview 2

Upgrading an enterprise View deployment involves several high-level tasks. Upgrading is a multistage process in which procedures must be performed in a particular order. You upgrade VMware View® Composer™ before upgrading View Connection Server and the other View servers.

IMPORTANT The VMware View® Client with Local Mode feature, for using offline desktops, has been removed, and therefore this overview does not include steps for upgrading View Transfer Server instances and View Client with Local Mode. In place of the Local Mode feature, VMware recommends using VMware® Mirage™, which is included with VMware Horizon 6.0. For more information, see the View Release Notes, available at https://www.vmware.com/support/pubs/view_pubs.html.

During an upgrade, View does not support View Composer provisioning and maintenance operations. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server and View Composer have been upgraded.

You must complete the upgrade process in a specific order. Order is also important within each upgrade stage.

NOTE This overview relates to upgrades for major, minor, and maintenance releases. For information about patches, see Chapter 8, "Applying View Patches," on page 59.

How many of the following tasks you need to complete depends on which components of View you use in your deployment.

1 On the physical or virtual machines that host View Composer and VMware® vCenter Server™, make backups and temporarily halt certain scheduled tasks. See "Preparing vCenter Server and View Composer for an Upgrade," on page 21.

   For details about which versions of View are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

2 On the physical or virtual machines that host View Connection Server instances, make backups and record various configuration and system settings. See "Preparing View Connection Server for an Upgrade," on page 23.

3 If you use security servers, perform the tasks in "Prepare to Upgrade or Reinstall a Security Server," on page 24.

4 Upgrade View Composer on the existing host or migrate to a new machine. See "Upgrade View Composer," on page 27.

5 Upgrade View Connection Server on the existing host or migrate to a new machine. See "Upgrade View Connection Servers in a Replicated Group," on page 36.

IMPORTANT After you upgrade a View Connection Server instance to the latest version, you cannot downgrade that instance to an earlier version. After you upgrade all View Connection Server instances in a replicated group, you cannot add another instance that runs an earlier version.

6 If you use security servers, upgrade them. See "Upgrade View Security Server," on page 41.

7 Upgrade the group policies used in Active Directory. See "Using View Group Policy Administrative Template Files," on page 43.

8 If you are also upgrading VMware vSphere components, upgrade vCenter Server. See "Upgrade vCenter Server," on page 42.

9 If you are also upgrading vSphere, upgrade the VMware® ESXi™ hosts and virtual machines. See Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45.

10 If you currently use Windows Terminal Services servers as desktop sources, upgrade to Windows Server 2008 R2 or later and verify that the RDS Host role is installed. See "Upgrade RDS Hosts That Provide Session-Based Desktops," on page 47

11 Upgrade the Horizon™ View Agent™ software that runs on the physical or virtual machines that are used as desktop sources, as full-clone desktops in a pool, and as individual desktops in a manual pool. See "Upgrade View Agent," on page 48.

12 Use the newly upgraded virtual machine desktop sources to create upgraded pools of desktops. See "Upgrade View Composer Desktop Pools," on page 50.

13 Upgrade the Horizon Client software that runs on end users' client devices. See "Upgrade the Client Application," on page 54.

Because certain commands can simultaneously upgrade more than one stage, VMware recommends that you thoroughly understand the irreversible changes at each stage before you upgrade your production environments.

System Requirements for Upgrades 3

Hosts and virtual machines in a View deployment must meet specific hardware and operating system requirements.

This chapter includes the following topics:

View Composer Requirements

With View Composer, you can deploy multiple linked-clone desktops from a single centralized base image. View Composer has specific installation and storage requirements.

Supported Operating Systems for View Composer

View Composer supports 64-bit operating systems with specific requirements and limitations. You can install View Composer on the same physical or virtual machine as vCenter Server or on a separate server.

Table 3-1. Operating System Support for View Composer

Operating System	Version	Edition
Windows Server 2008 R2	64-bit	Standard Enterprise
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise
Windows Server 2012 R2	64-bit	Standard

If you plan to install View Composer on a different physical or virtual machine than vCenter Server, see "Hardware Requirements for Standalone View Composer," on page 14.

Hardware Requirements for Standalone View Composer

If you install View Composer on a different physical or virtual machine from the one used for vCenter Server, you must use a dedicated machine that meets specific hardware requirements.

A standalone View Composer installation works with vCenter Server installed on a separate Windows Server machine or with the Linux-based vCenter Server appliance. VMware recommends having a one-to-one mapping between each View Composer service and vCenter Server instance.

Table 3-2. View Composer Hardware Requirements

Hardware Component	Required	Recommended
Processor	1.4 GHz or faster Intel 64 or AMD 64 processor with 2 CPUs	2GHz or faster and 4 CPUs
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs
Memory	4GB RAM or higher	8GB RAM or higher for deployments of 50 or more remote desktops
Disk space	40GB	60GB

IMPORTANT The physical or virtual machine that hosts View Composer must use a static IP address.

Database Requirements for View Composer

View Composer requires an SQL database to store data. The View Composer database must reside on, or be available to, the View Composer server host.

If a database server instance already exists for vCenter Server, View Composer can use that existing instance if it is a version listed in Table 3-3. For example, View Composer can use the Microsoft SQL Server instance provided with vCenter Server. If a database server instance does not already exist, you must install one.

View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and View database events.

IMPORTANT If you create the View Composer database on the same SQL Server instance as vCenter Server, do not overwrite the vCenter Server database.

The following table lists the supported database servers and versions. For a complete list of database versions supported with vCenter Server, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

The versions of vCenter Server listed in the table column headings are general. For specific supported update versions of each vCenter Server release, see the VMware Product Interoperability Matrixes at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Table 3-3. Supported Database Servers for View Composer

Database	vCenter Server 5.5	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1
Microsoft SQL Server 2012 Express (32- and 64-bit)	Yes	Yes	Yes	No
Microsoft SQL Server 2012 (SP1) Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes	No

Table 3-3. Supported Database Servers for View Composer (Continued)

Database	vCenter Server 5.5	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1
Microsoft SQL Server 2008 Express (R2 SP2) (64-bit)	Yes	Yes	Yes	No
Microsoft SQL Server 2008 (SP3), Standard, Enterprise, and Datacenter (32- and 64-bit)	No	Yes	Yes	Yes
Microsoft SQL Server 2008 (R2 SP2), Standard and Enterprise (32- and 64-bit)	Yes	Yes	Yes	Yes
Oracle 10g Release 2, Standard, Standard ONE, and Enterprise [10.2.0.4] (32- and 64-bit)	No	Yes	Yes	Yes
Oracle 11g Release 2, Standard, Standard ONE, and Enterprise [11.2.0.3] (32- and 64-bit)	Yes	Yes	Yes	Yes

Upgrade Requirements for View Composer

The View Composer upgrade process has specific requirements and limitations.

To run the View Composer installer, you must be a domain user with Administrator privileges on the system.

Security-Related Requirements

- View Composer requires an SSL certificate that is signed by a CA (certificate authority). If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, you must import the new certificate and run the `SviConfig ReplaceCertificate` utility to bind your new certificate to the port used by View Composer.

  If you install vCenter Server and View Composer on the same Windows Server computer, they can use the same SSL certificate, but you must configure the certificate separately for each component.

  For complete information about security certificate requirements, see "Configuring SSL Certificates for View Servers" in the *View Installation* guide.

- Certificates for vCenter Server, View Composer, and View servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *View Installation* guide.

- Verify that no applications that run on the View Composer computer use Windows SSL libraries that require SSL version 2 (SSLv2) provided through the Microsoft Secure Channel (Schannel) security package. The View Composer installer disables SSLv2 on the Microsoft Schannel. Applications such as Tomcat, which uses Java SSL, or Apache, which uses OpenSSL, are not affected by this constraint.

- To enhance the security of View Composer, disable the weak cryptographic cipher suites on the Windows Server computer on which the View Composer service is installed. See "Disable Weak Cryptographic Cipher Suites on the View Composer Server" in the *View Installation* guide.

View Connection Server Requirements

View Connection Server acts as a broker for client connections by authenticating and then directing incoming user requests to the appropriate remote desktops and applications. View Connection Server has specific hardware, operating system, installation, and supporting software requirements.

Hardware Requirements for View Connection Server

You must install all View Connection Server installation types, including standard, replica, and security server installations, on a dedicated physical or virtual machine that meets specific hardware requirements.

Table 3-4. View Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Network Adapter	100Mpbs NIC	1Gbps NICs
Memory Windows Server 2008 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops
Memory Windows Server 2012 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more remote desktops

These requirements also apply to replica and security server View Connection Server instances that you install for high availability or external access.

IMPORTANT The physical or virtual machine that hosts View Connection Server must use a static IP address.

Supported Operating Systems for View Connection Server

You must install View Connection Server on a supported Windows Server operating system.

The following operating systems support all View Connection Server installation types, including standard, replica, and security server installations.

Table 3-5. Operating System Support for View Connection Server

Operating System	Version	Edition
Windows Server 2008 R2	64-bit	Standard Enterprise
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise
Windows Server 2012 R2	64-bit	Standard

Upgrade Requirements for View Connection Server

The View Connection Server upgrade process has specific requirements and limitations.

- View Connection Server requires a valid license key for this latest release.
- The domain user account that you use to install the new version of View Connection Server must have administrative privileges on the View Connection Server host. The View Connection Server administrator must have administrative credentials for vCenter Server.

- When you run the installer, you authorize a View Administrators account. You can specify the local Administrators group or a domain user or group account. View assigns full View Administration rights, including the right to install replicated View Connection Server instances, to this account only. If you specify a domain user or group, you must create the account in Active Directory before you run the installer.
- When you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password. The password must contain between 1 and 128 characters.

Security-Related Requirements

- View Connection Server requires an SSL certificate that is signed by a CA (certificate authority) and that your clients can validate. Although a default self-signed certificate is generated in the absence of a CA-signed certificate when you install View Connection Server, you must replace the default self-signed certificate as soon as possible. Self-signed certificates are shown as invalid in View Administrator.

  Also, updated clients expect information about the server's certificate to be communicated as part of the SSL handshake between client and server. Often updated clients do not trust self-signed certificates.

  For complete information about security certificate requirements, see "Configuring SSL Certificates for View Servers" in the *View Installation* guide. Also see the *Scenarios for Setting Up SSL Connections to View* document, which describes setting up intermediate servers that perform tasks such as load balancing and off-loading SSL connections.

  NOTE If your original servers already have SSL certificates signed by a CA, during the upgrade, View imports your existing CA-signed certificate into the Windows Server certificate store.

- Certificates for vCenter Server, View Composer, and View servers must include certificate revocation lists (CRLs). For more information, see "Configuring Certificate Revocation Checking on Server Certificates" in the *View Installation* guide.

  IMPORTANT If your company uses proxy settings for Internet access, you might have to configure your View Connection Server hosts to use the proxy. This step ensures that servers can access certificate revocation checking sites on the Internet. You can use Microsoft Netshell commands to import the proxy settings to View Connection Server. For more information, see "Troubleshooting View Server Certificate Revocation Checking" in the *View Administration* guide.

- If you plan to pair a security server with this View Connection Server instance, verify that Windows Firewall with Advanced Security is set to **on** in the active profiles. It is recommended that you turn this setting to **on** for all profiles. By default, IPsec rules govern connections between security server and View Connection Server and require Windows Firewall with Advanced Security to be enabled.
- If your network topology includes a firewall between a security server and a View Connection Server instance, you must configure the firewall to support IPsec. See the *View Installation* document.

If you plan to perform fresh installations of View Connection Server instances on additional physical or virtual machines, see the complete list of installation requirements in the *View Installation* document.

Virtualization Software Requirements for View Connection Server

View Connection Server requires certain versions of VMware virtualization software.

If you are using vSphere, you must use a supported version of vSphere ESX/ESXi hosts and vCenter Server.

For details about which versions of View are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

View Administrator Requirements

Administrators use View Administrator to configure View Connection Server, deploy and manage remote desktops and applications, control user authentication, initiate and examine system events, and carry out analytical activities. Client systems that run View Administrator must meet certain requirements.

View Administrator is a Web-based application that is installed when you install View Connection Server. You can access and use View Administrator with the following Web browsers:

- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10 (from a Windows 8 system in Desktop mode)
- Firefox 6 and later releases

To use View Administrator with your Web browser, you must install Adobe Flash Player 10.1 or later. Your client system must have access to the Internet to allow Adobe Flash Player to be installed.

The computer on which you launch View Administrator must trust the root and intermediate certificates of the server that hosts View Connection Server. The supported browsers already contain certificates for all of the well-known certificate authorities (CAs). If your certificates come from a CA that is not well known, you must follow the instructions in the *View Installation* document about importing root and intermediate certificates.

To display text properly, View Administrator requires Microsoft-specific fonts. If your Web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac OS X, make sure that Microsoft-specific fonts are installed on your computer.

Currently, the Microsoft Web site does not distribute Microsoft fonts, but you can download them from independent Web sites.

Horizon Client Requirements

Horizon Client runs on many types of devices: Windows, Mac, and Linux desktops and laptops; Linux thin and zero clients; tablets; and phones. All of these devices have specific requirements.

For information about operating system requirements, hardware requirements, and browser requirements of a specific type client device, go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html and see the document for that type of client device.

IMPORTANT The features that are available for thin client devices and zero clients are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin and zero client devices, see the VMware Compatibility Guide, available on the VMware Web site.

Supported Operating Systems for View Agent

The View Agent component assists with session management, single sign-on, device redirection, and other features. You must install View Agent on all virtual machines, physical systems, and RDS hosts.

The following table lists the Windows operating system versions that are supported on virtual machines in a desktop pool.

Table 3-6. Operating Systems for Linked-Clone and Full-Clone Remote Desktops

Guest Operating System	Version	Edition	Service Pack
Windows 8.1	64-bit and 32-bit	Enterprise and Professional	None and Update
Windows 8	64-bit and 32-bit	Enterprise and Professional	None
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP2
Windows XP	32-bit	Professional	SP3
Windows Server 2008 R2	64-bit	Datacenter	SP1

IMPORTANT The virtual machine version must support the guest operating system. For example, to install Windows 8.1, you must use a vSphere 5.1 or later virtual machine.

The following table lists the Windows operating systems versions that are supported for creating desktop pools and application pools on an RDS host.

Table 3-7. Operating Systems for RDS Hosts, Providing Remote Desktops or Applications

Guest Operating System	Edition	Service Pack
Windows Server 2008 R2	Standard, Enterprise, and Datacenter	SP1
Windows Server 2012	Standard and Datacenter	None
Windows Server 2012 R2	Standard and Datacenter	None

Preparing for a View Upgrade

4

Before you start the upgrade process, you must review system requirements for the new version, back up databases, take snapshots of virtual machines that host server components, and document configuration settings.

This chapter includes the following topics:

Preparing vCenter Server and View Composer for an Upgrade

Because vCenter Server and View Composer are often installed on the same virtual or physical machine, some preparation tasks apply to both.

Preparing for Upgrades That Include vSphere

If you are upgrading vCenter Server in addition to upgrading to the latest version of View, you must consult the *VMware vSphere Upgrade Guide* and perform the following tasks in the following order:

1. Verify that the virtual or physical machine meets the system requirements for the version of vCenter Server that you want to upgrade to.
2. Verify that the virtual or physical machine on which the current View Composer is installed meets the security requirements for the new version.

   See "Upgrade Requirements for View Composer," on page 15.
3. If you are upgrading from View 5.0.x or an earlier version, verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable. For information about replacing the default certificate for vCenter Server, see the *vSphere Examples and Scenarios* document. Note that this issue does not occur if you are upgrading from View 5.1 or a later release.
4. If vCenter Server is installed in a virtual machine, take a snapshot of the virtual machine.

   For instructions on taking snapshots, see the vSphere Client™ online help.
5. If the computer name is longer than 15 characters, shorten the name to 15 or fewer characters.
6. Back up the vCenter Server database and the View Composer database.

   For instructions on performing a database backup, see the documentation from your database vendor.

7 Verify that the database server is compatible with the version of vCenter Server you plan to use.

   For example, if the database server is Oracle 9i, you must upgrade.

8 Verify that the database is compatible with the new version of View Composer.

   View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and View database events.

9 Make a copy of the folder that contains SSL certificates.

   This folder is located at `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter`.

10 Document the IP address and system name of the machine on which vCenter Server is installed.

11 For all linked-clone desktop pools, use View Administrator to disable provisioning of new virtual machines.

   Because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.

12 If any desktop pools are set to refresh the OS disk on logoff, use View Administrator to edit the **Desktop/Pools** settings for that pool and set **Refresh OS disk on logoff** to **Never**.

   This setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop on which View Agent has not yet been upgraded.

13 If any desktop pools are scheduled to do a refresh or recompose operation, use View Administrator to cancel these tasks.

Preparing for Upgrades of View Composer Only

If you are upgrading only View Composer and are not upgrading vCenter Server, you must perform the following tasks:

1 If you are upgrading from View 5.0.x or an earlier version, verify that the server on which View Composer is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if View Composer does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that View Composer is unavailable. For information about replacing the default certificate for View Composer, see the topic "Configuring SSL Certificates for View Servers" in the *View Installation* document. You must run the `SviConfig RelaceCertificate` command. Note that this issue does not occur if you are upgrading from View 5.1 or a later release.

2 Verify that the virtual or physical machine on which the current View Composer is installed meets the security requirements for the new version.

   See "Upgrade Requirements for View Composer," on page 15.

3 If View Composer is installed in a virtual machine, take a snapshot of the virtual machine.

   For instructions on taking snapshots, see the vSphere Client online help.

4 Back up the vCenter Server database and the View Composer database.

   For instructions on performing a database backup, see the documentation from your database vendor.

5 Verify that the database is compatible with the new version of View Composer.

   View Composer supports a subset of the database servers that vCenter Server supports. If you are already using vCenter Server with a database server that is not supported by View Composer, continue to use that database server for vCenter Server and install a separate database server to use for View Composer and View database events.

6 Make a copy of the folder that contains SSL certificates.

This folder is located at `%ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter`.

7 Document the IP address and system name of the machine on which vCenter Server is installed.

8 For all linked-clone desktop pools, use View Administrator to disable provisioning of new virtual machines.

Because View Composer might be upgraded during a different maintenance window than its desktop pools, provisioning must be postponed until both components are upgraded.

9 If any desktop pools are set to refresh the OS disk on logoff, use View Administrator to edit the **Desktop/Pools** settings for that pool and set **Refresh OS disk on logoff** to **Never**.

This setting prevents an error from occurring when the newly upgraded View Composer attempts to refresh a desktop on which View Agent has not yet been upgraded.

10 If any desktop pools are scheduled to do a refresh or recompose operation, use View Administrator to cancel these tasks.

Preparing View Connection Server for an Upgrade

Before you upgrade View Connection Server or before you upgrade any of the vSphere components that View Connection Server relies on, you must perform several tasks to ensure that these upgrades are successful.

- Verify that the virtual or physical machine on which the current View Connection Server instance is installed meets the system requirements for the new version.

  See "View Connection Server Requirements," on page 16.

- If View Connection Server is installed in a virtual machine, take a snapshot of the virtual machine. If you have a replicated group of View Connection Server instances, take a snapshot of only one View Connection Server instance.

  For instructions on taking snapshots, see the vSphere Client online help. If you ever need to revert to this snapshot and if you have other View Connection Server instances in a replicated group, you must uninstall those instances before you revert the master to the snapshot. After you revert, you can reinstall the replicated instances and point to the instance you reverted.

  You can label the snapshot Upgrade Preparation Phase.

- If your deployment currently uses the Local Mode feature, ask end users to check in their Local Mode desktops, or use View Administrator to roll back the Local Mode desktops so that no desktops are shown as checked out in View Administrator.

  IMPORTANT If any Local Mode desktops are checked out at the time you run the View Connection Server installer to install the upgrade, the upgrade will fail.

- If your deployment currently uses the Local Mode feature, open View Administrator, go to **View Configuration > Servers**, and remove all Transfer Server instances.

- Open View Administrator and document all the global settings and settings for desktops and pools: Pools section and Desktops section in the Inventory tree, and the Global Settings section in the View Configuration tree.

  For example, take a screen shot of the applicable settings. If you have multiple instances of View Connection Server in a replicated group, you need only document the settings for one instance.

- Use the `vdmexport.exe` utility to back up the LDAP database.

For instructions, see the administration guide for your current version of the *View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need only export the data from one instance.

- Document the IP address and system name of the machine on which View Connection Server is installed.
- Determine if your company has written any batch files or scripts that run against the View database on the View Connection Server instance, and if so, document their names and locations.
- If you use load balancers for View Connection Server, document the configuration settings for the load balancers.

Prepare to Upgrade or Reinstall a Security Server

Before you can upgrade or reinstall a security server instance, you must remove the current IPsec rules that govern communication between the security server and its paired View Connection Server instance. If you do not take this step, the upgrade or reinstallation fails.

IMPORTANT This task pertains to View 5.1 and later security servers. If does not apply to View 5.0.x and earlier security servers.

By default, communication between a security server and its paired View Connection Server instance is governed by IPsec rules. When you upgrade or reinstall the security server and pair it again with the View Connection Server instance, a new set of IPsec rules must be established. If the existing IPsec rules are not removed before you upgrade or reinstall, the pairing fails.

You must take this step when you upgrade or reinstall a security server and are using IPsec to protect communication between the security server and View Connection Server.

You can configure an initial security server pairing without using IPsec rules. Before you install the security server, you can open View Administrator and deselect the global setting **Use IPSec for Security Server Connections**, which is enabled by default. If IPsec rules are not in effect, you do not have to remove them before you upgrade or reinstall.

NOTE You do not have to remove a security server from View Administrator before you upgrade or reinstall the security server. Remove a security server from View Administrator only if you intend to remove the security server permanently from the View environment.

With View 5.0.x and earlier releases, you could remove a security server either from within the View Administrator user interface or by using the `vdmadmin -S` command-line command. In View 5.1 and later releases, you must use `vdmadmin -S`. See "Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option" in the *View Administration* document.

CAUTION If you remove the IPsec rules for an active security server, all communication with the security server is lost until you upgrade or reinstall the security server.

Procedure

1. In View Administrator, click **View Configuration > Servers**.
2. In the **Security Servers** tab, select a security server and click **More Commands > Prepare for Upgrade or Reinstallation**.

   If you disabled IPsec rules before you installed the security server, this setting is inactive. In this case, you do not have to remove IPsec rules before you reinstall or upgrade.
3. Click **OK**.

The IPsec rules are removed and the **Prepare for Upgrade or Reinstallation** setting becomes inactive, indicating that you can reinstall or upgrade the security server.

Upgrading View Server Components 5

The server components that you must upgrade include View Connection Server, replicated servers, and security servers. Depending on the optional components you use, you might also need to upgrade View Composer.

NOTE The Local Mode feature for Horizon Client has been removed, and therefore View Transfer Server instances are no longer required. In place of the Local Mode feature, VMware recommends using Mirage, which is included with VMware Horizon 6. For more information, see the View Release Notes, available at https://www.vmware.com/support/pubs/view_pubs.html.

During an upgrade, View does not support View Composer provisioning and maintenance operations. Operations such as provisioning and recomposing linked-clone desktops are not supported during the transitional period when any View servers are still running the earlier version. You can successfully perform these operations only when all instances of View Connection Server and View Composer have been upgraded.

For View patch releases, see Chapter 8, "Applying View Patches," on page 59.

This chapter includes the following topics:

Upgrade View Composer

During the first maintenance window, you will upgrade View Composer. Operations such as provisioning and recomposing linked-clone desktops are not supported until all View servers are upgraded.

IMPORTANT If your current version of View Composer is installed on a computer with a Windows Server 2003 operating system, see the procedure called "Manually Migrate View Composer to the New Machine" in the *VMware View 4.6 Upgrades* document. After you migrate View Composer 2.6 to a system with a Windows Server operating system that is supported for this release, you can perform an in-place upgrade to the latest version of View Composer.

To migrate an already upgraded View Composer to a different physical or virtual machine, see "Migrate View Composer to Another Machine," on page 31.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Complete the tasks listed in "Preparing for Upgrades of View Composer Only," on page 22.
- Verify that the server on which View Composer is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if View Composer does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Determine whether to let the installer wizard upgrade the View Composer database if a schema upgrade is required. You can choose to run the `SviConfig` command-line utility after the wizard finishes to upgrade the database schema manually and to create a log of the upgrade.

Procedure

1 On the virtual or physical machines where View Composer is installed, download and run the installer for View Composer.

  You can download the installer from the VMware Web site.

  Step-by-step instructions for running the installer appear in the *View Installation* document.

2 Specify whether you want the wizard to upgrade the database schema if a schema upgrade is required.

  If a dialog box appears with the message `"Database upgrade completed with warnings"` you can click **OK** and safely ignore the message.

3 When the wizard prompts you for the View Composer port number, verify that the port number is set to `18443`.

What to do next

If you need to do a manual upgrade of the database schema, see "Run SviConfig to Manually Upgrade the Database," on page 29.

At your next maintenance window, continue with the View upgrade. See "Upgrade View Connection Servers in a Replicated Group," on page 36.

Manually Upgrading the View Composer Database

Rather than letting the View Composer installer upgrade the database when a schema update is required, you can manually upgrade the database. You can use the `SviConfig` utility when you must observe the upgrade process more closely or when upgrade tasks must be distributed to IT administrators with different responsibilities.

When you upgrade View Composer to a version with an updated database schema, an installer prompt asks if you want the wizard to upgrade the database. If you choose not to use the installer wizard, you must use the `SviConfig` utility to upgrade the database and migrate the existing data.

Using the `SviConfig` command-line utility has the following advantages:

- This utility returns result codes and creates a log of the database upgrade to simplify troubleshooting if the upgrade fails.
- You can separate the upgrade tasks. A vSphere or View administrator can run the View Composer installer to upgrade the software. A database administrator (DBA) can use `SviConfig` to upgrade the View Composer database.

- The software upgrade and the database upgrade can occur during different maintenance windows. For example, your site might run database-maintenance operations on weekends only, whereas software-maintenance tasks can occur during the week.

Run SviConfig to Manually Upgrade the Database

With the `SviConfig` command-line utility, you can upgrade the View Composer database separately from the View Composer software. This utility also creates a log file to simplify troubleshooting if the upgrade fails.

IMPORTANT Only experienced View Composer administrators should use the `SviConfig` utility. This utility is intended to resolve issues relating to the View Composer service.

Prerequisites

- Back up the View Composer database. For instructions, see the documentation for your database server.
- Verify that you know the database source name (DSN) for the View Composer database.
- Verify that you know the user name and password for the database administrator account for this database.

Procedure

1 On the vCenter Server virtual or physical machine, open a Windows command prompt and navigate to the `SviConfig` executable file.

The file is located with the View Composer application. The default path is `C:\Program Files (86)\VMware\VMware View Composer\sviconfig.exe`.

2 Enter the command to stop VMware View Composer.

```
net stop svid
```

3 Run the `SviConfig databaseupgrade` command.

```
sviconfig –operation=databaseupgrade
                  –DsnName=target_DSN
                  –Username=database_administrator_username
```

For example:

```
sviconfig –operation=databaseupgrade –dsnname=LinkedClone
–username=Admin
```

4 When prompted, supply the password.

A successful operation displays output that shows the upgrade steps.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

5 Enter the command to start the View Composer.

```
net start svid
```

A complete log of the upgrade process is created and placed in `C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log`.

What to do next

If the database upgrade fails, see "Troubleshooting a View Composer Database Upgrade Failure," on page 30.

If the result code is any number other than 0, which means success, see "Result Codes for a Manual Database Schema Update," on page 30.

Result Codes for a Manual Database Schema Update

When you manually upgrade the View Composer database, the `sviconfig databaseupgrade` command displays a result code.

Table 5-1 shows the `sviconfig databaseupgrade` result codes.

Table 5-1. Result Codes for the databaseupgrade Command

Code	Description
0	The operation ended successfully.
1	The supplied DSN could not be found.
2	Invalid database administrator credentials were provided.
3	The driver for the database is not supported.
4	An unexpected problem arose and the command failed to complete.
14	Another application is using the View Composer service. Shut down the service before executing the command.
15	A problem arose during the restore process. Details are provided in the onscreen log output.
17	Unable to upgrade the database data.
18	Unable to connect to the database server.

Troubleshooting a View Composer Database Upgrade Failure

When you upgrade the View Composer service with the View Composer installer or run the `SviConfig databaseupgrade` command, the operation might fail to upgrade the View Composer database.

Problem

The `SviConfig databaseupgrade` operation displays error code `17`, or the View Composer installer displays a warning message.

```
Database upgrade completed with warnings
```

Cause

The database-upgrade software contacts vCenter Server to get additional data about desktops. The database upgrade might fail if the desktops are not available, the ESXi host is not running, or vCenter Server is not available.

Solution

1 See the View Composer `SviConfig` log file for more information.

The default location of this file is `C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log`. The upgrade script logs a message for each failure.

2 Examine the log records to identify the desktops that failed to upgrade.

Option	Action
The desktop exists but is unavailable.	Make the desktop available again. Depending on the cause of the failure, you might have to restart the ESXi host or vCenter Server, or take another action.
The desktop does not exist.	Ignore the log message. NOTE A deleted desktop might appear to exist in View Administrator if an administrator deletes the desktop virtual machine directly in vSphere.

3 Run the `SviConfig databaseupgrade` command again.

Migrate View Composer to Another Machine

In some situations, you might need to migrate a VMware Horizon View Composer service to a new Windows Server virtual or physical machine. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your View deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server machine.

You can migrate View Composer from the vCenter Server machine to a standalone machine or from a standalone machine to the vCenter Server machine.

IMPORTANT These topics pertain to migrating the latest version of View Composer to another machine. You must upgrade from the earlier version of View Composer before you perform these tasks.

If your current version of View Composer is installed on a machine that does not meet the system requirements for the new version of View Composer, you cannot use these procedures. For example, if you have View Composer 2.6, which is included with View 4.6, installed on a Windows Server 2003 operating system, see the procedure called "Manually Migrate View Composer to the New Machine" in the *VMware View 4.6 Upgrades* document. After you migrate View Composer 2.6 to a system with a Windows Server operating system that is supported for this release, you can perform an in-place upgrade to the latest version of View Composer.

- Guidelines for Migrating View Composer on page 32

  The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

- Migrate View Composer with an Existing Database on page 32

  When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

- Migrate View Composer Without Linked-Clone Virtual Machines on page 34

  If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

- Prepare a Microsoft .NET Framework for Migrating RSA Keys on page 35

  To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

- Migrate the RSA Key Container to the New View Composer Service on page 35

  To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

Guidelines for Migrating View Composer

The steps you take to migrate the VMware Horizon View Composer service depend on whether you intend to preserve existing linked-clone virtual machines.

To preserve the linked-clone virtual machines in your deployment, the VMware Horizon View Composer service that you install on the new virtual or physical machine must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new machine.

Whether or not you migrate the View Composer database, the database must be configured on an available machine in the same domain as the new machine on which you install the VMware Horizon View Composer service, or on a trusted domain.

View Composer creates RSA key pairs to encrypt and decrypt authentication information stored in the View Composer database. To make this data source compatible with the new VMware Horizon View Composer service, you must migrate the RSA key container that was created by the original VMware Horizon View Composer service. You must import the RSA key container to the machine on which you install the new service.

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

NOTE Each instance of the VMware Horizon View Composer service must have its own View Composer database. Multiple VMware Horizon View Composer services cannot share a View Composer database.

Migrate View Composer with an Existing Database

When you migrate View Composer to another physical or virtual machine, if you intend to preserve your current linked-clone virtual machines, the new VMware Horizon View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server machine to a standalone machine
- From a standalone machine to a vCenter Server machine
- From a standalone machine to another standalone machine
- From a vCenter Server machine to another vCenter Server machine

When you migrate the VMware Horizon View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server machine that you are migrating as well.

When you install the VMware Horizon View Composer service on the new machine, you must configure the service to connect to the View Composer database.

Prerequisites

- Familiarize yourself with the View Composer migration requirements. See "Guidelines for Migrating View Composer," on page 32.
- Familiarize yourself with the steps for migrating the RSA key container to the new VMware Horizon View Composer service. See "Prepare a Microsoft .NET Framework for Migrating RSA Keys," on page 35 and "Migrate the RSA Key Container to the New View Composer Service," on page 35.
- Familiarize yourself with installing the VMware Horizon View Composer service. See "Installing View Composer" in the *View Installation* document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *View Installation* document.
- Familiarize yourself with configuring View Composer in View Administrator. See the topics about configuring View Composer settings and View Composer domains in the *View Administration* document.

Procedure

1 Disable virtual machine provisioning in the vCenter Server instance that is associated with the VMware Horizon View Composer service.

   a In View Administrator, select **View Configuration > Servers**.

   b On the **vCenter Servers** tab, select the vCenter Server instance and click **Disable Provisioning**.

2 (Optional) Migrate the View Composer database to a new location.

   If you need to take this step, consult your database administrator for migration instructions.

3 Uninstall the VMware Horizon View Composer service from the current machine.

4 (Optional) Migrate the RSA key container to the new machine.

5 Install the VMware Horizon View Composer service on the new machine.

   During the installation, specify the DSN of the database that was used by the original VMware Horizon View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.

   If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new VMware Horizon View Composer service must have access to the original database information about the linked clones.

6 Configure an SSL server certificate for View Composer on the new machine.

   You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.

7 In View Administrator, configure the new View Composer settings.

   a In View Administrator, select **View Configuration > Servers**.

   b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.

   c In the View Composer Server Settings pane, click **Edit** and provide the new View Composer settings.

      If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

      If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

d In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.

e Click **OK**.

Migrate View Composer Without Linked-Clone Virtual Machines

If the current VMware Horizon View Composer service does not manage any linked-clone virtual machines, you can migrate View Composer to a new physical or virtual machine without migrating the RSA keys to the new machine. The migrated VMware Horizon View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

Prerequisites

- Familiarize yourself with installing the VMware Horizon View Composer service. See "Installing View Composer" in the *View Installation* document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *View Installation* document.
- Familiarize yourself with the steps for removing View Composer from View Administrator. See topic about removing View Composer from View Administrator in the *View Administration* document.

  Before you can remove View Composer, verify that it no longer manages any linked-clone virtual machines. If any linked clones remain, you must delete them.
- Familiarize yourself with configuring View Composer in View Administrator. See the topics about configuring View Composer settings and View Composer domains in the *View Administration* document.

Procedure

1 In View Administrator, remove View Composer from View Administrator.

  a Select **View Configuration > Servers**.

  b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with the View Composer service and click **Edit**.

  c In the View Composer Server Settings pane, click **Edit**.

  d Select **Do not use View Composer** and click **OK**.

2 Uninstall the VMware Horizon View Composer service from the current machine.

3 Install the VMware Horizon View Composer service on the new machine.

  During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.

4 Configure an SSL server certificate for View Composer on the new machine.

  You might be able to copy the certificate that was installed for View Composer on the original machine, or you can install a new certificate.

5 In View Administrator, configure the new View Composer settings.

  a In View Administrator, select **View Configuration > Servers**.

  b On the **vCenter Servers** tab, select the vCenter Server instance that is associated with this View Composer service and click **Edit**.

  c In the View Composer Server Settings pane, click **Edit**.

d Provide the new View Composer settings.

If you are installing View Composer with vCenter Server on the new machine, select **View Composer co-installed with the vCenter Server**.

If you are installing View Composer on a standalone machine, select **Standalone View Composer Server** and provide the FQDN of the View Composer machine and the user name and password of the View Composer user.

e In the Domains pane, click **Verify Server Information** and add or edit the View Composer domains as needed.

f Click **OK**.

Prepare a Microsoft .NET Framework for Migrating RSA Keys

To use an existing View Composer database, you must migrate the RSA key container between machines. You migrate the RSA key container by using the ASP.NET IIS registration tool provided with the Microsoft .NET Framework.

Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool. Go to http://www.microsoft.com/net.

Procedure

1 Install the .NET Framework on the physical or virtual machine on which the VMware Horizon View Composer service associated with the existing database is installed.

2 Install the .NET Framework on the destination machine on which you want to want to install the new VMware Horizon View Composer service.

What to do next

Migrate the RSA key container to the destination machine. See "Migrate the RSA Key Container to the New View Composer Service," on page 35.

Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source physical or virtual machine on which the existing VMware Horizon View Composer service resides to the machine on which you want to install the new VMware Horizon View Composer service.

You must perform this procedure before you install the new VMware Horizon View Composer service.

Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination machines. See "Prepare a Microsoft .NET Framework for Migrating RSA Keys," on page 35.

Procedure

1 On the source machine on which the existing VMware Horizon View Composer service resides, open a command prompt and navigate to the `%windir%\Microsoft.NET\Framework\v2.0xxxxx` directory.

2 Type the `aspnet_regiis` command to save the RSA key pair in a local file.

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

The ASP.NET IIS registration tool exports the RSA public-private key pair from the `SviKeyContainer` container to the `keys.xml` file and saves the file locally.

3 Copy the `keys.xml` file to the destination machine on which you want to install the new VMware Horizon View Composer service.

4 On the destination machine, open a command prompt and navigate to the `%windir%\Microsoft.NET\Framework\v2.0xxxxx` directory.

5 Type the `aspnet_regiis` command to migrate the RSA key pair data.

```
aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp
```

where *path* is the path to the exported file.

The `-exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this machine and imported to another machine. If you previously migrated the keys to this machine without using the `-exp` option, you can import the keys again using the `-exp` option so that you can export the keys in the future.

The registration tool imports the key pair data into the local key container.

What to do next

Install the new VMware Horizon View Composer service on the destination machine. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original VMware Horizon View Composer service. For installation instructions, see "Installing View Composer" in the *View Installation* document.

Complete the steps to migrate View Composer to a new machine and use the same database. See "Migrate View Composer with an Existing Database," on page 32.

Upgrade View Connection Servers in a Replicated Group

If you spread the upgrade tasks across multiple maintenance windows, you can verify success or discover issues at each phase of the process. VMware recommends upgrading all server components during the first maintenance window.

To use the new features of the latest version of View, you must upgrade. For a list of the new features included in the latest release, see the release notes.

NOTE This procedure describes an in-place upgrade. To migrate to a different machine, see "Upgrade to the Latest Version of View Connection Server on a Different Machine," on page 39.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time the upgrade takes depends on the number of View Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.
- If you use View Composer, verify that View Composer has been upgraded. See "Upgrade View Composer," on page 27. After you upgrade View Connection Server, you must add View Composer using View Administrator.
- Familiarize yourself with the security-related requirements of View, and verify that these requirements are met. See "Upgrade Requirements for View Connection Server," on page 16. You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to **on**, and configure any back-end firewalls to support IPsec.
- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable.

- Complete the tasks listed in "Preparing View Connection Server for an Upgrade," on page 23.

  IMPORTANT If any Local Mode desktops are checked out at the time you run the View Connection Server installer to install the upgrade, the upgrade will fail.

- Verify that you have a license for the new version.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- If you are unfamiliar with the `vdmexport.exe` utility, print the instructions for using it from the *View Administration* document. You will use this utility to back up the View LDAP database as part of the upgrade procedure.
- If you use security servers, familiarize yourself with the instructions on running the installer to create a security server that uses the new security server pairing mechanism. See the *View Installation* document for your current version of View.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

1 On the host of one of the View Connection Server instances in the group, download and run the installer for the new version of View Connection Server.

  You do not need to stop any services before performing the upgrade. The installer stops and restarts services as necessary. In fact, the VMwareVDMDS service must be running in order to upgrade the View LDAP database.

  The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.

  The View LDAP is also upgraded.

2 Verify that the VMware Horizon View Connection Server service restarts after the installer wizard closes.

3 Verify that you can log in to View Connection Server, and click **About** in View Administrator to verify that the new version is being used.

4 Go to **View Configuration > Product Licensing and Usage**, click **Edit License**, enter the VMware Horizon license key, and click **OK**.

5 Verify that you can log in to a remote desktop.

6 Repeat the previous steps to upgrade each View Connection Server instance in the group.

  IMPORTANT If you do not upgrade all View Connection Server instances in a replicated group, the health indicators in the View Administrator dashboard might show that one or more instances are in an error state. This situation arises because different versions supply different kinds of data. The solution is to upgrade all instances in the replicated group.

7 Use the `vdmexport.exe` utility to back up the newly upgraded View LDAP database.

  If you have multiple instances of View Connection Server in a replicated group, you need only export the data from one instance.

8 Verify or, if necessary, change the port number used for View Composer.

   a Edit the configuration for the vCenter Server instance and make sure that the View Composer port is set to `18443`.

     The port number must match the port number specified during the View Composer upgrade.

   b Supply the vCenter Server password.

   c Select the **Enable View Composer** check box and click **OK**.

9 Log in to View Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

   If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

   For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see "Accept the Thumbprint of a Default SSL Certificate," on page 38.

If the upgrade fails on one or more of the View Connection Server instances, see "Create a Replicated Group After Reverting View Connection Server to a Snapshot," on page 40.

If the upgrade is successful, upgrade the other View server components. If you use security servers, see "Upgrade View Security Server," on page 41.

If you ever reinstall View Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to View, you must ensure that the SSL certificates that are used for the vCenter Server and View Composer instances are valid and trusted by View Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by View Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but View Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

NOTE If you install vCenter Server and View Composer on the same Windows Server host, they can use the same SSL certificate, but you must configure the certificate separately for each component.

For details about configuring SSL certificates, see "Configuring SSL Certificates for View Servers" in the *View Installation* document.

You first add vCenter Server and View Composer in View Administrator by using the Add vCenter Server wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer.

After these servers are added, you can reconfigure them in the Edit vCenter Server dialog box.

NOTE You also must accept a certificate thumbprint when you upgrade from an earlier release and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the View Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. You must click **Verify** and follow the procedure shown here.

Similarly, in View Administrator you can configure a SAML authenticator for use by a View Connection Server instance. If the SAML server certificate is not trusted by View Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML authenticator in View. After a SAML authenticator is configured, you can reconfigure it in the Edit View Connection Server dialog box.

Procedure

1 When View Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.

2 Examine the certificate thumbprint in the Certificate Information window.

3 Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.

   a On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.

   b Navigate to the vCenter Server or View Composer certificate.

   c Click the Certificate Details tab to display the certificate thumbprint.

   Similarly, examine the certificate thumbprint for a SAML authenticator. If appropriate, take the preceding steps on the SAML authenticator host.

4 Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.

   Similarly, verify that the thumbprints match for a SAML authenticator.

5 Determine whether to accept the certificate thumbprint.

Option	Description
The thumbprints match.	Click **Accept** to use the default certificate.
The thumbprints do not match.	Click **Reject**. Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.

Upgrade to the Latest Version of View Connection Server on a Different Machine

As part of your upgrade, you can migrate View Connection Server to a new machine. For example, if you have View 4.6.x Connection Server on a 32-bit Windows 2003 Server machine, you can migrate to a 64-bit Windows Server 2008 R2 machine.

Prerequisites

- Upgrade at least one existing View Connection Server instance to the latest version. See "Upgrade View Connection Servers in a Replicated Group," on page 36. During this upgrade, your existing View LDAP will be upgraded.

- Verify that the new physical or virtual machine meets the system requirements for installing View Connection Server. See "Supported Operating Systems for View Connection Server," on page 16 and "Hardware Requirements for View Connection Server," on page 16.
- Familiarize yourself with the security-related requirements of View, and verify that these requirements are met. See "Upgrade Requirements for View Connection Server," on page 16.
- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have a domain user account with administrative privileges on the host you will use to run the installer.
- Familiarize yourself with the procedure for installing a replicated instance. See the *View Installation* document. You install a replicated instance as part of this procedure.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

1 Verify that an upgraded instance of View Connection Server is running and is accessible to the new machine where you plan to install View Connection Server.

When you install View Connection Server on the new host, you will point to this existing instance.

2 On the new machine, install a replicated instance of View Connection Server.

The View LDAP on the new instance will replicate that of the upgraded source instance.

3 If applicable, uninstall View Connection Server from the old host by using the Windows **Add/Remove Programs** utility.

4 In View Administrator, go to **View Configuration > Servers > Connection Servers** tab and determine whether the View Connection Server instance that was uninstalled still appears in the list.

5 If the uninstalled View Connection Server instance still appears in the list, use a `vdmadmin` command to remove it.

```
vdmadmin.exe –S –s server_name –r
```

In this example, *server_name* is the host name or IP address of the View Connection Server host. For more information about the `vdmadmin` command-line tool, see the *View Administration* document.

A new instance of View Connection Server is added to a group and an old instance is removed.

What to do next

Upgrade the other View server components..

If you ever reinstall View Connection Server on a server that has a data collector set configured to monitor performance data, stop the data collector set and start it again.

Create a Replicated Group After Reverting View Connection Server to a Snapshot

If an upgrade fails, or if for some other reason, you must revert a virtual machine that hosts View Connection Server to a snapshot, you must uninstall the other View Connection Server instances in the group and recreate the replicated group.

If you revert one View Connection Server virtual machine to a snapshot, the View LDAP objects in the database of that virtual machine are no longer consistent with the View LDAP objects in the databases of the other replicated instances. After you revert to a snapshot, the following event is logged in the Windows Event log, in the VMwareVDMDS Event log (Event ID 2103): `The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure.` The reverted virtual machine stops replicating its View LDAP.

If you find it necessary to revert to a snapshot, you must uninstall other View Connection Server instances and uninstall the View LDAP on those virtual machines and then reinstall replica instances.

Prerequisites

Determine which View Connection Server instance is to be the new standard, or master, View Connection Server. This Connection Server has the desired View configuration data.

Procedure

1 On all View Connection Server instances except the one chosen to be the new standard View Connection Server instance, uninstall View Connection Server and the View LDAP instance.

   The View LDAP instance is called AD LDS Instance VMwareVDMDS.

2 On the virtual machine that hosts the standard, or master, View Connection Server instance, open a command prompt and enter the following command to ensure that replication is not disabled.

```
repadmin /options localhost:389 –DISABLE_OUTBOUND_REPL –DISABLE_INBOUND_REPL
```

3 On the virtual machines that are to host the replica View Connection Server instances, run the View Connection Server installer, select the **View Replica Server** installation option, and specify the host name or IP address of the standard View Connection Server instance.

The replicated group of View Connection Server instances is recreated and their View LDAP objects are consistent.

Upgrade View Security Server

After you upgrade View Connection Server, you can upgrade the security servers that are paired with it.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance.
- Verify that you have upgraded View Connection Server. For instructions, see "Upgrade View Connection Servers in a Replicated Group," on page 36.
- Verify that the virtual or physical machine on which the current security server is installed meets the system requirements.

  See "View Connection Server Requirements," on page 16.
- Familiarize yourself with the security-related requirements of View, and verify that these requirements are met. See "Upgrade Requirements for View Connection Server," on page 16. You might need to obtain and install a CA-signed SSL server certificate that includes certificate revocation information, verify that Windows Firewall with Advanced Security is set to on, and configure any back-end firewalls to support IPsec.
- Verify that you have a user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- If you have not configured a security server pairing password, use the latest version of View Administrator to do so. The installation program will prompt you for this password during installation. See the topic called "Configure a Security Server Pairing Password" in the *View Installation* document.
- If you are upgrading a View 5.1 or later security server, remove existing IPsec rules for the security server. See "Prepare to Upgrade or Reinstall a Security Server," on page 24.

You do not need to make any changes to the configuration of existing load balancers.

Procedure

1 Run the installer for the latest version of View Connection Server.

The installer determines that an older version is already installed and performs an upgrade. The installer displays fewer installation options than during a fresh installation.

You will be prompted to supply the security server pairing password.

You might be prompted to dismiss a message box notifying you that the Security Server service was stopped. The installer stops the service in preparation for the upgrade.

2 After the installer wizard is finished, verify that the VMware Horizon View Security Server service is started.

3 Log in to View Administrator, select the security server in the Dashboard, and verify that the security server is now at the latest version.

4 Verify that you can log in to a remote desktop.

5 In View Administrator, go to **View Configuration > Servers > Security Servers** tab and remove any duplicate security servers from the list.

The automated security server pairing mechanism can produce duplicate entries in the **Security Servers** list if the full system name does not match the name that was assigned when the security server was originally created.

What to do next

Upgrade the other View server components, such as vCenter Server. See Chapter 5, "Upgrading View Server Components," on page 27.

If you have finished upgrading View server components, at your next maintenance window, continue with the View upgrade.

- If you are also upgrading vSphere components, see Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45.
- If you upgrading only View components, see "Upgrade View Agent," on page 48.

Upgrade vCenter Server

Perform a vCenter Server upgrade as part of the same maintenance window during which you upgrade other View server components. Before you upgrade vCenter Server, you must back up some View data. After the upgrade, if View Composer is running on the same server, you must restart the View Composer service.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. For information about how much time is required, see the *VMware vSphere Upgrade Guide*.
- Back up the vCenter Server database and the View Composer database.
- Back up the View LDAP database from a View Connection Server instance by using the `vdmexport.exe` utility.

  For instructions, see the *View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.
- Perform the tasks listed in "Preparing for Upgrades That Include vSphere," on page 21.

- Verify that the server on which vCenter Server is installed has a CA (certificate authority)-signed SSL server certificate installed and configured. After you upgrade View Connection Server, if vCenter Server does not use a CA-signed certificate, the default self-signed certificate is shown as invalid in View Administrator, and a message indicates that vCenter Server is unavailable.
- Complete the prerequisites listed in the *VMware vSphere Upgrade Guide*, using the version of the guide that corresponds to the version of vSphere that you plan to upgrade to.

Procedure

1 Upgrade vCenter Server as described in the *VMware vSphere Upgrade Guide*.

2 If View Composer is installed on the same host, restart the View Composer service.

3 Log in to View Administrator and examine the dashboard to verify that the vCenter Server and View Composer icons are green.

   If either of these icons is red and an Invalid Certificate Detected dialog box appears, you must click **Verify** and either accept the thumbprint of the untrusted certificate, as described in "What to Do Next," or install a valid CA-signed SSL certificate.

   For information about replacing the default certificate for vCenter Server, see the *VMware vSphere Examples and Scenarios* document.

What to do next

To use a default or self-signed certificate from vCenter Server or View Composer, see "Accept the Thumbprint of a Default SSL Certificate," on page 38.

If you have finished upgrading View server components, at your next maintenance window, continue with the View upgrade.

- If you are also upgrading vSphere components, see Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45.
- If you upgrading only View components, see "Upgrade View Agent," on page 48.

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-View-Extras-Bundle-x.x.x-yyyyyyy.zip`, where *x.x.x* is the version and *yyyyyyy* is the build number. You can download the file from the VMware Horizon (with View) download site at http://www.vmware.com/go/downloadview.

To upgrade group policies, simply use the Group Policy Object Editor on your Active Directory server to add the new version of the template files.

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.

Upgrade ESXi Hosts and Their Virtual Machines

6

Upgrading ESXi hosts and virtual machines is the most time-consuming aspect of this middle phase of a View upgrade.

This procedure provides an overview of the tasks you must perform during the second and subsequent maintenance windows. To complete some of these tasks, you might need step-by-step instructions found in the *VMware vSphere Upgrade Guide* and the *View Administrattion* document.

For details about which versions of View are compatible with which versions of vCenter Server and ESXi, see the VMware Product Interoperability Matrix at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

IMPORTANT To use the space-efficient disk format feature for linked-clone pools, you must upgrade vCenter Server, ESXi hosts, virtual machines, and the VMware Tools software in the virtual machines to VMware vSphere 5.1 or later.

To use the VMware® Virtual SAN™ feature, you must upgrade to vSphere 5.5 Update 1 or later.

Prerequisites

- Complete the procedure described in "Upgrade View Connection Servers in a Replicated Group," on page 36.
- Perform the ESXi upgrade preparation tasks listed in the *VMware vSphere Upgrade Guide*.

Procedure

1 Upgrade ESXi hosts, cluster by cluster.

   For instructions, see the *VMware vSphere Upgrade Guide*. If you have many clusters, this step could take several maintenance windows to complete. Upgrading ESXi hosts might include the following tasks:

   a Use VMware vSphere® vMotion® to move the virtual machines off of the ESXi host.

   b Put the host into maintenance mode.

   c Perform the upgrade.

   d Use VMotion to move the virtual machines back onto the host.

   e Perform post-upgrade tasks for ESXi hosts.

   Every host must be a member of a cluster, as mentioned in the prerequisites.

2 If an upgraded host does not reconnect itself to vCenter Server, use vSphere Client to reconnect the host to vCenter Server.

3 If you use View Composer, after all ESXi hosts are upgraded, on the vCenter Server host, restart the View Composer service.

4 (Optional) Upgrade VMware® Tools™ and the virtual machines on all parent virtual machines, virtual machine templates, and virtual machines that host View server components such as View Connection Server instances.

   a Plan for down time, as described in the *VMware vSphere Upgrade Guide*.

   b Update VMware Tools, and upgrade the virtual machine hardware for virtual machines that will be used as sources for remote desktops.

      To use the Windows 7 3D rendering feature, you must upgrade the virtual machine hardware to version 8 or later.

      To use the space-efficient disk format feature, you must upgrade the virtual machine hardware to version 9 or later. This feature pertains to linked-clone pools.

      If you use VMware vSphere® Update Manager™, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

5 (Optional) If you use full-clone desktops, on each virtual machine, upgrade VMware Tools and the virtual hardware for virtual machines that will be used as sources for remote desktops.

   To use the Windows 7 3D rendering feature, you must upgrade the virtual machine hardware to version 8 or later.

   If you use vSphere Update Manager, you can update VMware Tools and then the virtual hardware version in the correct order for all the virtual machines in a particular folder. See the *VMware vSphere Upgrade Guide*.

What to do next

Upgrade View Agent. See "Upgrade View Agent," on page 48.

Upgrading Remote Desktops and Horizon Client 7

The remote desktop and the client components that you can upgrade include Horizon Client for any of the supported desktop and mobile client platforms, thin clients provided by VMware partners, and the View Agent, which runs inside the operating systems of remote desktops and Microsoft RDS hosts.

This chapter includes the following topics:

Upgrade RDS Hosts That Provide Session-Based Desktops

On RDS hosts with Windows Server 2008 R2 or a later operating system, you can upgrade the View Agent software and edit pool settings so that the RDS host can provide remote desktops and remote Windows-based applications.

With VMware Horizon 6.0, you can use Microsoft RDS hosts to provide remote applications, in addition to remote desktops. With this added functionality, the previously hidden server farm name is displayed in View Administrator.

Prerequisites

- Verify that at least one View Connection Server instance in the replicated group has been upgraded. View Connection Server must be upgraded first so that the secure JMS pairing mechanism can work with View Agent.
- Verify that the RDS host currently hosting remote desktops is running Windows Server 2008 R2. Windows Server 2008 (Terminal Services) was supported for earlier versions of View but is not a supported operating system for this release. If you do not have Windows Server 2008 R2, you must do a fresh installation rather than an upgrade. For a list of supported operating systems, see "Supported Operating Systems for View Agent," on page 18.
- Verify that the RDS Host role is installed in the operating system. See the procedure called "Install Remote Desktop Services on Windows Server 2008 R2" in the *Setting Up Desktop and Application Pools in View* document.

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.

Procedure

1 In View Administrator, edit the desktop pool settings for the pool to disable the pool.

Go to **Catalog > Desktop Pools**, select the pool, and click **Edit**.

2 On the Windows Server 2008 R2 RDS host, download and run the installer for the new version of View Agent.

You can download the installer from the VMware Web site.

3 In View Administrator, edit the farm settings and set the default display protocol to **PCoIP**.

Go to **Resources > Farms**, select the farm, and click **Edit**.

You can also use a setting that allows the end user to choose the protocol. To use remote applications, the protocol must be PCoIP.

4 In View Administrator, edit the desktop pool settings for the pool to enable the pool.

This host can now provide remote applications in addition to remote desktops. In View Administrator, if you go to **Catalog > Desktop Pools**, you see that the type of pool is **RDS Desktop Pool**. If you go to **Resources > Farms**, you see a farm ID in the list that corresponds to the pool ID.

What to do next

Upgrade the clients. See "Upgrade the Client Application," on page 54.

Upgrade View Agent

The strategy for upgrading View Agent depends on the type of desktop source.

NOTE To upgrade the operating system in a virtual machine desktop from Windows 8 to Windows 8.1, you must uninstall View Agent, upgrade the operating system from Windows 8 to Windows 8.1, and then reinstall View Agent. Alternatively, you can perform a fresh installation of Windows 8.1 and then install View Agent.

This procedure provides an overview of the tasks you must perform to upgrade from View Agent in virtual machines used as desktop sources. To complete some of these tasks, you might need the step-by-step instructions found in the vSphere Client online help or in *Setting Up Desktop and Application Pools in View*, available by clicking the **Help** button in View Administrator. To upgrade View Agent on a Terminal Services host or Microsoft RDS host, see "Upgrade RDS Hosts That Provide Session-Based Desktops," on page 47.

IMPORTANT The View Agent installer now includes all components that were previously included in the Remote Experience Agent, which was part of the VMware Horizon™ View™ Feature Pack. To upgrade features that were installed with the Remote Experience Agent, you can simply run the View Agent installer. This installer removes the Remote Experience Agent before performing the upgrade. If, for some reason, you decide to manually remove the Remote Experience Agent, be sure to do so before you run the installer for the new version of View Agent.

Prerequisites

- Verify that at least one View Connection Server instance in the replicated group has been upgraded. View Connection Server must be upgraded first so that the secure JMS pairing mechanism can work with View Agent.
- If you are upgrading ESXi hosts and virtual machines, complete the procedure described in Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45.

- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.

Procedure

1 If you use View Composer, upgrade the View Agent on a parent virtual machine and create a desktop pool for testing purposes.

   a Download and run the new version of the View Agent installer on a parent virtual machine.

   You can download the installer from the VMware Web site.

   b Create a small linked-clone desktop pool from this virtual machine.

   c Test a virtual machine desktop from the desktop pool to verify that all the usage scenarios function properly.

   For example, create a desktop pool that contains one virtual machine desktop, and verify that you can use Horizon Client to log in to that desktop.

   Step-by-step instructions for running the View Agent installer and creating desktop pools appear in *Setting Up Desktop and Application Pools in View*, available by clicking the **Help** button in View Administrator.

IMPORTANT If you are upgrading from View 5.1.x or earlier, and you use Sysprep, and your end users will connect USB devices to their remote desktops, you must follow the procedure described in the VMware Knowledge Base, at http://kb.vmware.com/kb/2051801. Otherwise, after you upgrade to View Agent 6.0, the USB redirection feature might not work.

---

2 On the other parent virtual machines and virtual machine templates, download and run the installer for the vew version of View Agent.

   Step-by-step instructions for running the View Agent installer and creating desktop pools appear in *Setting Up Desktop and Application Pools in View*, available by clicking the **Help** button in View Administrator.

3 If you use View Composer, take a snapshot of each upgraded parent virtual machine that you use to create linked-clone desktop pools.

   You use the new snapshot for recomposing all the virtual machines in the pool.

   For instructions on taking snapshots, see the vSphere Client online help.

4 If you use full-clone desktops or other virtual machines that you added as individual desktops or as part of a manual pool, upgrade View Agent by using whatever third-party tools you usually use for software upgrades.

5 For automated and manual Windows 7 and 8 pools that are not linked-clone pools, to turn on the 3D rendering feature, edit the pool and power the virtual machine desktops off and on.

   a Configure the following pool settings:

      - Set the pool to use the PCoIP display protocol.
      - Set **Allow users to choose protocol** to **No**.
      - Turn on the **3D Rendering** feature.

   b Power off each virtual machine and power it on again.

   Restarting a virtual machine, rather than powering off and on, does not cause the setting to take effect.

6 If you use physical PCs as desktop sources, download and run the installer for the new version of View Agent on these physical machines.

You can download the installer from the VMware Web site.

7 Use a Horizon Client that has not been upgraded to verify that you can log in to the upgraded remote desktop sources with your old client software.

What to do next

If you use View Composer desktop pools, recompose or recreate the pools. See "Upgrade View Composer Desktop Pools," on page 50.

Upgrade clients. See "Upgrade the Client Application," on page 54.

Upgrade View Composer Desktop Pools

Part of the final phase of a View upgrade includes upgrading View Composer desktop pools.

Upgrading pools that were created with View Composer requires that you use a snapshot taken after upgrading View Agent on the parent virtual machine.

IMPORTANT If you use View Composer linked clones and you want to use the space reclamation feature available with vSphere 5.1 and later virtual machines, you must configure certain settings in View LDAP and in View Administrator, in addition to performing the steps in this procedure. For a complete list of tasks, see "Tasks for Upgrading Desktop Pools to Use Space Reclamation," on page 51.

NOTE If you are also upgrading the virtual hardware version, such as upgrading to virtual hardware version 8 or later, included with vSphere 5 or later, the snapshot of the upgraded parent virtual machine is used to upgrade the virtual hardware version of the rest of the virtual machines in the linked-clone pool.

Upgrading in this way, from one virtual hardware version (or compatibility level) to a higher version, is supported. You cannot, however, recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.

Prerequisites

- Complete the procedure described in "Upgrade View Composer," on page 27.
- Complete the procedure described in "Upgrade View Connection Servers in a Replicated Group," on page 36.
- If you are also upgrading ESXi hosts and virtual machines, complete the procedure described in Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45.

  To use the 3D rendering feature, you must upgrade the virtual hardware version to 8 or later in Windows 7 and 8 virtual machines.

  To use the space-efficient disk format feature, you must upgrade vCenter Server, ESXi hosts, virtual machines, and the VMware Tools software in the virtual machines to VMware vSphere 5.1 or later. That is, the virtual machines must use virtual hardware version to 9 or later.
- Complete the procedure described in "Upgrade View Agent," on page 48 for upgrading the agent in the parent virtual machine.

  IMPORTANT If you are upgrading from View 5.1.x or earlier, and you use Sysprep, and your end users will connect USB devices to their remote desktops, you must follow the procedure described in the VMware Knowledge Base, at http://kb.vmware.com/kb/2051801. Otherwise, after you upgrade to View Agent 6.0, the USB redirection feature might not work.

- Plan maintenance windows carefully so that recreating and recomposing desktop pools will not overwhelm the storage array and ESXi hosts.

Procedure

1 If you disabled provisioning of new virtual machines in preparation for the upgrade, enable provisioning again.

2 For pools composed of Windows 7 or 8 desktops, to turn on the 3D rendering feature, edit the pool to configure the following settings:

   - Set the pool to use the PCoIP display protocol.
   - Set **Allow users to choose protocol** to **No.**
   - Turn on the **3D Rendering** feature.

   This feature is available for Windows 7 and 8 desktops that use virtual hardware version 8 or later, available with vSphere 5 or later.

3 To enable the space reclamation feature available with vSphere 5.1 virtual machines, in the **Advanced Storage** section of pool settings, select **Reclaim VM disk space**, and set the threshold for space reclamation to 1GB.

4 To enable View Storage Accelerator, available with vSphere 5.0 or later virtual machines, in the **Advanced Storage** section of pool settings, verify that the **Use View Storage Accelerator** check box is selected.

   View Storage Accelerator can improve performance during boot storms and anti-virus scanning I/O storms by allowing ESXi 5.0 and later hosts to cache common virtual machine disk data.

   IMPORTANT This feature is turned on by default. View Storage Accelerator requires 1GB of RAM per ESXi host.

5 Use the snapshot you created after upgrading the parent virtual machine to recompose desktop pools.

6 If you changed the **Refresh OS disk on logoff** setting for a pool to **Never** in preparation for the upgrade, change the setting back to reflect the appropriate refresh policy.

7 If you canceled any refresh or recompose operations for any desktop pools, schedule the tasks again.

What to do next

Upgrade the clients. See "Upgrade the Client Application," on page 54.

Tasks for Upgrading Desktop Pools to Use Space Reclamation

Starting with vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones. Upgrading pools to use this feature involves changing settings in vCenter Server, View LDAP, and pool settings and then recomposing the pool.

NOTE The space reclamation feature is not supported if your virtual machine desktops are hosted on Virtual SAN datastores.

Although the space reclamation feature reduces the amount of disk space used for a virtual machine, it can reclaim only space that is not used. This feature cannot reclaim disk space created by virtual machines that have not been optimized. To optimize an operating system image, you can turn off Windows services such as the indexer service, the defragmenter service, and restore points. For details, see the topics "Optimize Windows Guest Operating System Performance," "Optimize Windows 7 and Windows 8 Guest Operating System Performance," and "Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops," in *Setting Up Desktop and Application Pools in View*.

IMPORTANT Because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

1 If all vCenter Server instances and ESXi hosts for the pool are not at VMware vSphere 5.1 or later, upgrade them to 5.1 or later.

   For instructions, see the *VMware vSphere Upgrade Guide*.

2 If all virtual machine desktops in the pool are not VMware vSphere 5.1 (virtual hardware version 9) or later virtual machines, upgrade them.

   - In the parent virtual machine, upgrade VMware Tools to the latest VMware vSphere 5.1 or later version, and upgrade the virtual machine to the latest version, which must be virtual hardware version 9 or later.

     For instructions, see the *VMware vSphere Upgrade Guide*.

   - Take a snapshot of the parent virtual machine. For instructions on taking snapshots, see the vSphere Client online help.

   - Use the snapshot of the parent virtual machine you just created to recompose the desktop pool. For instructions on recomposing pools, click the **Help** button in View Administrator.

   Recomposing the pool from a snapshot of an upgraded virtual machine is just one method of upgrading all virtual machines in a linked-clone pool. You can also upgrade the virtual machines one by one.

3 Upgrade the disk format used for the virtual machines.

   - On the View Connection Server host, use ADSIEdit to navigate to the server group that corresponds to the pool, and change the value in the **pae-UseSeSparseFormat** field from **0** to **1**.

   - Recompose the desktop pool.

4 Use View Administrator to edit the vCenter Server settings, navigate to the **Storage** tab, and select **Reclaim VM disk space**.

   For instructions on editing server settings, click the **Help** button in View Administrator.

5 Use View Administrator to edit the pool settings, navigate to the **Advanced Storage** section, select **Reclaim VM disk space**, and set the threshold for space reclamation to 1GB.

Tasks for Upgrading Desktop Pools to Use a Virtual SAN Datastore

Starting with vSphere 5.5 Update 1, you can use the Virtual SAN feature for high-performance storage and policy-based management. Upgrading pools to use this feature involves changing a pool setting and then rebalancing the pool.

With Virtual SAN, the locally attached physical storage disks available on a cluster of vSphere hosts are aggregated into one virtual datastore. You specify this 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).

View defines virtual machine storage requirements, such as capacity, performance, and availability, in the form of default storage policy profiles, depending on the pool settings used. Storage is provisioned and automatically configured according to the assigned policies.

NOTE The space reclamation feature is not supported if your virtual machine desktops are hosted on Virtual SAN datastores.

Upgrading from View 5.3.1 on a Virtual SAN Datastore

Horizon 6.0 with View introduced some new default storage policies for Virtual SAN. These policies will not automatically apply to existing virtual machine desktops created on Virtual SAN by View 5.3.1 after the desktop pool is upgraded to 6.0. In addition, when you upgrade from View 5.3.1, the **Use VMware Virtual SAN** pool setting will not automatically be enabled, even if the pool is on a Virtual SAN datastore. You have the following upgrade options:

- After upgrading, continue to use the default storage policies that were used with View 5.3.1. If you choose this option, edit the pool settings so that **Use VMware Virtual SAN** is enabled.
- Use the procedure described in this topic so that the desktop pool uses the new default storage policies. This procedure involves rebalancing the desktop pool to a non-Virtual SAN datastore and then upgrading and rebalancing back to the Virtual SAN datastore.

IMPORTANT The tasks outlined in this procedure describe upgrading from a View 5.3.1 desktop pool using a Virtual SAN datastore on a VMware vSphere 5.5 Update 1 cluster. Upgrading from Virtual SAN datastore on a VMware vSphere 5.5 or earlier cluster (a Tech Preview feature) is not supported.

Also, because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

1. Verify that all virtual machines in the pool are VMware vSphere 5.5 Update 1 or later virtual machines.
2. Edit the pool settings of the desktop pool to change the datastore from a Virtual SAN datastore to a non-Virtual SAN datastore, and use the **Rebalance** command.

   For instructions on editing server settings and using the **Rebalance** command, click the **Help** button in View Administrator.
3. Upgrade the desktop pool to the latest version, as described in "Upgrade View Composer Desktop Pools," on page 50.

   This process includes installing the latest version of View Agent on the parent virtual machine and taking a snapshot.
4. Recompose the pool on the non-Virtual SAN datastore using the snapshot of the parent virtual machine you just created.

   For instructions on recomposing pools, click the **Help** button in View Administrator.
5. Edit the pool settings of the newly upgraded desktop pool to change the datastore from a non-Virtual SAN datastore to a Virtual SAN datastore, and use the **Rebalance** command.

Upgrading from a Non-Virtual SAN Datastore to a Virtual SAN Datastore

The tasks outlined in this procedure describe upgrading from a non-Virtual SAN datastore to a Virtual SAN datastore. Upgrading from Virtual SAN datastore on a VMware vSphere 5.5 or earlier cluster (a Tech Preview feature) is not supported.

IMPORTANT Because this procedure involves recomposing the desktop pool, any changes that end users have made to the operating system disk will be lost.

1. Verify that all ESXi hosts in the cluster used for the pool are upgraded to 5.5 Update 1 or later and that they meet the system requirements for the Virtual SAN feature.

   For information about upgrades, see Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45 and see the *VMware vSphere Upgrade Guide*. For information about Virtual SAN requirements, see the *vSphere Storage* document.

2. If all virtual machines in the pool are not VMware vSphere 5.5 Update 1 or later virtual machines, upgrade them.

   For instructions, see Chapter 6, "Upgrade ESXi Hosts and Their Virtual Machines," on page 45 and see the *VMware vSphere Upgrade Guide*.

3. Use vCenter Server 5.5 Update 1 or later to enable Virtual SAN for the vSphere cluster.

   For more information, see the *vSphere Storage* document.

4. Upgrade the desktop pool to the latest version, as described in "Upgrade View Composer Desktop Pools," on page 50.

   This process includes installing the latest version of View Agent on the parent virtual machine and taking a snapshot.

5. Recompose the pool on the non-Virtual SAN datastore using the snapshot of the parent virtual machine you just created.

   For instructions on recomposing pools, click the **Help** button in View Administrator.

6. Edit the pool settings of the newly upgraded desktop pool to enable the **Use VMware Virtual SAN** pool setting, change the datastore from a non-Virtual SAN datastore to a Virtual SAN datastore, and use the **Rebalance** command.

   For instructions on editing server settings and using the **Rebalance** command, click the **Help** button in View Administrator.

Upgrade the Client Application

The final phase of a View upgrade includes upgrading to the latest version of Horizon Client and upgrading the firmware on thin client devices if you use them.

The Local Mode feature for Horizon Client has been removed. In its place, VMware recommends using Mirage, which is included with VMware Horizon 6. For more information, see the View Release Notes, available at https://www.vmware.com/support/pubs/view_pubs.html.

IMPORTANT Upgrading involves running the new version of the Horizon Client installer without first removing the older version of the client application. If your end users have the Windows-based View Client 4.6.0 or an earlier version, instruct them to remove the client software before downloading and running the latest Horizon Client installer.

Prerequisites

- Complete the procedures for upgrading the server components, which can include View Connection Server and View Composer. See Chapter 5, "Upgrading View Server Components," on page 27.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the installer and perform the upgrade.
- Verify that the client desktop, laptop, tablet, or phone meets the operating system requirements and hardware requirements of Horizon Client. See the "Using 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.

Procedure

1 Have end users upgrade to the latest version of Horizon Client.

Option	Action
Horizon Client	Download and send the Horizon Client installers to your end users or post them on a Web site and ask end users to download the installer and run it. You can download the installers or have your end users download them from the VMware Web site at https://www.vmware.com/go/viewclients. For mobile clients, you can alternatively instruct your end users to get the latest version of Horizon Client from other Web sites that sell apps, including the Apple App Store, Google Play, Amazon, and Windows Store.
VMware Horizon user Web portal	End users can open a browser and browse to a View Connection Server instance. The Web page that appears is called the VMware Horizon user Web portal, and it contains links for downloading the installer file for Horizon Client. NOTE The default links in Web page point to the Horizon Client download site. You can change the default links to point elsewhere. See "Configure the VMware Horizon Web Portal Page for End Users," on page 55.
Thin client	Upgrade the thin client firmware and install the new Horizon Client software on end users' client devices. Thin clients and zero clients are provided by VMware partners.

2 Have end users verify that they can log in and connect to their remote desktops.

Configure the VMware Horizon Web Portal Page for End Users

You can configure this Web page to show or hide the icon for downloading Horizon Client or the icon for connecting to a remote desktop through HTML Access. You can also configure other links on this page.

By default, the portal page shows both an icon for downloading and installing the native Horizon Client and an icon for connecting through HTML Access. In some cases, however, you might want to have the links point to an internal Web server, or you might want to make specific client versions available on your own server. You can reconfigure the page to point to a different URL.

You can make installer links for specific client operating systems. For example, if you browse to the portal page from a Mac OS X system, the link for the native Mac OS X installer appears. For Windows clients, you can make separate links for 32-bit and 64-bit installers.

IMPORTANT If you upgraded from View Connection Server 5.x or an earlier release and did not have the HTML Access component installed, and if you previously edited the portal page to point to your own server for downloading Horizon Client, those customizations might be hidden after you install View Connection Server 6.0 or later. With Horizon 6 or later, the HTML Access component is automatically installed during an upgrade of View Connection Server.

If you already installed the HTML Access component separately for View 5.x, any customizations you made to the Web page are preserved. If you did not have the HTML Access component installed, any customizations you had made are hidden. The customizations for earlier releases reside in the `portal-links.properties` file, which is no longer used.

Procedure

1 On the View Connection Server host, open the `portal-links-html-access.properties` file with a text editor.

The location of this file is *`CommonAppDataFolder`*`\VMware\VDM\portal\portal-links-html-access.properties`. For Windows Server 2008 operating systems, the *CommonAppDataFolder* directory is `C:\ProgramData`. To display the `C:\ProgramData` folder in Windows Explorer, you must use the Folder Options dialog box to show hidden folders.

NOTE Customizations for View 5.x and earlier releases resided in the `portal-links.properties` file, which is located in the same *`CommonAppDataFolder`*`\VMware\VDM\portal\` directory as the `portal-links-html-access.properties` file.

2 Edit the configuration properties to set them appropriately.

By default, both the installer icon and the HTML Access icon are enabled and a link points to the client download page on the VMware Web site. To disable an icon, which removes the icon from the Web page, set the property to `false`.

Option	Property Setting
Disable HTML Access	`enable.webclient=false` If this option is set to false but the `enable.download` option is set to true, the user is taken to a Web page for downloading the native Horizon Client installer. If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Disable downloading Horizon Client	`enable.download=false` If this option is set to false but the `enable.webclient` option is set to true, the user is taken to the HTML Access login Web page. If both options are set to false, the user sees the following message: `"Contact your local administrator for instructions on accessing this Connection Server."`
Change the URL of the Web page for downloading Horizon Client	`link.download=https://`*`url-of-web-server`* Use this property if you plan to create your own Web page.

Option	Property Setting

Create links for specific installers	The following examples show full URLs, but you can use relative URLs if you place the installer files in the `downloads` directory, which is under the `C:\Program Files\VMware\VMware View\Server\broker\webapps\` directory on View Connection Server, as described in the next step.
	■ 32-bit Windows installer:
	`link.win32=https://server/downloads/VMware-Horizon-Client.exe`
	■ 64-bit Windows installer:
	`link.win64=https://server/downloads/VMware-Horizon-Client.exe`
	■ Linux installer:
	`link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz`
	■ Mac OS X installer:
	`link.mac=https://server/downloads/VMware-Horizon-Client.dmg`
	■ iOS installer:
	`link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip`
	■ Android installer:
	`link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk`

Change the URL for the Help link	`link.help` By default, this link points to a help system hosted on the VMware Web site. The Help link appears in the upper-right corner of the screen. For the HTML Access login screen and the desktop selector screen, the Help link is a question mark icon. After you are logged in to a desktop, the Help link is a Help command in the drop-down menu on the right end of the client menu bar.

3 To have users download installers from a location other than the VMware Web site, place the installer files on the HTTP server where the installer files will reside.

This location must correspond to the URLs you specified in the `portal-links-html-access.properties` file from the previous step. For example, to place the files in a `downloads` folder on the View Connection Server host, use the following path:

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

The links to the installer files could then use relative URLs with the format `/downloads/`*`client-installer-file-name`*.

4 Restart the View Web Component service.

8 Applying View Patches

Patch releases can include installer files for the following View components: View Composer, View Connection Server, View Agent, and various clients. The patch components that you must apply depend on the bug fixes that your View deployment requires.

Depending on which bug fixes you require, install the applicable View components, in the following order:

1 View Composer

2 View Connection Server

3 View Agent

4 Horizon Client

This chapter includes the following topics:

Apply a Patch for View Composer

Applying a patch involves uninstalling the current version and then installing the patch version. Not all patch releases include patches for View Composer.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. Budget 15 minutes to half an hour for each instance of View Composer.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.
- If View Composer is installed in a virtual machine, take a snapshot of the virtual machine.

  For instructions on taking snapshots, see the vSphere Client online help.
- Back up the vCenter Server database and the View Composer database.

  For instructions on performing a database backup, see the documentation from your database vendor.
- For all linked-clone desktop pools, disable provisioning of new virtual machines.
- If any desktop pools are scheduled to do a refresh or recompose operation, cancel these tasks.

Procedure

1 On the virtual machine that hosts View Composer, download the installer file for the patch version of View Composer.

  Your contact at VMware will provide instructions for this download.

2 Use the Windows **Add/Remove Programs** utility to remove your previously installed View Composer.

3 Run the installer that you downloaded for the patch release of View Composer.

4 Verify that the VMware Horizon View Composer service restarts after the installer wizard closes.

5 If applicable, apply the patch for View Agent on a parent virtual machine and create a desktop pool for testing purposes.

  a Use the Windows **Add/Remove Programs** utility to remove your previously installed View Agent.

  b Download and run the View Agent patch installer on a parent virtual machine.

    Your contact at VMware will provide instructions for this download.

  c Create a small linked-clone desktop pool from this virtual machine.

  d Test a virtual desktop from the desktop pool to verify that all the usage scenarios function properly.

    For example, create a desktop pool that contains one virtual desktop, and verify that you can use Horizon Client to log in to that desktop.

    Step-by-step instructions for running the View Agent installer and creating desktop pools appear in *Setting Up Desktop and Application Pools in View*, available by clicking the **Help** button in View Administrator.

  e Verify that virtual desktops from the test desktop pool work as expected.

What to do next

Apply the patch to View Connection Server, if applicable.

Apply a Patch for View Connection Server

Applying a patch involves uninstalling the current version and then installing the patch version.

Prerequisites

- Determine when to perform this procedure. Choose an available desktop maintenance window. The amount of time required depends on the number of View Connection Server instances in the group. Budget 15 minutes to half an hour for each instance.
- Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.

Procedure

1 If View Connection Server is installed in a virtual machine, take a snapshot of the virtual machine.

  For instructions on taking snapshots, see the vSphere Client online help.

2 On one of the View Connection Server instances in a replicated group, download the installer file for the patch version of View Connection Server.

  Your contact at VMware will provide instructions for this download.

3 Use the Windows **Add/Remove Programs** utility to remove your previously installed View Connection Server, but do not remove **Adam Instance VMwareVDMDS**.

4 Run the installer that you downloaded for the patch release of View Connection Server.

For information about running the installer, see the *View Installation* document.

5 Follow the installation wizard prompts and click **OK** when asked to continue the installation with the existing ADAM instance.

6 Verify that the VMware Horizon View Connection Server service restarts after the installer wizard closes.

7 Repeat the previous steps for the other View Connection Server instances in the replicated group.

8 Repeat this process for View security servers.

What to do next

If applying the patch fails on one or more of the View Connection Server instances, see "Create a Replicated Group After Reverting View Connection Server to a Snapshot," on page 40.

Apply the patch to View Agent, if applicable.

Apply a Patch for View Agent

Applying a patch involves uninstalling the current version and then installing the patch version.

The following steps need to be performed on the parent virtual machine, for linked-clone desktop pools, or on each virtual machine desktop in a full-clone pool, or on individual desktop virtual machines for pools that contain only one virtual machine desktop.

Prerequisites

Verify that you have a domain user account with administrative privileges on the hosts that you will use to run the patch installer.

Procedure

1 On all parent virtual machines, virtual machines used for full-clone templates, full clones in a pool, and manually added individual virtual machines, download the installer file for the patch version of View Agent.

Your contact at VMware will provide instructions for this download.

2 Use the Windows **Add/Remove Programs** utility to remove the previously installed View Agent.

3 Run the installer that you downloaded for the patch release of View Agent.

Step-by-step instructions for running the View Agent installer appear in *Setting Up Desktop and Application Pools in View*.

4 If you disabled provisioning of new virtual machines in preparation for applying a patch to View Composer, enable provisioning again.

5 For parent virtual machines that will be used to create linked-clone desktop pools, take a snapshot of the virtual machine.

For instructions on taking snapshots, see the vSphere Client online help.

6 For linked-clone desktop pools, use the snapshot you created to recompose the desktop pools.

7 Verify that you can log in to the patched desktop pools with Horizon Client.

8 If you canceled any refresh or recompose operations for any linked-clone desktop pools, schedule the tasks again.

Apply a Patch for Horizon Client

On desktop client devices, applying a patch involves uninstalling the current version and then installing the patch version of Horizon Client. On mobile clients, applying a patch involves simply installing the update from the Web site that sells apps, such as Google Play, Windows Store, or the Apple App Store.

Procedure

1 On each client system, download the installer file for the patch version of Horizon Client.

Your contact at VMware will provide instructions for this download. As mentioned previously, for some clients, you might get the patch release from an app store.

2 If the client device is a desktop or laptop, remove the current version of the client software from your device.

Use the customary device-specific method for removing applications.

3 If applicable, run the installer that you downloaded for the patch release of the Horizon Client.

If you got the patch from the Apple App Store or Google Play, the app is usually installed when you download it, and you do not need to run an installer.

4 Verify that you can log in to the patched desktop pools with the newly patched Horizon Client.

Upgrading vSphere Components Separately in a View Environment

9

If you upgrade vSphere components separately from View components, you must back up some View data and reinstall some View software.

Instead of performing an integrated upgrade of View and vSphere components, you can choose to first upgrade all View components and then upgrade vSphere components, or the reverse. You might also upgrade only vSphere components when a new version or update of vSphere is released.

When you upgrade vSphere components separately from View components, you must perform the following additional tasks:

1 Before you upgrade vCenter Server, back up the vCenter Server database and the View Composer database.

2 Before you upgrade vCenter Server, back up the View LDAP database from a View Connection Server instance by using the `vdmexport.exe` utility.

   For instructions, see the *View Administration* document. If you have multiple instances of View Connection Server in a replicated group, you need to export the data from only one instance.

3 If you use View Composer, after you upgrade all ESXi hosts that are managed by a particular vCenter Server instance, restart the View Composer service on that host.

4 After you upgrade VMware Tools in virtual machines that are used as remote desktops, reinstall View Agent.

   Reinstalling View Agent guarantees that the drivers in the virtual machine remain compatible with the other View components.

   Step-by-step instructions for running the View Agent installer appear in *Setting Up Desktop and Application Pools in View*.

Index