VMware Horizon View Installation

View 5.2
View Manager 5.2
View Composer 5.2

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-001020-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

VMware Horizon View Installation

VMware Horizon View Installation explains how to install the VMware® Horizon View™ server and client components.

Intended Audience

This information is intended for anyone who wants to install VMware Horizon View. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

System Requirements for Server Components

1

Hosts that run VMware Horizon View server components must meet specific hardware and software requirements.

This chapter includes the following topics:

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 View desktop. View Connection Server has specific hardware, operating system, installation, and supporting software requirements.

- Hardware Requirements for View Connection Server on page 8

  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.

- Supported Operating Systems for View Connection Server on page 8

  You must install View Connection Server on a Windows Server 2008 R2 operating system.

- Virtualization Software Requirements for View Connection Server on page 8

  View Connection Server requires certain versions of VMware virtualization software.

- Network Requirements for Replicated View Connection Server Instances on page 8

  If you install replicated View Connection Server instances, configure the instances in the same location and connect them over a high-performance LAN.

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 1-1. View Connection Server Hardware Requirements

Hardware Component	Required	Recommended
Processor	Pentium IV 2.0GHz processor or higher	4 CPUs
Networking	One or more 10/100Mbps network interface cards (NICs)	1Gbps NICs
Memory Windows Server 2008 64-bit	4GB RAM or higher	At least 10GB RAM for deployments of 50 or more View 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 Windows Server 2008 R2 operating system.

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

Table 1-2. 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

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

Network Requirements for Replicated View Connection Server Instances

If you install replicated View Connection Server instances, configure the instances in the same location and connect them over a high-performance LAN.

When installing replicated View Connection Server instances, you must configure the instances in the same physical location and connect them over a high-performance LAN. Do not use a WAN, MAN (metropolitan area network), or other non-LAN to connect replicated View Connection Server instances.

Even a high-performance WAN, MAN, or other non-LAN with low average latency and high throughput might have periods when the network cannot deliver the performance characteristics that are needed for View Connection Server instances to maintain consistency.

If the View LDAP configurations on View Connection Server instances become inconsistent, users might not be able to access their desktops. A user might be denied access when connecting to a View Connection Server instance with an out-of-date configuration.

View Administrator Requirements

Administrators use View Administrator to configure View Connection Server, deploy and manage desktops, 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 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 *VMware Horizon 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.

View Composer Requirements

View Manager uses View Composer to 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 on page 10

  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.

- Hardware Requirements for Standalone View Composer on page 10

  With View 5.1 and later releases, View Composer is no longer required to be installed on the same physical or virtual machine as vCenter Server. If you install View Composer on a separate server, you must use a dedicated physical or virtual machine that meets specific hardware requirements.

- Database Requirements for View Composer on page 10

  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.

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 1-3. 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

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 10.

Hardware Requirements for Standalone View Composer

With View 5.1 and later releases, View Composer is no longer required to be installed on the same physical or virtual machine as vCenter Server. If you install View Composer on a separate server, you must use a dedicated physical or virtual machine that meets specific hardware requirements.

A standalone View Composer installation works with vCenter Server installed on a Windows Server computer and 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 1-4. 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 View 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 already exists for vCenter Server, View Composer can use that existing database server if it is a version listed in Table 1-5. For example, View Composer can use the Microsoft SQL Server 2005 or 2008 Express instance provided with vCenter Server. If a database server 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 Manager 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.

Table 1-5 lists the supported database servers and versions. For a complete list of database versions supported with vCenter Server, see the *VMware vSphere Compatibility Matrixes* on the VMware vSphere documentation Web site.

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 vSphere Compatibility Matrixes* on the VMware vSphere documentation Web site.

Table 1-5. Supported Database Servers for View Composer

Database	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1	vCenter Server 4.0
Microsoft SQL Server 2005 (SP4), Standard, Enterprise, and Datacenter (32- and 64-bit)	Yes	Yes	Standard only	Standard only
Microsoft SQL Server 2008 Express (R2 SP1) (64-bit)	Yes	Yes	No	No
Microsoft SQL Server 2008 (SP2), Standard, Enterprise, and Datacenter (32- and 64-bit)	Yes	Yes	Yes	Yes
Microsoft SQL Server 2008 (R2), 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)	Yes	Yes	Yes	Yes
Oracle 11g Release 2, Standard, Standard ONE, and Enterprise [11.2.0.1] with Patch 5 (32- and 64-bit)	Yes	Yes	Yes	Yes

NOTE If you use an Oracle 11g R2 database, you must install Oracle 11.2.0.1 Patch 5. This patch requirement applies to both 32-bit and 64-bit versions.

View Transfer Server Requirements

View Transfer Server is an optional View Manager component that supports check in, check out, and replication of desktops that run in local mode. View Transfer Server has specific installation, operating system, and storage requirements.

- Installation and Upgrade Requirements for View Transfer Server on page 12

  You must install View Transfer Server as a Windows application in a virtual machine that meets specific requirements.

- Supported Operating Systems for View Transfer Server on page 12

  You must install View Transfer Server on a supported operating system with at least the minimum required amount of RAM.

- Storage Requirements for View Transfer Server on page 13

  View Transfer Server transfers static content to and from the Transfer Server repository and dynamic content between local desktops and remote desktops in the datacenter. View Transfer Server has specific storage requirements.

Installation and Upgrade Requirements for View Transfer Server

You must install View Transfer Server as a Windows application in a virtual machine that meets specific requirements.

IMPORTANT If users will be checking out local desktops that use the space-efficient sparse disk format (SE-Flex), available starting with vSphere 5.1, View Transfer Server must be hosted on a vSphere 5.1 or later virtual machine (virtual hardware version 9). The SE Sparse disk format allows stale or deleted data within a guest operating system to be reclaimed with a wipe and shrink process.

To use the space reclamation feature, you must verify that your vCenter Server and hosts are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later. In an ESXi cluster, verify that all the hosts are version 5.1 with download patch ESXi510-201212001 or later.

The virtual machine that hosts View Transfer Server must meet several requirements regarding network connectivity:

- It must be managed by the same vCenter Server instance as the local desktops that it will manage.
- It does not have to be part of a domain.
- It must use a static IP address.

The View Transfer Server software cannot coexist on the same virtual machine with any other View Manager software component, including View Connection Server.

Do not manually add or remove PCI devices on the virtual machine that hosts View Transfer Server. If you add or remove PCI devices, View might be unable to discover hot-added devices, which might cause data transfer operations to fail.

You can install multiple View Transfer Server instances for high availability and scalability.

Supported Operating Systems for View Transfer Server

You must install View Transfer Server on a supported operating system with at least the minimum required amount of RAM.

Table 1-6. Operating System Support for View Transfer Server

Operating System	Version	Edition	Minimum RAM
Windows Server 2008 R2	64-bit	Standard Enterprise	4GB
Windows Server 2008 R2 SP1	64-bit	Standard Enterprise	4GB

IMPORTANT Configure two virtual CPUs for virtual machines that host View Transfer Server.

Storage Requirements for View Transfer Server

View Transfer Server transfers static content to and from the Transfer Server repository and dynamic content between local desktops and remote desktops in the datacenter. View Transfer Server has specific storage requirements.

- The disk drive on which you configure the Transfer Server repository must have enough space to store your static image files. Image files are View Composer base images.
- View Transfer Server must have access to the datastores that store the desktop disks to be transferred. The datastores must be accessible from the ESX/ESXi host where the View Transfer Server virtual machine is running.
- The recommended maximum number of concurrent disk transfers that View Transfer Server can support is 20.

  During a transfer operation, a local desktop's virtual disk is mounted on View Transfer Server. The View Transfer Server virtual machine has four SCSI controllers. This configuration allows multiple disks to be attached to the virtual machine at one time.
- Because local desktops can contain sensitive user data, make sure data is encrypted during its transit over the network.

  In View Administrator, you can configure data-transfer security options on each View Connection Server instance. To configure these options in View Administrator, click **View Configuration > Servers**, select a View Connection Server instance, and click **Edit**.
- When View Transfer Server is added to View Manager, its Distributed Resource Scheduler (DRS) automation policy is set to Manual, which effectively disables DRS.

  To migrate a View Transfer Server instance to another ESX host or datastore, you must place the instance in maintenance mode before you begin the migration.

  When View Transfer Server is removed from View Manager, the DRS automation policy is reset to the value it had before View Transfer Server was added to View Manager.

System Requirements for Guest Operating Systems

2

Systems running View Agent or Standalone View Persona Management must meet certain hardware and software requirements.

This chapter includes the following topics:

Supported Operating Systems for View Agent

The View Agent component assists with session management, single sign-on, and device redirection. You must install View Agent on all virtual machines, physical systems, and terminal servers that will be managed by View Manager.

Table 2-1. View Agent Operating System Support

Guest Operating System	Version	Edition	Service Pack
Windows 8	64-bit and 32-bit	Enterprise and Professional	N/A
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3
Windows 2008 R2 Terminal Server	64-bit	Standard	SP1
Windows 2008 Terminal Server	64-bit	Standard	SP2

To use the View Persona Management setup option with View Agent, you must install View Agent on Windows 8, Windows 7, Windows Vista, or Windows XP virtual machines. This option does not operate on physical computers or Microsoft Terminal Servers.

You can install the standalone version of View Persona Management on physical computers. See "Supported Operating Systems for Standalone View Persona Management," on page 16.

Supported Operating Systems for Standalone View Persona Management

The standalone View Persona Management software provides persona management for standalone physical computers and virtual machines that do not have View Agent 5.*x* installed. When users log in, their profiles are downloaded dynamically from a remote profile repository to their standalone systems.

NOTE To configure View Persona Management for View desktops, install View Agent with the **View Persona Management** setup option. The standalone View Persona Management software is intended for non-View systems only.

Table 2-2 lists the operating systems supported for the standalone View Persona Management software.

Table 2-2. Operating System Support for Standalone View Persona Management

Guest Operating System	Version	Edition	Service Pack
Windows 8	64-bit and 32-bit	Pro - Desktop and Enterprise - Desktop	N/A
Windows 7	64-bit and 32-bit	Enterprise and Professional	None and SP1
Windows Vista	32-bit	Business and Enterprise	SP1 and SP2
Windows XP	32-bit	Professional	SP3

The standalone View Persona Management software is not supported on Microsoft Terminal Services or Microsoft Remote Desktop Services.

Remote Display Protocol and Software Support

Remote display protocols and software provide access to the desktops of remote computers over a network connection. View Client supports the Microsoft Remote Desktop Protocol (RDP) and PCoIP from VMware.

- Horizon View with PCoIP on page 16

  PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

- Microsoft RDP on page 18

  Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

Horizon View with PCoIP

PCoIP provides an optimized desktop experience for the delivery of the entire desktop environment, including applications, images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP can compensate for an increase in latency or a reduction in bandwidth, to ensure that end users can remain productive regardless of network conditions.

PCoIP is supported as the display protocol for View desktops with virtual machines and with physical machines that contain Teradici host cards.

PCoIP Features

Key features of PCoIP include the following:

- Users outside the corporate firewall can use this protocol with your company's virtual private network (VPN), or users can make secure, encrypted connections to a View security server in the corporate DMZ.
- Advanced Encryption Standard (AES) 128-bit encryption is supported and is turned on by default. You can, however, change the encryption key cipher to AES-192 or AES-256.
- Connections to Windows desktops with the View Agent operating system versions listed in "Supported Operating Systems for View Agent," on page 15 are supported.
- Connections from all types of View clients.
- MMR redirection is supported for some Windows client operating systems and some View desktop (agent) operating systems. See "Feature Support Matrix" in the *VMware Horizon View Architecture Planning* document..
- USB redirection is supported for some client types.
- Audio redirection with dynamic audio quality adjustment for LAN and WAN is supported.
- Optimization controls for reducing bandwidth usage on the LAN and WAN.
- Multiple monitors are supported for some client types. For example, on Windows-based clients, you can use up to four monitors and adjust the resolution for each monitor separately, with a resolution of up to 2560x1600 per display. Pivot display and autofit are also supported.

  When the 3D feature is enabled, up to 2 monitors are supported with a resolution of up to 1920 X 1200.
- 32-bit color is supported for virtual displays.
- ClearType fonts are supported.
- Copy and paste of text and images between a Windows-based client operating system and a View desktop is supported, up to 1MB. Supported file formats include text, images, and RTF (Rich Text Format). You cannot copy and paste system objects such as folders and files between systems.

For information about which client devices support specific PCoIP features, go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Recommended Guest Operating System Settings

Recommended guest operating system settings include the following settings:

- For Windows XP desktops: 768MB RAM or more and a single CPU.
- For Windows 7 or 8 desktops: 1GB of RAM or more and a dual CPU is recommended for playing in high-definition, full screen mode, or 720p or higher formatted video.

Video Quality Requirements

480p-formatted video — You can play video at 480p or lower at native resolutions when the View desktop has a single virtual CPU. If the operating system is Windows 7 or later and you want to play the video in high-definition Flash or in full screen mode, the desktop requires a dual virtual CPU. Even with a dual virtual CPU desktop, as low as 360p-formatted video played in full screen mode can lag behind audio, particularly on Windows clients.

720p-formatted video — You can play video at 720p at native resolutions if the View desktop has a dual virtual CPU. Performance might be affected if you play videos at 720p in high definition or in full screen mode.

1080p-formatted video If the View desktop has a dual virtual CPU, you can play 1080p formatted video, although the media player might need to be adjusted to a smaller window size.

3D If you use VMware vSphere 5.1 or later, you can configure View desktops to use software or hardware accelerated graphics.

- With Virtual Shared Graphics Acceleration (vSGA), a vSphere 5.1 feature that uses physical graphics cards installed on the ESXi hosts, you can use 3D applications for design, modeling, and multimedia.
- With the software accelerated graphics feature, available with vSphere 5.0 and later, you can use less demanding 3D applications such as Windows Aero themes, Microsoft Office 2010, and Google Earth.

  This non-hardware accelerated graphics feature enables you to run DirectX 9 and OpenGL 2.1 applications without requiring a physical graphics processing unit (GPU).

For 3D applications, up to 2 monitors are supported, and the maximum screen resolution is 1920 x 1200. The guest operating system on the View desktops must be Windows 7 or later.

Hardware Requirements for Client Systems

For information about processor and memory requirements, see the "Using VMware View Client" document for the specific type of desktop or mobile client device. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Microsoft RDP

Remote Desktop Protocol is the same multichannel protocol many people already use to access their work computer from their home computer. Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data.

Microsoft RDP provides the following features:

- With RDP 6, you can use multiple monitors in span mode. RDP 7 has true multiple monitor support, for up to 16 monitors.
- You can copy and paste text and system objects such as folders and files between the local system and the View desktop.
- 32-bit color is supported for virtual displays.
- RDP supports 128-bit encryption.
- Users outside the corporate firewall can use this protocol with your company's virtual private network (VPN), or users can make secure, encrypted connections to a View security server in the corporate DMZ.

NOTE For Windows XP desktop virtual machines, you must install the RDP patches listed in Microsoft Knowledge Base (KB) articles 323497 and 884020. If you do not install the RDP patches, a `Windows Sockets failed error` message might appear on the client.

Hardware Requirements for Client Systems

For information about processor and memory requirements, see the "Using VMware View Client" document for the specific type of client system. Go to https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

NOTE iOS and Android client devices use only the PCoIP display protocol.

Preparing Active Directory 3

View uses your existing Microsoft Active Directory infrastructure for user authentication and management. You must perform certain tasks to prepare Active Directory for use with View.

View supports the following versions of Active Directory:

- Windows 2003 Active Directory
- Windows 2008 Active Directory

This chapter includes the following topics:

Configuring Domains and Trust Relationships

You must join each View Connection Server host to an Active Directory domain. The host must not be a domain controller. You place View desktops in the same domain as the View Connection Server host or in a domain that has a two-way trust relationship with the View Connection Server host's domain.

You can entitle users and groups in the View Connection host's domain to View desktops and pools. You can also select users and groups from the View Connection Server host's domain to be administrators in View Administrator. To entitle or select users and groups from a different domain, you must establish a two-way trust relationship between that domain and the View Connection Server host's domain.

Users are authenticated against Active Directory for the View Connection Server host's domain and against any additional user domains with which a trust agreement exists.

NOTE Because security servers do not access any authentication repositories, including Active Directory, they do not need to reside in an Active Directory domain.

Trust Relationships and Domain Filtering

To determine which domains it can access, a View Connection Server instance traverses trust relationships beginning with its own domain.

For a small, well-connected set of domains, View Connection Server can quickly determine the full list of domains, but the time that it takes increases as the number of domains increases or as the connectivity between the domains decreases. The list might also include domains that you would prefer not to offer to users when they log in to their View desktops.

You can use the `vdmadmin` command to configure domain filtering to limit the domains that a View Connection Server instance searches and that it displays to users. See the *VMware Horizon View Administration* document for more information.

Creating an OU for View Desktops

You should create an organizational unit (OU) specifically for your View desktops. An OU is a subdivision in Active Directory that contains users, groups, computers, or other OUs.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your desktops, you can create a GPO for your View group policies and link it to the OU that contains your View desktops. You can also delegate control of the OU to subordinate groups, such as server operators or individual users.

If you use View Composer, you should create a separate Active Directory container for linked-clone desktops that is based on the OU for your View desktops. View administrators that have OU administrator privileges in Active Directory can provision linked-clone desktops without domain administrator privileges. If you change administrator credentials in Active Directory, you must also update the credential information in View Composer.

Creating OUs and Groups for Kiosk Mode Client Accounts

A client in kiosk mode is a thin client or a locked-down PC that runs View Client to connect to a View Connection Server instance and launch a remote desktop session. If you configure clients in kiosk mode, you should create dedicated OUs and groups in Active Directory for kiosk mode client accounts.

Creating dedicated OUs and groups for kiosk mode client accounts partitions client systems against unwarranted intrusion and simplifies client configuration and administration.

See the *VMware Horizon View Administration* document for more information.

Creating Groups for View Users

You should create groups for different types of View users in Active Directory. For example, you can create a group called VMware Horizon View Users for your View desktop users and another group called VMware Horizon View Administrators for users that will administer View desktops.

Creating a User Account for vCenter Server

You must create a user account in Active Directory to use with vCenter Server. You specify this user account when you add a vCenter Server instance in View Administrator.

The user account must be in the same domain as your View Connection Server host or in a trusted domain. If you use View Composer, you must add the user account to the local Administrators group on the vCenter Server computer.

You must give the user account privileges to perform certain operations in vCenter Server. If you use View Composer, you must give the user account additional privileges. See "Configuring User Accounts for vCenter Server and View Composer," on page 87 for information on configuring these privileges.

Create a User Account for View Composer

If you use View Composer, you must create a user account in Active Directory to use with View Composer. View Composer requires this account to join linked-clone desktops to your Active Directory domain.

To ensure security, you should create a separate user account to use with View Composer. By creating a separate account, you can guarantee that it does not have additional privileges that are defined for another purpose. You can give the account the minimum privileges that it needs to create and remove computer objects in a specified Active Directory container. For example, the View Composer account does not require domain administrator privileges.

Procedure

1 In Active Directory, create a user account in the same domain as your View Connection Server host or in a trusted domain.

2 Add the **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions to the account in the Active Directory container in which the linked-clone computer accounts are created or to which the linked-clone computer accounts are moved.

The following list shows all the required permissions for the user account, including permissions that are assigned by default:

- List Contents
- Read All Properties
- Write All Properties
- Read Permissions
- Reset Password
- Create Computer Objects
- Delete Computer Objects

NOTE If you select the **Allow reuse of pre-existing computer accounts** setting for a desktop pool, you only need to add the following permissions:

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

3 Make sure that the user account's permissions apply to the Active Directory container and to all child objects of the container.

What to do next

Specify the account in View Administrator when you configure View Composer for vCenter Server and when you configure and deploy linked-clone desktop pools.

Configure the Restricted Groups Policy

To be able to log in to a View desktop, users must belong to the local Remote Desktop Users group of the View desktop. You can use the Restricted Groups policy in Active Directory to add users or groups to the local Remote Desktop Users group of every View desktop that is joined to your domain.

The Restricted Groups policy sets the local group membership of computers in the domain to match the membership list settings defined in the Restricted Groups policy. The members of your View desktop users group are always added to the local Remote Desktop Users group of every View desktop that is joined to your domain. When adding new users, you need only add them to your View desktop users group.

Prerequisites

Create a group for View desktop users in your domain in Active Directory.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings**.

3 Right-click **Restricted Groups**, select **Add Group**, and add the Remote Desktop Users group.

4 Right-click the new restricted Remote Desktop Users group and add your View desktop users group to the group membership list.

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

Using View Group Policy Administrative Template Files

View includes several component-specific group policy administrative (ADM) template files.

During View Connection Server installation, the View ADM template files are installed in the *install_directory*\VMware\VMware View\Server\Extras\GroupPolicyFiles directory on your View Connection Server host. You must copy these files to a directory on your Active Directory server.

You can optimize and secure View desktops by adding the policy settings in these files to a new or existing GPO in Active Directory and then linking that GPO to the OU that contains your View desktops.

See the *VMware Horizon View Administration* document for information on using View group policy settings.

Prepare Active Directory for Smart Card Authentication

You might need to perform certain tasks in Active Directory when you implement smart card authentication.

- Add UPNs for Smart Card Users on page 23

  Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users that use smart cards to authenticate in View must have a valid UPN.

- Add the Root Certificate to Trusted Root Certification Authorities on page 24

  If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

- Add an Intermediate Certificate to Intermediate Certification Authorities on page 24

  If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

- Add the Root Certificate to the Enterprise NTAuth Store on page 25

  If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Add UPNs for Smart Card Users

Because smart card logins rely on user principal names (UPNs), the Active Directory accounts of users that use smart cards to authenticate in View must have a valid UPN.

If the domain a smart card user resides in is different from the domain that your root certificate was issued from, you must set the user's UPN to the Subject Alternative Name (SAN) contained in the root certificate of the trusted CA. If your root certificate was issued from a server in the smart card user's current domain, you do not need to modify the user's UPN.

NOTE You might need to set the UPN for built-in Active Directory accounts, even if the certificate is issued from the same domain. Built-in accounts, including Administrator, do not have a UPN set by default.

Prerequisites

- Obtain the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.
- If the ADSI Edit utility is not present on your Active Directory server, download and install the appropriate Windows Support Tools from the Microsoft Web site.

Procedure

1 On your Active Directory server, start the ADSI Edit utility.

2 In the left pane, expand the domain the user is located in and double-click `CN=Users`.

3 In the right pane, right-click the user and then click **Properties**.

4 Double-click the `userPrincipalName` attribute and type the SAN value of the trusted CA certificate.

5 Click **OK** to save the attribute setting.

Add the Root Certificate to Trusted Root Certification Authorities

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.

3 Right-click **Trusted Root Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the root certificate in their trusted root store.

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See "Add an Intermediate Certificate to Intermediate Certification Authorities," on page 24.

Add an Intermediate Certificate to Intermediate Certification Authorities

If you use an intermediate certification authority (CA) to issue smart card login or domain controller certificates, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

Procedure

1 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

2 Expand the **Computer Configuration** section and open the policy for **Windows Settings\Security Settings\Public Key**.

3 Right-click **Intermediate Certification Authorities** and select **Import**.

4 Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the Group Policy window.

All of the systems in the domain now have a copy of the intermediate certificate in their intermediate certification authority store.

Add the Root Certificate to the Enterprise NTAuth Store

If you use a CA to issue smart card login or domain controller certificates, you must add the root certificate to the Enterprise NTAuth store in Active Directory. You do not need to perform this procedure if the Windows domain controller acts as the root CA.

Procedure

- On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

  For example: **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

The CA is now trusted to issue certificates of this type.

Installing View Composer 4

To use View Composer, you create a View Composer database, install the View Composer service, and optimize your View infrastructure to support View Composer. You can install the View Composer service on the same host as vCenter Server or on a separate host.

View Composer is an optional feature. Install View Composer if you intend to deploy linked-clone desktop pools.

You must have a license to install and use the View Composer feature.

This chapter includes the following topics:

Prepare a View Composer Database

You must create a database and data source name (DSN) to store View Composer data.

The View Composer service does not include a database. If a database instance does not exist in your network environment, you must install one. After you install a database instance, you add the View Composer database to the instance.

You can add the View Composer database to the instance on which the vCenter Server database is located. You can configure the database locally, or remotely, on a network-connected Linux, UNIX, or Windows Server computer.

The View Composer database stores information about connections and components that are used by View Composer:

- vCenter Server connections
- Active Directory connections
- Linked-clone desktops that are deployed by View Composer
- Replicas that are created by View Composer

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

For a list of supported database versions, see "Database Requirements for View Composer," on page 10.

To add a View Composer database to an installed database instance, choose one of these procedures.

- Create a SQL Server Database for View Composer on page 28

  View Composer can store linked-clone desktop information in a SQL Server database. You create a View Composer database by adding it to SQL Server and configuring an ODBC data source for it.

- Create an Oracle Database for View Composer on page 30

  View Composer can store linked-clone desktop information in an Oracle 11g or 10g database. You create a View Composer database by adding it to an existing Oracle instance and configuring an ODBC data source for it. You can add a new View Composer database by using the Oracle Database Configuration Assistant or by running a SQL statement.

Create a SQL Server Database for View Composer

View Composer can store linked-clone desktop information in a SQL Server database. You create a View Composer database by adding it to SQL Server and configuring an ODBC data source for it.

Add a View Composer Database to SQL Server

You can add a new View Composer database to an existing Microsoft SQL Server instance to store linked-clone data for View Composer.

If the database resides locally, on the system on which View Composer will be installed, you can use the Integrated Windows Authentication security model. If the database resides on a remote system, you cannot use this method of authentication.

Prerequisites

- Verify that a supported version of SQL Server is installed on the computer on which you will install View Composer or in your network environment. For details, see "Database Requirements for View Composer," on page 10.
- Verify that you use SQL Server Management Studio or SQL Server Management Studio Express to create and administer the data source. You can download and install SQL Server Management Studio Express from the following Web site.

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

Procedure

1. On the View Composer computer, select **Start > All Programs > Microsoft SQL Server 2008** or **Microsoft SQL Server 2005**.
2. Select **SQL Server Management Studio Express** and connect to the existing SQL Server instance for vSphere Management.
3. In the Object Explorer panel, right-click the Databases entry and select **New Database**.
4. In the New Database dialog box, type a name in the Database name text box.

   For example: **`viewComposer`**
5. Click **OK**.

   SQL Server Management Studio Express adds your database to the Databases entry in the Object Explorer panel.
6. Exit Microsoft SQL Server Management Studio Express.

What to do next

Follow the instructions in "Add an ODBC Data Source to SQL Server," on page 29.

Add an ODBC Data Source to SQL Server

After you add a View Composer database to SQL Server, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

When you configure an ODBC DSN for View Composer, secure the underlying database connection to an appropriate level for your environment. For information about securing database connections, see the SQL Server documentation.

If the underlying database connection uses SSL encryption, we recommend that you configure your database servers with SSL certificates signed by a trusted CA. If you use self-signed certificates, your database connections might be susceptible to man-in-the-middle attacks.

Prerequisites

Complete the steps described in "Add a View Composer Database to SQL Server," on page 28.

Procedure

1 On the computer on which View Composer will be installed, select **Start > Administrative Tools > Data Source (ODBC)**.

2 Select the **System DSN** tab.

3 Click **Add** and select **SQL Native Client** from the list.

4 Click **Finish**.

5 In the Create a New Data Source to SQL Server setup wizard, type a name and description of the View Composer database.

For example: **`ViewComposer`**

6 In the Server text box, type the SQL Server database name.

Use the form *host_name**server_name*, where *host_name* is the name of the computer and *server_name* is the SQL Server instance.

For example: **`VCHOST1\VIM_SQLEXP`**

7 Click **Next**.

8 Make sure that the **Connect to SQL Server to obtain default settings for the additional configuration options** check box is selected and select an authentication option.

Option	Description
Windows NT authentication	Select this option if you are using a local instance of SQL Server. This option is also known as trusted authentication. Windows NT authentication is supported only if SQL Server is running on the local computer.
SQL Server authentication	Select this option if you are using a remote instance of SQL Server. Windows NT authentication is not supported on remote SQL Server.

9 Click **Next**.

10 Select the **Change the default database to** check box and select the name of the View Composer database from the list.

For example: **`ViewComposer`**

11 If the SQL Server connection is configured with SSL enabled, navigate to the Microsoft SQL Server DSN Configuration page and select **Use strong encryption for data**.

12 Finish and close the Microsoft ODBC Data Source Administrator wizard.

What to do next

Install the new View Composer service. See "Install the View Composer Service," on page 33.

Create an Oracle Database for View Composer

View Composer can store linked-clone desktop information in an Oracle 11g or 10g database. You create a View Composer database by adding it to an existing Oracle instance and configuring an ODBC data source for it. You can add a new View Composer database by using the Oracle Database Configuration Assistant or by running a SQL statement.

- Add a View Composer Database to Oracle 11g or 10g on page 30

  You can use the Oracle Database Configuration Assistant to add a new View Composer database to an existing Oracle 11g or 10g instance.

- Use a SQL Statement to Add a View Composer Database to an Oracle Instance on page 31

  The View Composer database must have certain table spaces and privileges. You can use a SQL statement to create the View Composer database in an Oracle 11g or 10g database instance.

- Configure an Oracle Database User for View Composer on page 31

  By default, the database user that runs the View Composer database has Oracle system administrator permissions. To restrict the security permissions for the user that runs the View Composer database, you must configure an Oracle database user with specific permissions.

- Add an ODBC Data Source to Oracle 11g or 10g on page 32

  After you add a View Composer database to an Oracle 11g or 10g instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

Add a View Composer Database to Oracle 11g or 10g

You can use the Oracle Database Configuration Assistant to add a new View Composer database to an existing Oracle 11g or 10g instance.

Prerequisites

Verify that a supported version of Oracle 11g or 10g is installed on the local or remote computer. See "Database Requirements for View Composer," on page 10.

Procedure

1 Start the **Database Configuration Assistant** on the computer on which you are adding the View Composer database.

Database Version	Action
Oracle 11g	Select **Start > All Programs > Oracle-OraDb11g_home > Configuration and Migration Tools > Database Configuration Assistant**.
Oracle 10g	Select **Start > All Programs > Oracle-OraDb10g_home > Configuration and Migration Tools > Database Configuration Assistant**.

2 On the Operations page, select **Create a database**.

3 On the Database Templates page, select the **General Purpose or Transaction Processing** template.

4 On the Database Identification page, type a Global Database Name and an Oracle System Identifier (SID) prefix.

  For simplicity, use the same value for both items.

5 On the Management Options page, click **Next** to accept the default settings.

6 On the Database Credentials page, select **Use the Same Administrative Passwords for All Accounts** and type a password.

7 On the remaining configuration pages, click **Next** to accept the default settings.

8 On the Creation Options page, verify that **Create Database** is selected and click **Finish**.

9 On the Confirmation page, review the options and click **OK**.

The configuration tool creates the database.

10 On the Database Creation Complete page, click **OK**.

What to do next

Follow the instructions in "Add an ODBC Data Source to Oracle 11g or 10g," on page 32.

Use a SQL Statement to Add a View Composer Database to an Oracle Instance

The View Composer database must have certain table spaces and privileges. You can use a SQL statement to create the View Composer database in an Oracle 11g or 10g database instance.

When you create the database, you can customize the location of the data and log files.

Prerequisites

Verify that a supported version of Oracle 11g or 10g is installed on the local or remote computer. For details, see "Database Requirements for View Composer," on page 10.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL statement to create the database.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

In this example, `VCMP` is the sample name of the View Composer database and `vcmp01.dbf` is the name of the database file.

For a Windows installation, use Windows conventions in the directory path to the `vcmp01.dbf` file.

What to do next

If you want to run the View Composer database with specific security permissions, follow the instructions in "Configure an Oracle Database User for View Composer," on page 31.

Follow the instructions in "Add an ODBC Data Source to Oracle 11g or 10g," on page 32

Configure an Oracle Database User for View Composer

By default, the database user that runs the View Composer database has Oracle system administrator permissions. To restrict the security permissions for the user that runs the View Composer database, you must configure an Oracle database user with specific permissions.

Prerequisites

Verify that a View Composer database was created in an Oracle 11g or 10g instance.

Procedure

1 Log in to a SQL*Plus session with the system account.

2 Run the following SQL command to create a View Composer database user with the correct permissions.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
   grant resource to VCMPADMIN;
   grant create view to VCMPADMIN;
   grant create sequence to VCMPADMIN;
   grant create table to VCMPADMIN;
   grant create materialized view to VCMPADMIN;
   grant execute on dbms_lock to VCMPADMIN;
   grant execute on dbms_job to VCMPADMIN;
   grant unlimited tablespace to VCMPADMIN;
```

In this example, the user name is `VCMPADMIN` and the View Composer database name is `VCMP`.

By default the `resource` role has the `create procedure`, `create table`, and `create sequence` privileges assigned. If the `resource` role does not have these privileges, explicitly grant them to the View Composer database user.

Add an ODBC Data Source to Oracle 11g or 10g

After you add a View Composer database to an Oracle 11g or 10g instance, you must configure an ODBC connection to the new database to make this data source visible to the View Composer service.

When you configure an ODBC DSN for View Composer, secure the underlying database connection to an appropriate level for your environment. For information about securing database connections, see the Oracle database documentation.

If the underlying database connection uses SSL encryption, we recommend that you configure your database servers with SSL certificates signed by a trusted CA. If you use self-signed certificates, your database connections might be susceptible to man-in-the-middle attacks.

Prerequisites

Verify that you completed the steps described in "Add a View Composer Database to Oracle 11g or 10g," on page 30 or "Use a SQL Statement to Add a View Composer Database to an Oracle Instance," on page 31.

Procedure

1 On the View Composer database computer, select **Start > Administrative Tools > Data Source (ODBC)**.

2 From the Microsoft ODBC Data Source Administrator wizard, select the **System DSN** tab.

3 Click **Add** and select the appropriate Oracle driver from the list.

For example: **`OraDb11g_home`**

4 Click **Finish**.

5 In the Oracle ODBC Driver Configuration dialog box, type a DSN to use with View Composer, a description of the data source, and a user ID to connect to the database.

If you configured an Oracle database user ID with specific security permissions, specify this user ID.

NOTE You use the DSN when you install the View Composer service.

6 Specify a **TNS Service Name** by selecting the Global Database Name from the drop-down menu.

The Oracle Database Configuration Assistant specifies the Global Database Name.

7 To verify the data source, click **Test Connection** and click **OK**.

What to do next

Install the new View Composer service. See "Install the View Composer Service," on page 33.

Configuring an SSL Certificate for View Composer

By default, a self-signed certificate is installed with View Composer. You can use the default certificate for testing purposes, but for production use you should replace it with a certificate that is signed by a Certificate Authority (CA).

You can configure a certificate before or after you install View Composer. In View 5.1 and later releases, you configure a certificate by importing it into the Windows local computer certificate store on the Windows Server computer where View Composer is, or will be, installed.

- If you import a CA-signed certificate before you install View Composer, you can select the signed certificate during the View Composer installation. This approach eliminates the manual task of replacing the default certificate after the installation.
- 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.

For details about configuring SSL certificates and using the `SviConfig ReplaceCertificate` utility, see Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

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.

Install the View Composer Service

To use View Composer, you must install the View Composer service. View Manager uses View Composer to create and deploy linked-clone desktops in vCenter Server.

You can install the View Composer service on the Windows Server computer on which vCenter Server is installed or on a separate Windows Server computer. A standalone View Composer installation works with vCenter Server installed on a Windows Server computer and with the Linux-based vCenter Server Appliance.

The View Composer software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, security server, View Connection Server, View Agent, View Client, or View Transfer Server.

Prerequisites

- Verify that your installation satisfies the View Composer requirements described in "View Composer Requirements," on page 9.
- Verify that you have a license to install and use View Composer.
- Verify that you have the DSN, domain administrator user name, and password that you provided in the ODBC Data Source Administrator wizard. You enter this information when you install the View Composer service.
- If you plan to configure an SSL certificate signed by a CA for View Composer during the installation, verify that your certificate is imported in the Windows local computer certificate store. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.
- 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 run the View Composer installer, you must be a domain user with Administrator privileges on the system.

Procedure

1 Download the View Composer installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

The installer filename is `VMware-viewcomposer-y.y.y-xxxxxx.exe`, where *xxxxxx* is the build number and *y.y.y* is the version number. This installer file installs the View Composer service on 64-bit Windows Server operating systems.

2 To start the View Composer installation program, right-click the installer file and select **Run as administrator**.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Type the DSN for the View Composer database that you provided in the Microsoft or Oracle ODBC Data Source Administrator wizard.

For example: **`VMware View Composer`**

NOTE If you did not configure a DSN for the View Composer database, click **ODBC DSN Setup** to configure a name now.

6 Type the domain administrator user name and password that you provided in the ODBC Data Source Administrator wizard.

If you configured an Oracle database user with specific security permissions, specify this user name.

7 Type a port number or accept the default value.

View Connection Server uses this port to communicate with the View Composer service.

8 Provide an SSL certificate.

Option	Action
Create default SSL certificate	Select this radio button to create a default SSL certificate for the View Composer service. After the installation, you can replace the default certificate with an SSL certificate signed by a CA.
Use an existing SSL certificate	Select this radio button if you installed a signed SSL certificate that you want to use for the View Composer service. Select an SSL certificate from the list.

9 Click **Install** and **Finish** to complete the View Composer service installation.

The VMware View Composer service starts.

View Composer uses the cryptographic cipher suites that are provided by the Windows Server operating system. You should follow your organization's guidelines for managing cipher suites on Windows Server systems. If your organization does not provide guidelines, VMware recommends that you disable weak cryptographic cipher suites on the View Composer server to enhance the security of your View environment. For information about managing cryptographic cipher suites, see your Microsoft documentation.

Configuring Your Infrastructure for View Composer

You can take advantage of features in vSphere, vCenter Server, Active Directory, and other components of your infrastructure to optimize the performance, availability, and reliability of View Composer.

Configuring the vSphere Environment for View Composer

To support View Composer, you should follow certain best practices when you install and configure vCenter Server, ESX/ESXi, and other vSphere components.

These best practices let View Composer work efficiently in the vSphere environment.

- After you create the path and folder information for linked-clone virtual machines, do not change the information in vCenter Server. Instead, use View Administrator to change the folder information.

  If you change this information in vCenter Server, View Manager cannot successfully look up the virtual machines in vCenter Server.
- Make sure that the vSwitch settings on the ESX/ESXi host are configured with enough ports to support the total number of virtual NICs that are configured on the linked-clone virtual machines that run on the ESX/ESXi host.
- When you deploy linked-clone desktops in a resource pool, make sure that your vSphere environment has enough CPU and memory to host the number of desktops that you require. Use vSphere Client to monitor CPU and memory usage in resource pools.
- In vSphere 5.1 and later, a cluster that is used for View Composer linked clones can contain more than eight ESX/ESXi hosts if the replica disks are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts.

  In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts.
- Use vSphere DRS. DRS efficiently distributes linked-clone virtual machines among your hosts.

NOTE Storage vMotion is not supported for linked-clone desktops.

Additional Best Practices for View Composer

To make sure that View Composer works efficiently, check that your dynamic name service (DNS) operates correctly, and run antivirus software scans at staggered times.

By making sure that DNS resolution operates correctly, you can overcome intermittent issues caused by DNS errors. The View Composer service relies on dynamic name resolution to communicate with other computers. To test DNS operation, ping the Active Directory and View Connection Server computers by name.

If you stagger the run times for your antivirus software, performance of the linked-clone desktops is not affected. If the antivirus software runs in all linked clones at the same time, excessive I/O operations per second (IOPS) occur in your storage subsystem. This excessive activity can affect performance of the linked-clone desktops.

Installing View Connection Server 5

To use View Connection Server, you install the software on supported computers, configure the required components, and, optionally, optimize the components.

This chapter includes the following topics:

Installing the View Connection Server Software

Depending on the performance, availability, and security needs of your View deployment, you can install a single instance of View Connection Server, replicated instances of View Connection Server, and security servers. You must install at least one instance of View Connection Server.

When you install View Connection Server, you select a type of installation.

Standard installation	Generates a View Connection Server instance with a new View LDAP configuration.
Replica installation	Generates a View Connection Server instance with a View LDAP configuration that is copied from an existing instance.
Security server installation	Generates a View Connection Server instance that adds an additional layer of security between the Internet and your internal network.

Installation Prerequisites for View Connection Server

Before you install View Connection Server, you must verify that your installation environment satisfies specific prerequisites.

- View Connection Server requires a valid license key for View Manager. The following license keys are available:
  - View Manager
  - View Manager with View Composer and Local Mode
- You must join the View Connection Server host to an Active Directory domain. View Connection Server supports the following versions of Active Directory:
  - Windows 2003 Active Directory
  - Windows 2008 Active Directory

  The View Connection Server host must not be a domain controller.

  NOTE View Connection Server does not make, nor does it require, any schema or configuration updates to Active Directory.
- Do not install View Connection Server on systems that have the Windows Terminal Server role installed. You must remove the Windows Terminal Server role from any system on which you install View Connection Server.
- Do not install View Connection Server on a system that performs any other functions or roles. For example, do not use the same system to host vCenter Server.
- The system on which you install View Connection Server must have a static IP address.
- To run the View Connection Server installer, you must use a domain user account with Administrator privileges on the system.
- When you install View Connection Server, 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.

Install View Connection Server with a New Configuration

To install View Connection Server as a single server or as the first instance in a group of replicated View Connection Server instances, you use the standard installation option.

When you select the standard installation option, the installation creates a new, local View LDAP configuration. The installation loads the schema definitions, Directory Information Tree (DIT) definition, and ACLs and initializes the data.

After installation, you manage most View LDAP configuration data by using View Administrator. View Connection Server automatically maintains some View LDAP entries.

The View Connection Server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, security server, View Composer, View Agent, View Client, or View Transfer Server.

When you install View Connection Server with a new configuration, you can participate in a customer experience improvement program. VMware collects anonymous data about your deployment in order to improve VMware's response to user requirements. No data that identifies your organization is collected. You can choose not to participate by deselecting this option during the installation. If you change your mind about

participating after the installation, you can either join or withdraw from the program by editing the Product Licensing and Usage page in View Administrator. To review the list of fields from which data is collected, including the fields that are made anonymous, see "Information Collected by the Customer Experience Improvement Program" in the *VMware Horizon View Administration* document.

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- If you intend to authorize a domain user or group as the View Administrators account, verify that you created the domain account in Active Directory.
- If you use MIT Kerberos authentication to log in to a Windows Server 2008 R2 computer on which you are installing View Connection Server, install the Microsoft hotfix that is described in KB 978116 at http://support.microsoft.com/kb/978116.
- Prepare a data recovery password. 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. Follow your organization's best practices for generating secure passwords.

  IMPORTANT You will need the data recovery password to keep View operating and avoid downtime in a Business Continuity and Disaster Recovery (BCDR) scenario. You can provide a password reminder with the password when you install View Connection Server.

- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 55.
- 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 back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.

Procedure

1. Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2. To start the View Connection Server installation program, double-click the installer file.
3. Accept the VMware license terms.
4. Accept or change the destination folder.
5. Select the **View Standard Server** installation option.
6. Type a data recovery password and, optionally, a password reminder.

7 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

8 Authorize a View Administrators account.

Only members of this account can log in to View Administrator, exercise full View administration rights, and install replicated View Connection Server instances and other View servers.

Option	Description
Authorize the local Administrators group	Allows users in the local Administrators group to administer View.
Authorize a specific domain user or domain group	Allows the specified domain user or group to administer View.

9 If you specified a domain View Administrators account, and you are running the installer as a local administrator or another user without access to the domain account, provide credentials to log in to the domain with an authorized user name and password.

Use *domain name**user name* or user principal name (UPN) format. UPN format can be *user@domain.com*.

10 Choose whether to participate in the customer experience improvement program.

If you participate, you can optionally select the type, size, and location of your organization.

11 Complete the installation wizard to finish installing View Connection Server.

12 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The View services are installed on the Windows Server computer:

- VMware View Connection Server
- VMware View Framework Component
- VMware View Message Bus Component
- VMware View Script Host
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway
- VMware View Blast Secure Gateway
- VMware View Web Component
- VMware VDMDS, which provides View LDAP directory services

For information about these services, see the *VMware Horizon View Administration* document.

What to do next

Configure SSL server certificates for View Connection Server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

Perform initial configuration on View Connection Server. See Chapter 8, "Configuring View for the First Time," on page 87.

If you plan to include replicated View Connection Server instances and security servers in your deployment, you must install each server instance by running the View Connection Server installer file.

If you are reinstalling View Connection Server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install View Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to perform a standard installation of View Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

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

Prerequisites

- Verify that you can log in as a domain user with administrator privileges on the Windows Server computer on which you install View Connection Server.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- If you intend to authorize a domain user or group as the View Administrators account, verify that you created the domain account in Active Directory.
- If you use MIT Kerberos authentication to log in to a Windows Server 2008 R2 computer on which you are installing View Connection Server, install the Microsoft hotfix that is described in KB 978116 at http://support.microsoft.com/kb/978116.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 55.
- 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 back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.
- Verify that the Windows computer on which you install View Connection Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 57.
- Familiarize yourself with the silent installation properties available with a standard installation of View Connection Server. See "Silent Installation Properties for a View Connection Server Standard Installation," on page 42.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

IMPORTANT When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using View Administrator.

4 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The View services are installed on the Windows Server computer. For details, see "Install View Connection Server with a New Configuration," on page 38.

What to do next

Configure SSL server certificates for View Connection Server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

If you are configuring View for the first time, perform initial configuration on View Connection Server. See Chapter 8, "Configuring View for the First Time," on page 87.

Silent Installation Properties for a View Connection Server Standard Installation

You can include specific View Connection Server properties when you perform a silent installation from the command line. You must use a *PROPERTY=value* format so that Microsoft Windows Installer (MSI) can interpret the properties and values.

Table 5-1. MSI Properties for Silently Installing View Connection Server in a Standard Installation

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path.	`%ProgramFiles%\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation For example, to perform a standard installation, define `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1`	1

Table 5-1. MSI Properties for Silently Installing View Connection Server in a Standard Installation (Continued)

MSI Property	Description	Default Value
VDM_INITIAL_ADMIN_SID	The SID of the initial View Administrators user or group that is authorized with full administration rights in View. The default value is the SID of the local Administrators group on the View Connection Server computer. You can specify a SID of a domain user or group account.	S-1-5-32-544
VDM_SERVER_RECOVERY_PWD	The data recovery password. If a data recovery password is not set in View LDAP, this property is mandatory. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_PWD_REMINDER	The data recovery password reminder. This property is optional.	None

Install a Replicated Instance of View Connection Server

To provide high availability and load balancing, you can install one or more additional instances of View Connection Server that replicate an existing View Connection Server instance. After a replica installation, the existing and newly installed instances of View Connection Server are identical.

When you install a replicated instance, View Manager copies the View LDAP configuration data from the existing View Connection Server instance.

After the installation, the View Manager software maintains identical View LDAP configuration data on all View Connection Server instances in the replicated group. When a change is made on one instance, the updated information is copied to the other instances.

If a replicated instance fails, the other instances in the group continue to operate. When the failed instance resumes activity, its configuration is updated with the changes that took place during the outage.

NOTE Replication functionality is provided by View LDAP, which uses the same replication technology as Active Directory.

The replica server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a security server, View Connection Server, View Composer, View Agent, View Client, or View Transfer Server.

Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with the View Administrators role. You specify the account or group with the View Administrators role when you install the first instance of View Connection Server. The role can be assigned to the local Administrators group or a domain user or group. See "Install View Connection Server with a New Configuration," on page 38.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- If you use MIT Kerberos authentication to log in to a Windows Server 2008 R2 computer on which you are installing View Connection Server, install the Microsoft hotfix that is described in KB 978116 at http://support.microsoft.com/kb/978116.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.

- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See "Network Requirements for Replicated View Connection Server Instances," on page 8.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- If you install a replicated View Connection Server instance that is View 5.1 or later, and the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier, prepare a data recovery password. See "Install View Connection Server with a New Configuration," on page 38.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 55.
- 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 back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 To start the View Connection Server installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select the **View Replica Server** installation option.

6 Enter the host name or IP address of the existing View Connection Server instance you are replicating.

7 Type a data recovery password and, optionally, a password reminder.

You are prompted for a data recovery password only if the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier.

8 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

9 Complete the installation wizard to finish installing the replicated instance.

10 Check for new patches on the Windows Server computer and run Windows Update as needed.

Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The View services are installed on the Windows Server computer:

- VMware View Connection Server
- VMware View Framework Component
- VMware View Message Bus Component
- VMware View Script Host
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway
- VMware View Blast Secure Gateway
- VMware View Web Component
- VMware VDMDS, which provides View LDAP directory services

For information about these services, see the *VMware Horizon View Administration* document.

What to do next

Configure an SSL server certificate for the View Connection Server instance. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

You do not have to perform an initial View configuration on a replicated instance of View Connection Server. The replicated instance inherits its configuration from the existing View Connection Server instance.

However, you might have to configure client connection settings for this View Connection Server instance, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 101 and "Sizing Windows Server Settings to Support Your Deployment," on page 110.

If you are reinstalling View Connection Server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install a Replicated Instance of View Connection Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install a replicated instance of View Connection Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

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

Prerequisites

- Verify that at least one View Connection Server instance is installed and configured on the network.
- To install the replicated instance, you must log in as a user with credentials to access the View Administrators account. You specify the View Administrators account when you install the first instance of View Connection Server. The account can be the local Administrators group or a domain user or group account. See "Install View Connection Server with a New Configuration," on page 38.
- If the existing View Connection Server instance is in a different domain than the replicated instance, the domain user must also have View Administrator privileges on the Windows Server computer where the existing instance is installed.
- If you use MIT Kerberos authentication to log in to a Windows Server 2008 R2 computer on which you are installing View Connection Server, install the Microsoft hotfix that is described in KB 978116 at http://support.microsoft.com/kb/978116.
- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.

- Verify that the computers on which you install replicated View Connection Server instances are connected over a high-performance LAN. See "Network Requirements for Replicated View Connection Server Instances," on page 8.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Connection Server," on page 55.
- 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 back-end firewall between a security server and the View Connection Server instance, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 57.
- Familiarize yourself with the silent installation properties available with a replica installation of View Connection Server. See "Silent Installation Properties for a Replicated Instance of View Connection Server," on page 47.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

   For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`

   If you install a replicated View Connection Server instance that is View 5.1 or later, and the existing View Connection Server instance you are replicating is View 5.0.*x* or earlier, you must specify a data recovery password, and you can add a password reminder. For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

   Important When you perform a silent installation, the full command line, including the data recovery password, is logged in the installer's `vminst.log` file. After the installation is complete, either delete this log file or change the data recovery password by using View Administrator.

4 Check for new patches on the Windows Server computer and run Windows Update as needed.

   Even if you fully patched the Windows Server computer before you installed View Connection Server, the installation might have enabled operating system features for the first time. Additional patches might now be required.

The View services are installed on the Windows Server computer. For details, see "Install a Replicated Instance of View Connection Server," on page 43.

What to do next

Configure an SSL server certificate for the View Connection Server instance. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

You do not have to perform an initial View configuration on a replicated instance of View Connection Server. The replicated instance inherits its configuration from the existing View Connection Server instance.

However, you might have to configure client connection settings for this View Connection Server instance, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 101 and "Sizing Windows Server Settings to Support Your Deployment," on page 110.

Silent Installation Properties for a Replicated Instance of View Connection Server

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

Table 5-2. MSI Properties for Silently installing a Replicated Instance of View Connection Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a replicated instance, define `VDM_SERVER_INSTANCE_TYPE=2` This MSI property is required when installing a replica.	1
ADAM_PRIMARY_NAME	The host name or IP address of the existing View Connection Server instance you are replicating. For example: `ADAM_PRIMARY_NAME=cs1.companydomain.com` This MSI property is required.	None
ADAM_PRIMARY_PORT	The View LDAP port of the existing View Connection Server instance you are replicating. For example: `ADAM_PRIMARY_PORT=cs1.companydomain.com` This MSI property is optional.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1

Table 5-2. MSI Properties for Silently installing a Replicated Instance of View Connection Server (Continued)

MSI Property	Description	Default Value
VDM_SERVER_RECOVERY_PWD	The data recovery password. If a data recovery password is not set in View LDAP, this property is mandatory. NOTE The data recover password is not set in View LDAP if the standard View Connection Server instance you are replicating is View 5.0 or earlier. If the View Connection Server instance you are replicating is View 5.1 or later, you do not have to provide this property. The password must contain between 1 and 128 characters. Follow your organization's best practices for generating secure passwords.	None
VDM_SERVER_RECOVERY_PWD_REMINDER	The data recovery password reminder. This property is optional.	None

Configure a Security Server Pairing Password

Before you can install a security server, you must configure a security server pairing password. When you install a security server with the View Connection Server installation program, the program prompts you for this password during the installation process.

The security server pairing password is a one-time password that permits a security server to be paired with a View Connection Server instance. The password becomes invalid after you provide it to the View Connection Server installation program.

NOTE You cannot pair an older version of security server with the current version of View Connection Server. If you configure a pairing password on the current version of View Connecton Server and try to install an older version of security server, the pairing password will be invalid.

Procedure

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

2 In the Connection Servers tab, select the View Connection Server instance to pair with the security server.

3 From the **More Commands** drop-down menu, select **Specify Security Server Pairing Password**.

4 Type the password in the Pairing password and Confirm password text boxes and specify a password timeout value.

You must use the password within the specified timeout period.

5 Click **OK** to configure the password.

What to do next

Install a security server. See "Install a Security Server," on page 48.

IMPORTANT If you do not provide the security server pairing password to the View Connection Server installation program within the password timeout period, the password becomes invalid and you must configure a new password.

Install a Security Server

A security server is an instance of View Connection Server that adds an additional layer of security between the Internet and your internal network. You can install one or more security servers to be connected to a View Connection Server instance.

The security server software cannot coexist on the same virtual or physical machine with any other View Manager software component, including a replica server, View Connection Server, View Composer, View Agent, View Client, or View Transfer Server.

Prerequisites

- Determine the type of topology to use. For example, determine which load balancing solution to use. Decide if the View Connection Server instances that are paired with security servers will be dedicated to users of the external network. For information, see the *VMware Horizon View Architecture Planning* document.

  IMPORTANT If you use a load balancer, you must have static IP addresses for the load balancer and each security server. For example, if you use a load balancer with two security servers, you need 3 static IP addresses.

- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running a View Connection Server version that is compatible with the security server version. See "Horizon View Component Compatibility Matrix" in the *VMware Horizon View Upgrades* document.
- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.
- Configure a security server pairing password. See "Configure a Security Server Pairing Password," on page 48.
- Familiarize yourself with the format of external URLs. See "Configuring External URLs for Secure Gateway and Tunnel Connections," on page 104.
- 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.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See "Firewall Rules for View Connection Server," on page 55.
- If your network topology includes a back-end firewall between the security server and View Connection Server, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.
- If you are upgrading or reinstalling the security server, verify that the existing IPsec rules for the security server were removed. See "Prepare to Upgrade or Reinstall a Security Server," on page 54.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 To start the View Connection Server installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select the **View Security Server** installation option.

6 Type the fully qualified domain name or IP address of the View Connection Server instance to pair with the security server in the **Server** text box.

  The security server forwards network traffic to this View Connection Server instance.

7 Type the security server pairing password in the Password text box.

If the password has expired, you can use View Administrator to configure a new password and type the new password in the installation program.

8 In the **External URL** text box, type the external URL of the security server for View Clients that use the RDP or PCoIP display protocols.

The URL must contain the protocol, client-resolvable security server name, and port number. Tunnel clients that run outside of your network use this URL to connect to the security server.

For example: `https://view.example.com:443`

9 In the **PCoIP External URL** text box, type the external URL of the security server for View Clients that use the PCoIP display protocol.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach the security server. You can type into the text box only if a PCoIP Secure Gateway is installed on the security server.

10 In the **Blast External URL** text box, type the external URL of the security server for users who use HTML access to connect to View desktops.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

For example: `https://myserver.example.com:8443`

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this security server.

11 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually. Select this option only if your organization uses its own predefined rules for configuring Windows Firewall.

12 Complete the installation wizard to finish installing the security server.

The security server services are installed on the Windows Server computer:

- VMware View Security Server
- VMware View Framework Component
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway
- VMware Blast Secure Gateway

For information about these services, see *VMware Horizon View Administration*.

The security server appears in the Security Servers pane in View Administrator.

NOTE If the installation is cancelled or aborted, you might have to remove IPsec rules for the security server before you can begin the installation again. Take this step even if you already removed IPsec rules prior to reinstalling or upgrading security server. For instructions on removing IPsec rules, see "Prepare to Upgrade or Reinstall a Security Server," on page 54.

What to do next

Configure an SSL server certificate for the security server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

You might have to configure client connection settings for the security server, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 101 and "Sizing Windows Server Settings to Support Your Deployment," on page 110.

If your users connect to the security server through HTML Access, you must enable a rule in the Windows Firewall to open the HTML Access port. See "Open the Port Used by HTML Access on Security Servers," on page 103.

If you are reinstalling the security server on a Windows Server 2008 operating system and you have a data collector set configured to monitor performance data, stop the data collector set and start it again.

Install a Security Server Silently

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

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

Prerequisites

- Determine the type of topology to use. For example, determine which load balancing solution to use. Decide if the View Connection Server instances that are paired with security servers will be dedicated to users of the external network. For information, see the *VMware Horizon View Architecture Planning* document.

  IMPORTANT If you use a load balancer, you must have static IP addresses for the load balancer and each security server. For example, if you use a load balancer with two security servers, you need 3 static IP addresses.

- Verify that your installation satisfies the requirements described in "View Connection Server Requirements," on page 7.
- Prepare your environment for the installation. See "Installation Prerequisites for View Connection Server," on page 38.
- Verify that the View Connection Server instance to be paired with the security server is installed and configured and is running a View Connection Server version that is compatible with the security server version. See "Horizon View Component Compatibility Matrix" in the *VMware Horizon View Upgrades* document.
- Verify that the View Connection Server instance to be paired with the security server is accessible to the computer on which you plan to install the security server.
- Configure a security server pairing password. See "Configure a Security Server Pairing Password," on page 48.
- Familiarize yourself with the format of external URLs. See "Configuring External URLs for Secure Gateway and Tunnel Connections," on page 104.

- 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.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for a security server. See "Firewall Rules for View Connection Server," on page 55.
- If your network topology includes a back-end firewall between the security server and View Connection Server, you must configure the firewall to support IPsec. See "Configuring a Back-End Firewall to Support IPsec," on page 56.
- If you are upgrading or reinstalling the security server, verify that the existing IPsec rules for the security server were removed. See "Prepare to Upgrade or Reinstall a Security Server," on page 54.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 57.
- Familiarize yourself with the silent installation properties available with a security server. See "Silent Installation Properties for a Security Server," on page 53.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

   For example:
```
VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:
443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172
VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443
VDM_SERVER_SS_PWD=secret"
```

The View services are installed on the Windows Server computer. For details, see "Install a Security Server," on page 48.

NOTE If the installation is cancelled or aborted, you might have to remove IPsec rules for the security server before you can begin the installation again. Take this step even if you already removed IPsec rules prior to reinstalling or upgrading security server. For instructions on removing IPsec rules, see "Prepare to Upgrade or Reinstall a Security Server," on page 54.

What to do next

Configure an SSL server certificate for the security server. See Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

You might have to configure client connection settings for the security server, and you can tune Windows Server settings to support a large deployment. See "Configuring View Client Connections," on page 101 and "Sizing Windows Server Settings to Support Your Deployment," on page 110.

If your users connect to the security server through HTML Access, you must enable a rule in the Windows Firewall to open the HTML Access port. See "Open the Port Used by HTML Access on Security Servers," on page 103.

Silent Installation Properties for a Security Server

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

Table 5-3. MSI Properties for Silently Installing a Security Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a security server, define `VDM_SERVER_INSTANCE_TYPE=3` This MSI property is required when installing a security server.	1
VDM_SERVER_NAME	The host name or IP address of the existing View Connection Server instance to pair with the security server. For example: `VDM_SERVER_NAME=cs1.internaldomain.com` This MSI property is required.	None
VDM_SERVER_SS_EXTURL	The external URL of the security server. The URL must contain the protocol, externally resolvable security server name, and port number For example: `VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` This MSI property is required.	None
VDM_SERVER_SS_PWD	The security server pairing password. For example: `VDM_SERVER_SS_PWD=secret` This MSI property is required.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1
VDM_SERVER_SS_PCOIP_IP ADDR	The PCoIP Secure Gateway external IP address. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` This property is required if you plan to use the PCoIP Secure Gateway component.	None
VDM_SERVER_SS_PCOIP_T CPPORT	The PCoIP Secure Gateway external TCP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_TCPPORT=4172` This property is required if you plan to use the PCoIP Secure Gateway component.	None

Table 5-3. MSI Properties for Silently Installing a Security Server (Continued)

MSI Property	Description	Default Value
VDM_SERVER_SS_PCOIP_UDPPORT	The PCoIP Secure Gateway external UDP port number. This property is supported only when the security server is installed on Windows Server 2008 R2 or later. For example: `VDM_SERVER_SS_PCOIP_UDPPORT=4172` This property is required if you plan to use the PCoIP Secure Gateway component.	None
VDM_SERVER_SS_BSG_EXTURL	The Blast Secure Gateway external URL. The URL must contain the HTTPS protocol, an externally resolvable security server name, and port number For example: `VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443` The default port number is 8443. A Blast Secure Gateway must be installed on the security server to allow users to make Web connections to View desktops.	None
VDM_SERVER_SS_FORCE_IPSEC	Forces IPsec to be used between the security server and its paired View Connection Server instance. By default, an unattended installation and pairing of security server to a View Connection Server instance with IPsec disabled causes the pairing to fail. The default value of 1 forces IPsec pairing. Set this value to 0 to allow pairing without IPsec.	1

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 Horizon 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 *VMware Horizon 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.

What to do next

Upgrade or reinstall security server.

Firewall Rules for View Connection Server

Certain ports must be opened on the firewall for View Connection Server instances and security servers.

When you install View Connection Server, the installation program can optionally configure the required Windows firewall rules for you. These rules open the ports that are used by default. If you change the default ports after installation, you must manually configure the Windows firewall to allow View Client devices to connect to View through the updated ports.

Table 5-4. Ports Opened During View Connection Server Installation

Protocol	Ports	View Connection Server Instance Type
JMS	TCP 4001 in	Standard and replica
JMSIR	TCP 4100 in	Standard and replica
AJP13	TCP 8009 in	Standard and replica
HTTP	TCP 80 in	Standard, replica, and security server
HTTPS	TCP 443 in	Standard, replica, and security server
PCoIP	TCP 4172 in; UDP 4172 both directions	Standard, replica, and security server

Configuring a Back-End Firewall to Support IPsec

If your network topology includes a back-end firewall between security servers and View Connection Server instances, you must configure certain protocols and ports on the firewall to support IPsec. Without proper configuration, data sent between a security server and View Connection Server instance will fail to pass through the firewall.

By default, IPsec rules govern the connections between security servers and View Connection Server instances. To support IPsec, the View Connection Server installer can configure Windows firewall rules on the Windows Server hosts where View servers are installed. For a back-end firewall, you must configure the rules yourself.

NOTE It is highly recommended that you use IPsec. As an alternative, you can disable the View Administrator global setting, **Use IPsec for Security Server Connections**.

The following rules must allow bidirectional traffic. You might have to specify separate rules for inbound and outbound traffic on your firewall.

Different rules apply to firewalls that use network address translation (NAT) and those that do not use NAT.

Table 5-5. Non-NAT Firewall Requirements to Support IPsec Rules

Source	Protocol	Port	Destination	Notes
Security server	ISAKMP	UDP 500	View Connection Server	Security servers use UDP port 500 to negotiate IPsec security.
Security server	ESP	N/A	View Connection Server	ESP protocol encapsulates IPsec encrypted traffic. You do not have to specify a port for ESP as part of the rule. If necessary, you can specify source and destination IP addresses to reduce the scope of the rule.

The following rules apply to firewalls that use NAT.

Table 5-6. NAT Firewall Requirements to Support IPsec Rules

Source	Protocol	Port	Destination	Notes
Security server	ISAKMP	UDP 500	View Connection Server	Security servers use UDP port 500 to initiate IPsec security negotiation.
Security server	NAT-T ISAKMP	UDP 4500	View Connection Server	Security servers use UDP port 4500 to traverse NATs and negotiate IPsec security.

Reinstall View Connection Server with a Backup Configuration

In certain situations, you might have to reinstall the current version of a View Connection Server instance and restore the existing View configuration by importing a backup LDIF file that contains the View LDAP configuration data.

For example, as part of a business continuity and disaster recovery (BC/DR) plan, you might want to have a procedure ready to implement in case a datacenter stops functioning. The first step in such a plan is to ensure that the View LDAP configuration is backed up in another location. A second step is to install View Connection Server in the new location and import the backup configuration, as described in this procedure.

You might also use this procedure when you set up a second datacenter with the existing View configuration. Or you might use it if your View deployment contains only a single View Connection Server instance, and a problem occurs with that server.

You do not have to follow this procedure if you have multiple View Connection Server instances in a replicated group, and a single instance goes down. You can simply reinstall View Connection Server as a replicated instance. During the installation, you provide connection information to another View Connection Server instance, and View restores the View LDAP configuration from the other instance.

Prerequisites

- Verify that the View LDAP configuration was backed up to an encrypted LDIF file.
- Familiarize yourself with restoring a View LDAP configuration from an LDIF backup file by using the `vdmimport` command.

  See "Backing Up and Restoring View Configuration Data" in the *VMware Horizon View Administration* document.
- Familiarize yourself with the steps for installing a new View Connection Server instance. See "Install View Connection Server with a New Configuration," on page 38.

Procedure

1 Install View Connection Server with a new configuration.

2 Decrypt the encrypted LDIF file.

  For example:

```
vdmimport –d –p mypassword
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

3 Import the decrypted LDIF file to restore the View LDAP configuration.

  For example:

```
vdmimport –f MyDecryptedexport.LDF
```

  NOTE At this stage, the View configuration is not yet accessible. View clients cannot access View Connection Server or connect to their desktops.

4 Uninstall the View Connection Server from the computer by using the Windows **Add/Remove Programs** utility.

  Do not uninstall the View LDAP configuration, called the AD LDS Instance VMwareVDMDS instance. You can use the **Add/Remove Programs** utility to verify that the AD LDS Instance VMwareVDMDS instance was not removed from the Windows Server computer.

5 Reinstall View Connection Server.

  At the installer prompt, accept the existing View LDAP directory.

What to do next

Configure View Connection Server and your View environment as you would after you install a View Connection Server instance with a new configuration.

Microsoft Windows Installer Command-Line Options

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

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

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

Table 5-7 shows the command-line options that control the installer's bootstrap program.

Table 5-7. Command-Line Options for a View Component's Bootstrap Program

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

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

Table 5-8 shows the command-line options and MSI property values that are passed to the MSI installer.

Table 5-8. MSI Command-Line Options and MSI Properties

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

Table 5-8. MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
ADDLOCAL	Determines the component-specific features to install. In an interactive installation, the View installer displays custom setup options to select. The MSI property, ADDLOCAL, lets you specify these setup options on the command line. To install all available custom setup options, enter ADDLOCAL=ALL. For example: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" If you do not use the MSI property, ADDLOCAL, the default setup options are installed. To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format *ADDLOCAL=value,value,value...*. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" NOTE The Core feature is required in View Agent. This MSI property is optional.
REBOOT	You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.
/l*v *log_file*	Writes logging information into the specified log file with verbose output. For example: /l*v ""%TEMP%\vmmsi.log"" This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The /l*v option is optional.

Uninstalling View Products Silently by Using MSI Command-Line Options

You can uninstall View components by using Microsoft Windows Installer (MSI) command-line options.

Syntax

```
msiexec.exe
/qb
/x
product_code
```

Options

The /qb option displays the uninstall progress bar. To suppress displaying the uninstall progress bar, replace the /qb option with the /qn option.

The /x option uninstalls the View component.

The *product_code* string identifies the View component product files to the MSI uninstaller. You can find the *product_code* string by searching for ProductCode in the %TEMP%\vmmsi.log file that is created during the installation.

For information about MSI command-line options, see "Microsoft Windows Installer Command-Line Options," on page 57.

Examples

Uninstall a View Connection Server instance.

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

Installing View Transfer Server 6

View Transfer Server transfers data between local desktops and the datacenter during check in, check out, and replication. To install View Transfer Server, you install the software on a Windows Server virtual machine, add View Transfer Server to your View Manager deployment, and configure the Transfer Server repository.

You must install and configure View Transfer Server if you deploy View Client with Local Mode on client computers.

You must have a license to install View Transfer Server and use local desktops.

1 Install View Transfer Server on page 61

View Transfer Server downloads system-image files, synchronizes data between local desktops and the corresponding remote desktops in the datacenter, and transfers data when users check in and check out local desktops. You install View Transfer Server in a virtual machine that runs Windows Server.

2 Add View Transfer Server to View Manager on page 63

View Transfer Server works with View Connection Server to transfer files and data between local desktops and the datacenter. Before View Transfer Server can perform these tasks, you must add it to your View Manager deployment.

3 Configure the Transfer Server Repository on page 64

The Transfer Server repository stores View Composer base images for linked-clone desktops that run in local mode. To give View Transfer Server access to the Transfer Server repository, you must configure it in View Manager. If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository.

4 Firewall Rules for View Transfer Server on page 65

Certain incoming TCP ports must be opened on the firewall for View Transfer Server instances.

5 Installing View Transfer Server Silently on page 65

You can install View Transfer Server silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Install View Transfer Server

View Transfer Server downloads system-image files, synchronizes data between local desktops and the corresponding remote desktops in the datacenter, and transfers data when users check in and check out local desktops. You install View Transfer Server in a virtual machine that runs Windows Server.

At runtime, View Transfer Server is deployed to an Apache Web Server. When you install View Transfer Server, the installer configures Apache Web Server as a service on the virtual machine. The Apache service uses ports 80 and 443.

Prerequisites

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in "View Transfer Server Requirements," on page 11.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Verify that you did not manually add or remove PCI devices on the virtual machine on which you plan to install View Transfer Server. If you add or remove PCI devices, View might be unable to discover hot-added devices, which might cause data transfer operations to fail.
- Familiarize yourself with the network ports that must be opened on the Windows Firewall for View Connection Server instances. See "Firewall Rules for View Transfer Server," on page 65.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 To start the installation program, double-click the installer file.

3 Accept the VMware license terms.

4 Accept or change the destination folder.

5 Select **View Transfer Server**.

6 Configure the Apache Web Server to which View Transfer Server is deployed.

You can accept the default values for the network domain, Apache Server name, and administrator's email address that are provided by the installer.

7 Choose how to configure the Windows Firewall service.

Option	Action
Configure Windows Firewall automatically	Let the installer configure Windows Firewall to allow the required network connections.
Do not configure Windows Firewall	Configure the Windows firewall rules manually.

8 Complete the installation program to install View Transfer Server.

The VMware View Transfer Server, View Transfer Server Control Service, and VMware View Framework Component services are installed and started on the virtual machine.

What to do next

In View Administrator, add View Transfer Server to your View Manager deployment.

Add View Transfer Server to View Manager

View Transfer Server works with View Connection Server to transfer files and data between local desktops and the datacenter. Before View Transfer Server can perform these tasks, you must add it to your View Manager deployment.

You can add multiple View Transfer Server instances to View Manager. The View Transfer Server instances access one common Transfer Server repository. They share the transfer workload for the local desktops that are managed by a View Connection Server instance or by a group of replicated View Connection Server instances.

NOTE When View Transfer Server is added to View Manager, its Distributed Resource Scheduler (DRS) automation policy is set to Manual, which effectively disables DRS.

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that vCenter Server is added to View Manager. The **View Configuration > Servers** page in View Administrator displays vCenter Server instances that are added to View Manager.
- If View Transfer Server is version 5.1 or later, and you plan to use linked-clone desktops in local mode, verify that all replicated View Connection Server instances in the View configuration are version 5.1 or later. If an earlier version of View Connection Server sends a request to publish a base image to the Transfer Server repository, View Transfer Server cannot perform the publish operation.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 Click the Transfer Servers tab and click **Add**.

3 In the Add Transfer Server wizard, select the vCenter Server instance that manages the View Transfer Server virtual machine and click **Next**.

4 Select the virtual machine where View Transfer Server is installed and click **Finish**.

View Connection Server reconfigures the virtual machine with four SCSI controllers. The multiple SCSI controllers allow View Transfer Server to perform an increased number of disk transfers concurrently.

In View Administrator, the View Transfer Server instance appears in the Transfer Servers panel. If no Transfer Server repository is configured, the View Transfer Server status changes from **Pending** to **No Transfer Server Repository Configured**. If a Transfer Server repository is configured, the status changes from **Pending** to **Initializing Transfer Server Repository** to **Ready**.

This process can take several minutes. You can click the refresh button in View Administrator to check the current status.

When the View Transfer Server instance is added to View Manager, the Apache service is started on the View Transfer Server virtual machine.

CAUTION If your View Transfer Server virtual machine is an earlier version than hardware version 7, you must configure the static IP address on the View Transfer Server virtual machine after you add View Transfer Server to View Manager.

When multiple SCSI controllers are added to the View Transfer Server virtual machine, Windows removes the static IP address and reconfigures the virtual machine to use DHCP. After the virtual machine restarts, you must re-enter the static IP address in the virtual machine.

Configure the Transfer Server Repository

The Transfer Server repository stores View Composer base images for linked-clone desktops that run in local mode. To give View Transfer Server access to the Transfer Server repository, you must configure it in View Manager. If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository.

If View Transfer Server is configured in View Manager before you configure the Transfer Server repository, View Transfer Server validates the location of the Transfer Server repository during the configuration.

If you plan to add multiple View Transfer Server instances to this View Manager deployment, configure the Transfer Server repository on a network share. Other View Transfer Server instances cannot access a Transfer Server repository that is configured on a local drive on one View Transfer Server instance.

Make sure that the Transfer Server repository is large enough to store your View Composer-generated base images. A base image can be several gigabytes in size.

If you configure a remote Transfer Server repository on a network share, you must provide a user ID with credentials to access the network share. As a best practice, to enhance the security of access to the Transfer Server repository, make sure that you restrict network access for the repository to View administrators.

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that View Transfer Server is added to View Manager. See "Add View Transfer Server to View Manager," on page 63.

NOTE Adding View Transfer Server to View Manager before you configure the Transfer Server repository is a best practice, not a requirement.

Procedure

1 Configure a path and folder for the Transfer Server repository.

The Transfer Server repository can be on a local drive or a network share.

Option	Action
Local Transfer Server repository	On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: `C:\TransferRepository\`
Remote Transfer Server repository	Configure a UNC path for the network share. For example: `\\server.domain.com\TransferRepository\` All View Transfer Server instances that you add to this View Manager deployment must have network access to the shared drive.

2 In View Administrator, click **View Configuration > Servers**.

3 Put all View Transfer Server instances into maintenance mode.

a In the Transfer Servers panel, select a View Transfer Server instance.

b Click **Enter Maintenance Mode** and click **OK**.

The View Transfer Server status changes to **Maintenance mode**.

c Repeat Step 3a and Step 3b for each instance.

When all View Transfer Server instances are in maintenance mode, current transfer operations are stopped.

4 In the General panel on the Transfer Server repository page, click **Edit**.

5 Type the Transfer Server repository location and other information.

Option	Description
Network share	■ **Path**. Type the UNC path that you configured. ■ **User name**. Type the user ID of an administrator with credentials to access the network share. ■ **Password**. Type the administrator password. ■ **Domain**. Type the domain name of the network share in NetBIOS format. Do not use the `.com` suffix.
Local filesystem	Type the path that you configured on the local View Transfer Server virtual machine.

6 Click **OK**.

If the repository network path or local drive is incorrect, the Edit Transfer Server Repository dialog displays an error message and does not let you configure the location. You must type a valid location.

7 On the **View Configuration > Servers** page, select the View Transfer Server instance and click **Exit Maintenance Mode**.

The View Transfer Server status changes to **Ready**.

Firewall Rules for View Transfer Server

Certain incoming TCP ports must be opened on the firewall for View Transfer Server instances.

The installation program can optionally configure the required Windows firewall rules for you. These rules open the ports that are used by default. If you change the default ports after installation, you must manually configure the Windows firewall to allow View Client devices to connect to View Transfer Server through the updated ports.

Table 6-1 lists the incoming TCP ports that must be opened on the firewall for View Transfer Server instances.

Table 6-1. TCP Ports for View Transfer Server Instances

Protocol	Ports
HTTP	80
HTTPS	443

Installing View Transfer Server Silently

You can install View Transfer Server silently by typing the installer filename and installation options at the command line. With silent installation, you can efficiently deploy View components in a large enterprise.

Set Group Policies to Allow Silent Installation of View Transfer Server

Before you can install View Transfer Server silently, you must configure Microsoft Windows group policies to allow installation with elevated privileges.

You must set Windows Installer group policies for computers and for users on the local computer.

Prerequisites

Verify that you have local administrator privileges on the Windows Server computer on which you will install View Transfer Server.

Procedure

1 Log in to the Windows Server computer and click **Start > Run**.

2 Type **gpedit.msc** and click **OK**.

3 In the Group Policy Object Editor, click **Local Computer Policy > Computer Configuration**.

4 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

5 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

6 In the left pane, click **User Configuration**.

7 Expand **Administrative Templates**, expand **Windows Components**, open the **Windows Installer** folder, and double-click **Always install with elevated privileges**.

8 In the **Always Install with Elevated Privileges Properties** window, click **Enabled** and click **OK**.

What to do next

Install View Transfer Server silently.

Install View Transfer Server Silently

You can use the silent installation feature of the Microsoft Windows Installer (MSI) to install View Transfer Server on several Windows computers. In a silent installation, you use the command line and do not have to respond to wizard prompts.

Prerequisites

- Verify that you have local administrator privileges on the Windows Server on which you will install View Transfer Server.
- Verify that your installation satisfies the View Transfer Server requirements described in "View Transfer Server Requirements," on page 11.
- Verify that you have a license to install View Transfer Server and use local desktops.
- Verify that the virtual machine on which you install View Transfer Server has version 2.0 or later of the MSI runtime engine. For details, see the Microsoft Web site.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 57.
- Familiarize yourself with the silent installation properties available with View Transfer Server. See "Silent Installation Properties for View Transfer Server," on page 67.
- Verify that the Windows Installer group policies that are required for silent installation are configured on the Windows Server computer. See "Set Group Policies to Allow Silent Installation of View Transfer Server," on page 65.

Procedure

1 Download the View Connection Server installer file from the VMware product page at http://www.vmware.com/products/ to the Windows Server computer.

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

2 Open a command prompt on the Windows Server computer.

3 Type the installation command on one line.

For example: `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"`

The VMware View Transfer Server, View Transfer Server Control Service, and VMware View Framework Component services are installed and started on the virtual machine.

What to do next

In View Administrator, add View Transfer Server to your View Manager deployment.

Silent Installation Properties for View Transfer Server

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

Table 6-2. MSI Properties for Silently Installing View Transfer Server

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Connection Server software is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of two double quotes that enclose the path permit the MSI installer to interpret the space as a valid part of the path. This MSI property is optional.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	The type of View server installation: ■ **1**. Standard installation ■ **2**. Replica installation ■ **3**. Security server installation ■ **4**. View Transfer Server installation To install a View Transfer Server, define `VDM_SERVER_INSTANCE_TYPE=4` This MSI property is optional for a standard installation. It is required for all other types of installation.	1
SERVERDOMAIN	The network domain of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server network domain that is configured during an interactive installation. For example: `SERVERDOMAIN=companydomain.com` If you specify a custom Apache Web Server domain with the MSI property, `SERVERDOMAIN`, you also must specify custom `SERVERNAME` and `SERVERADMIN` properties. This MSI property is optional.	None
SERVERNAME	The host name of the virtual machine on which you install View Transfer Server. This value corresponds to the Apache Web Server host name that is configured during an interactive installation. For example: `SERVERNAME=ts1.companydomain.com` If you specify a custom Apache Web Server host name with the MSI property, `SERVERNAME`, you also must specify custom `SERVERDOMAIN` and `SERVERADMIN` properties. This MSI property is optional.	None

Table 6-2. MSI Properties for Silently Installing View Transfer Server (Continued)

MSI Property	Description	Default Value
SERVERADMIN	The email address of the administrator of Apache Web Server that is configured with View Transfer Server. For example: `SERVERADMIN=admin@companydomain.com` If you specify a custom Apache Web Server administrator with the MSI property, `SERVERADMIN`, you also must specify custom `SERVERDOMAIN` and `SERVERNAME` properties. This MSI property is optional.	None
FWCHOICE	The MSI property that determines whether to configure a firewall for the View Connection Server instance. A value of 1 configures a firewall. A value of 2 does not configure a firewall. For example: `FWCHOICE=1` This MSI property is optional.	1

Configuring SSL Certificates for View Servers

7

VMware strongly recommends that you configure SSL certificates for authentication of View Connection Server instances, security servers, and View Composer service instances.

A default SSL server certificate is generated when you install View Connection Server instances, security servers, or View Composer instances. You can use the default certificate for testing purposes.

IMPORTANT Replace the default certificate as soon as possible. The default certificate is not signed by a Certificate Authority (CA). Use of certificates that are not signed by a CA can allow untrusted parties to intercept traffic by masquerading as your server.

This chapter includes the following topics:

Understanding SSL Certificates for View Servers

You must follow certain guidelines for configuring SSL certificates for View servers and related components.

View Connection Server and Security Server

SSL is required for View Client connections to View. Client-facing View Connection Server instances, security servers, and intermediate servers that terminate SSL connections require SSL server certificates.

By default, when you install View Connection Server or security server, the installation generates a self-signed certificate for the View server. However, the installation uses an existing certificate in the following cases:

- If a valid certificate with a Friendly name of `vdm` already exists in the Windows Certificate Store

- If you upgrade to View 5.1 or later from an earlier release, and a valid keystore file is configured on the Windows Server computer. The installation extracts the keys and certificates and imports them into the Windows Certificate Store.

vCenter Server and View Composer

Before you add vCenter Server and View Composer to View Manager in a production environment, make sure that vCenter Server and View Composer use certificates that are signed by a CA.

For information about replacing the default certificate for vCenter Server, see "Replacing vCenter Server Certificates" on the VMware Technicap Papers site at http://www.vmware.com/resources/techresources/.

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.

PCoIP Secure Gateway

To comply with industry or jurisdiction security regulations, you can replace the default SSL certificate that is generated by the PCoIP Secure Gateway (PSG) service with a certificate that is signed by a CA. Configuring the PSG service to use a CA-signed certificate is highly recommended, particularly for deployments that require you to use security scanners to pass compliance testing. See "Configure the PCoIP Secure Gateway to Use a New SSL Certificate," on page 81.

Blast Secure Gateway

By default, the Blast Secure Gateway (BSG) uses the SSL certificate that is configured for the View Connection Server instance or security server on which the BSG is running. If you replace the default, self-signed certificate for a View server with a CA-signed certificate, the BSG also uses the CA-signed certificate.

View Transfer Server

You do not have to configure SSL certificates for View Transfer Server if you are installing View 5.1 or later.

A default, self-signed certificate is installed with View Transfer Server that View Connection Server uses to handle secondary connections to View Clients. See "View Transfer Server and SSL Certificates," on page 85.

SAML 2.0 Authenticator

VMware Horizon Suite uses SAML 2.0 authenticators to provide Web-based authentication and authorization across security domains. If you want View to delegate authentication to the Horizon Suite, you can configure View to accept SAML 2.0 authenticated sessions from Horizon Suite. When Horizon Application Manager is configured to support View, Horizon users can connect to View desktops by selecting desktop icons on the Horizon User Portal.

In View Administrator, you can configure SAML 2.0 authenticators for use with View Connection Server instances.

Before you add a SAML 2.0 authenticator in View Administrator, make sure that the SAML 2.0 authenticator uses a certificate that is signed by a CA.

Additional Guidelines

For general information about requesting and using SSL certificates that are signed by a CA, see "Benefits of Using SSL Certificates Signed by a CA," on page 86.

When View Clients connect to a View Connection Server instance or security server, they are presented with the View server's SSL server certificate and any intermediate certificates in the trust chain. To trust the server certificate, the client systems must have installed the root certificate of the signing CA.

When View Connection Server communicates with vCenter Server and View Composer, View Connection Server is presented with SSL server certificates and intermediate certificates from these servers. To trust the vCenter Server and View Composer servers, the View Connection Server computer must have installed the root certificate of the signing CA.

Similarly, if a SAML 2.0 authenticator is configured for View Connection Server, the View Connection Server computer must have installed the root certificate of the signing CA for the SAML 2.0 server certificate.

Overview of Tasks for Setting Up SSL Certificates

To set up SSL server certificates for View servers, you must perform several high-level tasks.

The procedures for carrying out these tasks are described in the topics that follow this overview.

1 Determine if you need to obtain a new signed SSL certificate from a CA.

  If your organization already has a valid SSL server certificate, you can use that certificate to replace the default SSL server certificate provided with View Connection Server, security server, or View Composer. To use an existing certificate, you also need the accompanying private key.

Starting Place	Action
Your organization provided you with a valid SSL server certificate.	Go directly to step 2.
You do not have an SSL server certificate.	Obtain a signed SSL server certificate from a CA.

2 Import the SSL certificate into the Windows local computer certificate store on the View server host.

3 For View Connection Server instances and security servers, modify the certificate Friendly name to **`vdm`**.

  Assign the Friendly name **`vdm`** to only one certificate on each View server host.

4 On View Connection Server computers, if the root certificate is not trusted by the Windows Server host, import the root certificate into the Windows local computer certificate store.

  Take this step for View Connection Server instances only. You do not have to import the root certificate to View Composer, vCenter Server, or security server hosts.

5 If your server certificate was signed by an intermediate CA, import the intermediate certificates into the Windows local computer certificate store.

  To simplify client configuration, import the entire certificate chain into the Windows local computer certificate store. If intermediate certificates are missing from the View server, they must be configured for View Clients and computers that launch View Administrator.

6 For View Composer instances, take one of these steps:

  - If you import the certificate into the Windows local computer certificate store before you install View Composer, you can select your certificate during the View Composer installation.
  - If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate after you install View Composer, run the `SviConfig ReplaceCertificate` utility to bind the new certificate to the port used by View Composer.

7 If your CA is not well known, configure View Clients to trust the root and intermediate certificates.

  Also ensure that the computers on which you launch View Administrator trust the root and intermediate certificates.

8 Determine whether to reconfigure certificate revocation checking.

View Connection Server performs certificate revocation checking on View servers, View Composer, and vCenter Server. Most certificates signed by a CA include certificate revocation information. If your CA does not include this information, you can configure the server not to check certificates for revocation.

If a SAML 2.0 authenticator is configured for use with a View Connection Server instance, View Connection Server also performs certificate revocation checking on the SAML 2.0 server certificate.

Obtaining a Signed SSL Certificate from a CA

If your organization does not provide you with an SSL server certificate, you must request a new certificate that is signed by a CA.

You can use several methods to obtain a new signed certificate. For example, you can use the Microsoft `certreq` utility to generate a Certificate Signing Request (CSR) and submit a certificate request to a CA.

See the *Obtaining SSL Certificates for VMware Horizon View Servers* document for an example that shows you how to use `certreq` to accomplish this task.

For testing purposes, you can obtain a free temporary certificate based on an untrusted root from many CAs.

When you generate a certificate request on a computer, make sure that a private key is generated also. When you obtain the SSL server certificate and import it into the Windows local computer certificate store, there must be an accompanying private key that corresponds to the certificate.

IMPORTANT Do not create certificates for View servers using a certificate template that is compatible only with a Windows Server 2008 enterprise CA or later.

IMPORTANT Do not generate certificates for View servers using a `KeyLength` value under 1024. View Client for Windows and View Client for Windows with Local Mode will not validate a certificate on a View server that was generated with a `KeyLength` under 1024, and the View Clients will fail to connect to View. Certificate validations that are performed by View Connection Server will also fail, resulting in the affected View servers showing as red in the View Administrator dashboard.

For general information about obtaining certificates, consult the Microsoft online help available with the Certificate Snap-in to MMC. If the Certificate Snap-in is not yet installed on your computer, see "Add the Certificate Snap-In to MMC," on page 74.

Obtain a Signed Certificate from a Windows Domain or Enterprise CA

To obtain a signed certificate from a Windows Domain or Enterprise CA, you can use the Windows Certificate Enrollment wizard in the Windows Certificate Store.

This method of requesting a certificate is appropriate if communications between computers remain within your internal domain. For example, obtaining a signed certificate from a Windows Domain CA might be appropriate for server-to-server communications.

If your View Clients connect to View servers from an external network, request SSL server certificates that are signed by a trusted, third-party CA.

Prerequisites

- Determine the fully qualified domain name (FQDN) that client computers use to connect to the host.
- Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC," on page 74.
- Verify that you have the appropriate credentials to request a certificate that can be issued to a computer or service.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (local computer)** node and select the **Personal** folder.

2 From the **Action** menu, go to **All Tasks > Request New Certificate** to display the Certificate Enrollment wizard.

3 Select a Certificate Enrollment Policy.

4 Select the types of certificates that you want to request and click **Enroll**.

5 Click **Finish**.

The new signed certificate is added to the **Personal > Certificates** folder in the Windows Certificate Store.

What to do next

- Verify that the server certificate and certificate chain were imported into the Windows Certificate Store.
- For a View Connection Server instance or security server, modify the certificate friendly name to **vdm**. See "Modify the Certificate Friendly Name," on page 75.
- For a View Composer server, bind the new certificate to the port that used by View Composer. See "Bind a New SSL Certificate to the Port Used by View Composer," on page 77.

Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate

To configure a View Connection Server instance, security server, or View Composer instance to use an SSL certificate, you must import the server certificate and the entire certificate chain into the Windows local computer certificate store on the View Connection Server, security server, or View Composer host.

By default, the Blast Secure Gateway (BSG) uses the SSL certificate that is configured for the View Connection Server instance or security server on which the BSG is running. If you replace the default, self-signed certificate for a View server with a CA-signed certificate, the BSG also uses the CA-signed certificate.

IMPORTANT To configure View Connection Server or security server to use a certificate, you must change the certificate Friendly name to **vdm**. Also, the certificate must have an accompanying private key.

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 run the `SviConfig ReplaceCertificate` utility to bind the new certificate to the port used by View Composer.

Procedure

1 Add the Certificate Snap-In to MMC on page 74

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the View server is installed.

2 Import a Signed Server Certificate into a Windows Certificate Store on page 74

You must import the SSL server certificate into the Windows local computer certificate store on the Windows Server host on which the View Connection Server instance, security server, or View Composer service is installed.

3 Modify the Certificate Friendly Name on page 75

To configure a View Connection Server instance or security server to recognize and use an SSL certificate, you must modify the certificate Friendly name to `vdm`.

4 Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store on page 76

If the Windows Server host on which View Connection Server is installed does not trust the root certificate for the signed SSL server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the View Connection Server host does not trust the root certificates of the SSL server certificates configured for security server, View Composer, and vCenter Server hosts, you also must import those root certificates.

5 Bind a New SSL Certificate to the Port Used by View Composer on page 77

If you configure a new SSL certificate after you install View Composer, you must run the `SviConfig ReplaceCertificate` utility to replace the certificate that is bound to the port used by View Composer. This utility unbinds the existing certificate and binds the new certificate to the port.

Add the Certificate Snap-In to MMC

Before you can add certificates to the Windows Certificate Store, you must add the Certificate snap-in to the Microsoft Management Console (MMC) on the Windows Server host on which the View server is installed.

Prerequisites

Verify that the MMC and Certificate snap-in are available on the Windows Server computer on which the View server is installed.

Procedure

1 On the Windows Server computer, click **Start** and type **`mmc.exe`**.

2 In the MMC window, go to **File > Add/Remove Snap-in**.

3 In the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

4 In the Certificates snap-in window, select **Computer account**, click **Next**, select **Local computer**, and click **Finish**.

5 In the Add or Remove snap-in window, click **OK**.

What to do next

Import the SSL server certificate into the Windows Certificate Store.

Import a Signed Server Certificate into a Windows Certificate Store

You must import the SSL server certificate into the Windows local computer certificate store on the Windows Server host on which the View Connection Server instance, security server, or View Composer service is installed.

Depending on your certificate file format, the entire certificate chain that is contained in the keystore file might be imported into the Windows local computer certificate store. For example, the server certificate, intermediate certificate, and root certificate might be imported.

For other types of certificate files, only the server certificate is imported into the Windows local computer certificate store. In this case, you must take separate steps to import the root certificate and any intermediate certificates in the certificate chain.

For more information about certificates, consult the Microsoft online help available with the Certificate snap-in to MMC.

Note If you off-load SSL connections to an intermediate server, you must import the same SSL server certificate onto both the intermediate server and the off-loaded View server. For details, see "Off-load SSL Connections to Intermediate Servers" in the *VMware Horizon View Administration* document.

Prerequisites

Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC," on page 74.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal** folder.

2 In the Actions pane, go to **More Actions > All Tasks > Import**.

3 In the Certificate Import wizard, click **Next** and browse to the location where the certificate is stored.

4 Select the certificate file and click **Open**.

To display your certificate file type, you can select its file format from the **File name** drop-down menu.

5 Type the password for the private key that is included in the certificate file.

6 Select **Mark this key as exportable**.

7 Select **Include all extendable properties**.

8 Click **Next** and click **Finish**.

The new certificate appears in the **Certificates (Local Computer) > Personal > Certificates** folder.

9 Verify that the new certificate contains a private key.

a In the **Certificates (Local Computer) > Personal > Certificates** folder, double-click the new certificate.

b In the General tab of the Certificate Information dialog box, verify that the following statement appears: `You have a private key that corresponds to this certificate`.

What to do next

Modify the certificate Friendly name to **`vdm`**.

Modify the Certificate Friendly Name

To configure a View Connection Server instance or security server to recognize and use an SSL certificate, you must modify the certificate Friendly name to `vdm`.

You do not have to modify the Friendly name of SSL certificates that are used by View Composer.

Prerequisites

Verify that the server certificate is imported into the **Certificates (Local Computer) > Personal > Certificates** folder in the Windows Certificate Store. See "Import a Signed Server Certificate into a Windows Certificate Store," on page 74.

Procedure

1 In the MMC window on the Windows Server host, expand the **Certificates (Local Computer)** node and select the **Personal > Certificates** folder.

2 Right-click the certificate that is issued to the View server host and click **Properties**.

3 On the General tab, delete the **Friendly name** text and type **`vdm`**.

4 Click **Apply** and click **OK**.

What to do next

Import the root certificate and intermediate certificates into the Windows local computer certificate store.

After all certificates in the chain are imported, you must restart the View Connection Server service or Security Server service to make your changes take effect.

Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store

If the Windows Server host on which View Connection Server is installed does not trust the root certificate for the signed SSL server certificate, you must import the root certificate into the Windows local computer certificate store. In addition, if the View Connection Server host does not trust the root certificates of the SSL server certificates configured for security server, View Composer, and vCenter Server hosts, you also must import those root certificates.

If the View Connection Server, security server, View Composer, and vCenter Server certificates are signed by a root CA that is known and trusted by the View Connection Server host, and there are no intermediate certificates in your certificate chains, you can skip this task. Commonly used Certificate Authorities are likely to be trusted by the host.

NOTE You do not have to import the root certificate into View Composer, vCenter Server, or security server hosts.

If a server certificate is signed by an intermediate CA, you also must import each intermediate certificate in the certificate chain. To simplify client configuration, import the entire intermediate chain to security server, View Composer, and vCenter Server hosts as well as View Connection Server hosts. If intermediate certificates are missing from a View Connection Server or security server host, they must be configured for View Clients and computers that launch View Administrator. If intermediate certificates are missing from a View Composer or vCenter Server host, they must be configured for each View Connection Server instance.

If you already verified that the entire certificate chain is imported into the Windows local computer certificate store, you can skip this task.

NOTE If a SAML 2.0 authenticator is configured for use by a View Connection Server instance, the same guidelines apply to the SAML 2.0 authenticator. If the View Connection Server host does not trust the root certificate configured for a SAML 2.0 authenticator, or if the SAML 2.0 server certificate is signed by an intermediate CA, you must ensure that the certificate chain is imported into the Windows local computer certificate store.

Procedure

1. In the MMC console on the Windows Server host, expand the **Certificates (Local Computer)** node and go to the **Trusted Root Certification Authorities > Certificates** folder.
   - If your root certificate is in this folder, and there are no intermediate certificates in your certificate chain, skip to step 7.
   - If your root certificate is not in this folder, proceed to step 2.
2. Right-click the **Trusted Root Certification Authorities > Certificates** folder and click **All Tasks > Import**.
3. In the Certificate Import wizard, click **Next** and browse to the location where the root CA certificate is stored.
4. Select the root CA certificate file and click **Open**.
5. Click **Next**, click **Next**, and click **Finish**.

6 If your server certificate was signed by an intermediate CA, import all intermediate certificates in the certificate chain into the Windows local computer certificate store.

   a Go to the **Certificates (Local Computer) > Intermediate Certification Authorities > Certificates** folder.

   b Repeat steps 3 through 6 for each intermediate certificate that must be imported.

7 Restart the View Connection Server service, Security Server service, View Composer service, or vCenter Server service to make your changes take effect.

Bind a New SSL Certificate to the Port Used by View Composer

If you configure a new SSL certificate after you install View Composer, you must run the `SviConfig ReplaceCertificate` utility to replace the certificate that is bound to the port used by View Composer. This utility unbinds the existing certificate and binds the new certificate to the port.

If you install the new certificate on the Windows Server computer before you install View Composer, you do not have to run the `SviConfig ReplaceCertificate` utility. When you run the View Composer installer, you can select a certificate signed by a CA instead of the default, self-signed certificate. During the installation, the selected certificate is bound to the port used by View Composer.

If you intend to replace an existing certificate or the default, self-signed certificate with a new certificate, you must use the `SviConfig ReplaceCertificate` utility.

Prerequisites

Verify that the new certificate was imported into the Windows local computer certificate store on the Windows Server computer on which View Composer is installed.

Procedure

1 Stop the View Composer service.

2 Open a command prompt on the Windows Server host where View Composer is installed.

3 Type the `SviConfig ReplaceCertificate` command.

   For example:

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

   where `–delete` is a required parameter that operates on the certificate that is being replaced. You must specify either `–delete=true` to delete the old certificate from the Windows local computer certificate store or `–delete=false` to keep the old certificate in the Windows certificate store.

   The utility displays a numbered list of SSL certificates that are available in the Windows local computer certificate store.

4 To select a certificate, type the number of a certificate and press Enter.

5 Restart the View Composer service to make your changes take effect.

Example: SviConfig ReplaceCertificate

The following example replaces the certificate that is bound to the View Composer port:

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

Configure View Clients to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by View Client computers and client computers that access View Administrator, you can configure all Windows client systems in a domain to trust the root and intermediate certificates. To do so, you must add the public key for the root certificate to the Trusted Root Certification Authorities group policy in Active Directory and add the root certificate to the Enterprise NTAuth store.

For example, you might have to take these steps if your organization uses an internal certificate service.

You do not have to take these steps if the Windows domain controller acts as the root CA, or if your certificates are signed by a well known CA. For well known CAs, the operating system venders preinstall the root certificate on client systems.

If your View server certificates are signed by a little-known intermediate CA, you must add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory.

For View Clients that run on other operating systems and devices, see the following instructions for distributing root and intermediate certificates that users can install:

- For View Client for Mac OS X, see "Configure View Client for Mac OS X to Trust Root and Intermediate Certificates," on page 79.
- For View Client for iPad, see "Configure View Client for iPad to Trust Root and Intermediate Certificates," on page 79.
- For View Client for Android, see documentation on the Google Web site, such as the *Android 3.0 User's Guide*
- For View Client for Linux, see the Ubuntu documentation

Prerequisites

Verify that the View server certificate was generated with a `KeyLength` value of 1024 or larger. View Client for Windows and View Client for Windows with Local Mode will not validate a certificate on a View server that was generated with a `KeyLength` under 1024, and the View Clients will fail to connect to View.

Procedure

1 On your Active Directory server, use the `certutil` command to publish the certificate to the Enterprise NTAuth store.

For example: **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

2 On the Active Directory server, navigate to the Group Policy Management plug-in.

AD Version	Navigation Path
Windows 2003	a Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. b Right-click your domain and click **Properties**. c On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in. d Right-click **Default Domain Policy**, and click **Edit**.
Windows 2008	a Select **Start > Administrative Tools > Group Policy Management**. b Expand your domain, right-click **Default Domain Policy**, and click **Edit**.

3 Expand the **Computer Configuration** section and go to **Windows Settings > Security Settings > Public Key Policies**.

4 Import the certificate.

Option	Description
Root certificate	a Right-click **Trusted Root Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.
Intermediate certificate	a Right-click **Intermediate Certification Authorities** and select **Import**. b Follow the prompts in the wizard to import the intermediate certificate (for example, `intermediateCA.cer`) and click **OK**.

5 Close the Group Policy window.

All systems in the domain now have certificate information in their trusted root certificate stores and intermediate certificate stores that allows them to trust the root and intermediate certificates.

Configure View Client for Mac OS X to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by computers that run View Client for Mac OS X, you can configure these computers to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the client computers.

Procedure

1 Deliver the root certificate and intermediate certificates to the computer that is running View Client for Mac OS X.

2 Open the root certificate on the Mac OS X computer.

The certificate displays the following message: `Do you want your computer to trust certificates signed by` *`CA name`* `from now on?`

3 Click **Always Trust**

4 Type the user password.

5 Repeat steps 2 through 4 for all intermediate certificates in the trust chain.

Configure View Client for iPad to Trust Root and Intermediate Certificates

If a View server certificate is signed by a CA that is not trusted by iPads that run View Client for iPad, you can configure the iPads to trust the root and intermediate certificates. You must distribute the root certificate and all intermediate certificates in the trust chain to the iPads.

Procedure

1 Send the root certificate and intermediate certificates as email attachments to the iPad.

2 Open the email attachment for the root certificate and select **Install**.

The certificate displays the following message:

`Unverifiable Profile. The authenticity of` *`Certificate name`* `cannot be verified. Installing this profile will change settings on your iPad.`

`Root Certificate. Installing the certificate` *`Certificate name`* `will add it to the list of trusted certificates on your iPad.`

3 Select **Install** again.

4 Repeat steps 2 and 3 for all intermediate certificates in the trust chain.

Configuring Certificate Revocation Checking on Server Certificates

Each View Connection Server instance performs certificate revocation checking on its own certificate and on those of the security servers paired to it. Each instance also checks the certificates of vCenter and View Composer servers whenever it establishes a connection to them. By default, all certificates in the chain are checked except the root certificate. You can, however, change this default.

If a SAML 2.0 authenticator is configured for use by a View Connection Server instance, View Connection Server also performs certificate revocation checking on the SAML 2.0 server certificate.

View supports various means of certificate revocation checking, such as certificate revocation lists (CRLs) and the Online Certificate Status Protocol (OCSP). A CRL is a list of revoked certificates published by the CA that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate.

With CRLs, the list of revoked certificates is downloaded from a certificate distribution point (DP) that is often specified in the certificate. The View server periodically goes to the CRL DP URL specified in the certificate, downloads the list, and checks it to determine whether the server certificate has been revoked. With OCSP, the View server sends a request to an OCSP responder to determine the revocation status of the certificate.

When you obtain a server certificate from a third-party certificate authority (CA), the certificate includes one or more means by which its revocation status can be determined, including, for example, a CRL DP URL or the URL for an OCSP responder. If you have your own CA and generate a certificate but do not include revocation information in the certificate, the certificate revocation check fails. An example of revocation information for such a certificate could include, for example, a URL to a Web-based CRL DP on a server where you host a CRL.

If you have your own CA but do not or cannot include certificate revocation information in your certificate, you can choose not to check certificates for revocation or to check only certain certificates in a chain. On the View server, with the Windows Registry Editor, you can create the string (REG_SZ) value **CertificateRevocationCheckType**, under `HKLM\Software\VMware, Inc.\VMware VDM\Security`, and set this value to one of the following data values.

Value	Description
1	Do not perform certificate revocation checking.
2	Check only the server certificate. Do not check any other certificates in the chain.
3	Check all certificates in the chain.
4	(Default) Check all certificates except the root certificate.

If this registry value is not set, or if the value set is not valid (that is, if the value is not 1, 2, 3, or 4), all certificates are checked except the root certificate. Set this registry value on each View server on which you intend to modify revocation checking. You do not have to restart the system after you set this value.

NOTE If your organization uses proxy settings for Internet access, you might have to configure your View Connection Server computers to use the proxy settings to ensure that certificate revocation checking can be performed for security servers or View Connection Server instances that are used for secure View Client connections. If a View Connection Server instance cannot access the Internet, certificate revocation checking might fail, and the View Connection Server instance or paired security servers might show up as red on the View Administrator dashboard. To resolve this issue, see "Troubleshooting Security Server Certificate Revocation Checking" in the *VMware Horizon View Administration* document.

Configuring Certificate Checking in View Client for Windows

You can use a security-related group policy setting in the View Client Configuration ADM template file (`vdm_client.adm`) to configure SSL server certificate checking in the Windows-based View Client.

Certificate checking occurs for SSL connections between View Connection Server and View Client. Certificate verification includes all the following checks:

- Has the certificate been revoked? Is it possible to determine whether the certificate has been revoked?
- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects the View client to a server with a certificate that does not match the host name the user entered. A mismatch can also occur if the user enters an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA.

  To pass this check, the certificate's chain of trust must be rooted in the local certificate store of the device.

When you first set up a View environment, a default self-signed certificate is used. By default,**Warn But Allow**is the certificate verification mode. In this mode, when either of the following server certificate issues occurs, a warning is displayed, but the user can choose to continue on and ignore the warning:

- A self-signed certificate is provided by the View server. In this case, it is acceptable if the certificate name does not match the View Connection Server name provided by the user in View Client.
- A verifiable certificate that was configured in your deployment has expired or is not yet valid.

You can change the default certificate verification mode. You can set the mode to **No Security**, so that no certificate checking is done, or you can set the mode to **Full Security**, so that users are not allowed to connect to the server if any one of the checks fails. You can also allow end users to set the mode for themselves.

Use the `Certificate verification mode` group policy setting in the Client Configuration ADM template file to change the verification mode. When this group policy setting is configured, the setting is locked in View Client. Users can view the selected verification mode in View Client, but cannot configure the setting. When this group policy setting is not configured or disabled, View Client users can select a verification mode.

ADM template files for View components are installed in the *`install_directory`*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` directory on your View Connection Server host. For information about using these templates to control GPO settings, see the *VMware Horizon View Administration* document.

Configure the PCoIP Secure Gateway to Use a New SSL Certificate

To comply with industry or jurisdiction security regulations, you can replace the default SSL certificate that is generated by the PCoIP Secure Gateway (PSG) service with a certificate that is signed by a CA.

In View 5.2 or later releases, the PSG service creates a default, self-signed SSL certificate when the service starts up. The PSG service presents the self-signed certificate to clients running View Client 2.0 (or View Client 5.2 for Windows) or later releases that connect to the PSG.

The PSG also provides a default legacy SSL certificate that is presented to clients running View Client 1.7 (or View Client 5.1 for Windows) or earlier releases that connect to the PSG.

The default certificates provide secure connections from View Clients to the PSG and do not require further configuration in View Administrator. However, configuring the PSG service to use a CA-signed certificate is highly recommended, particularly for deployments that require you to use security scanners to pass compliance testing.

Although it is not required, you are most likely to configure new CA-signed SSL certificates for your View servers before you replace the default PSG certificate with a CA-signed certificate. The procedures that follow assume that you already imported a CA-signed certificate into the Windows certificate store for the View server on which the PSG is running.

NOTE If you are using a security scanner for compliance testing, you might want to start by setting the PSG to use the same certificate as the View server and scan the View port before the PSG port. You can resolve trust or validation issues that occur during the scan of the View port to ensure that these issues do not invalidate your test of the PSG port and certificate. Next, you can configure a unique certificate for the PSG and do another scan.

Procedure

1 Verify That the Server Name Matches the PSG Certificate Subject Name on page 82

When a View Connection Server instance or security server is installed, the installer creates a registry setting with a value that contains the FQDN of the computer. You must verify that this value matches the server name part of the URL that security scanners use to reach the PSG port. The server name also must match the subject name or a subject alternate name (SAN) of the SSL certificate that you intend to use for the PSG.

2 Configure a PSG Certificate in the Windows Certificate Store on page 83

To replace the default PSG certificate with a CA-signed certificate, you must configure the certificate and its private key in the Windows local computer certificate store on the View Connection Server or security server computer on which the PSG is running.

3 Set the PSG Certificate Friendly Name in the Windows Registry on page 84

The PSG identifies the SSL certificate to use by means of the server name and certificate Friendly name. You must set the Friendly name value in the Windows registry on the View Connection Server or security server computer on which the PSG is running.

4 (Optional) Force a CA-Signed Certificate to Be Used for Connections to the PSG on page 85

You can ensure that all View Client connections to the PSG use the CA-signed certificate for the PSG instead of the default legacy certificate. This procedure is not required to configure a CA-signed certificate for the PSG. Take these steps only if it makes sense to force the use of a CA-signed certificate in your View deployment.

Verify That the Server Name Matches the PSG Certificate Subject Name

When a View Connection Server instance or security server is installed, the installer creates a registry setting with a value that contains the FQDN of the computer. You must verify that this value matches the server name part of the URL that security scanners use to reach the PSG port. The server name also must match the subject name or a subject alternate name (SAN) of the SSL certificate that you intend to use for the PSG.

For example, if a scanner connects to the PSG with the URL `https://view.customer.com:4172`, the registry setting must have the value `view.customer.com`. Note that the FQDN of the View Connection Server or security server computer that is set during installation might not be the same as this external server name.

Procedure

1 Start the Windows Registry Editor on the View Connection Server or security server computer where the PCoIP Secure Gateway is running.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni` registry setting.

3 Verify that the value of the `SSLCertPsgSni` setting matches the server name in the URL that scanners will use to connect to the PSG and matches the subject name or a subject alternate name of the SSL certificate that you intend to install for the PSG.

   If the value does not match, replace it with the correct value.

4 Restart the VMware View PCoIP Secure Gateway service to make your changes take effect.

What to do next

Import the CA-signed certificate into the Windows local computer certificate store and configure the certificate Firendly name.

Configure a PSG Certificate in the Windows Certificate Store

To replace the default PSG certificate with a CA-signed certificate, you must configure the certificate and its private key in the Windows local computer certificate store on the View Connection Server or security server computer on which the PSG is running.

If you intend the PSG to use a unique certificate, you must import the certificate into the Windows local computer certificate store with an exportable private key and set the appropriate Friendly name.

If you intend the PSG to use the same certificate as the View server, you do not have to follow this procedure. However, in the Windows registry you must set the server name to match the View server certificate subject name and set the Friendly name to **vdm**.

Prerequisites

- Verify that the key length is at least 1024 bits.
- Verify that the SSL certificate is valid. The current time on the View server computer must be within the certificate start and end dates.
- Verify that the certificate subject name or a subject alternate name matches the `SSLCertPsgSni` setting in the Windows registry. See "Verify That the Server Name Matches the PSG Certificate Subject Name," on page 82.
- Verify that the Certificate snap-in was added to MMC. See "Add the Certificate Snap-In to MMC," on page 74.
- Familiarize yourself with importing a certificate into the Windows certificate store. See "Import a Signed Server Certificate into a Windows Certificate Store," on page 74.
- Familiarize yourself with modifying the certificate Friendly name. See "Modify the Certificate Friendly Name," on page 75.

Procedure

1 In the MMC window on the Windows Server host, open the **Certificates (Local Computer) > Personal** folder.

2 Import the SSL certificate that is issued to the PSG by selecting **More Actions > All Tasks > Import**.

   Select the following settings in the Certificate Import wizard:

   a **Mark this key as exportable**

   b **Include all extendable properties**

   Complete the wizard to finish importing the certificate into the **Personal** folder

3 Verify that the new certificate contains a private key by taking one of these steps:

- Verify that a yellow key appears on the certificate icon.
- Double-click the certificate and verify that the following statement appears in the Certificate Information dialog box: `You have a private key that corresponds to this certificate.`.

4 Right-click the new certificate and click **Properties**.

5 On the General tab, delete the **Friendly name** text and type the Friendly name that you have chosen.

Make sure that you enter exactly the same name in the `SSLCertWinCertFriendlyName` setting in the Windows registry, as described in the next procedure.

6 Click **Apply** and click **OK**.

The PSG presents the CA-signed certificate to View Client devices that connect to the View server over PCoIP.

NOTE This procedure does not affect legacy View Client devices. The PSG continues to present the default legacy certificate to legacy View Client devices that connect the this View server over PCoIP.

What to do next

Configure the certificate Friendly name in the Windows registry.

Set the PSG Certificate Friendly Name in the Windows Registry

The PSG identifies the SSL certificate to use by means of the server name and certificate Friendly name. You must set the Friendly name value in the Windows registry on the View Connection Server or security server computer on which the PSG is running.

The certificate Friendly name **vdm** is used by all View Connection Server instances and security servers. By contrast, you can configure your own certificate Friendly name for the PSG certificate. You must configure a Windows registry setting to enable the PSG to match the correct name with the Friendly name that you will set in the Windows certificate store.

The PSG can use the same SSL certificate as the View server on which the PSG is running. If you configure the PSG to use the same certificate as the View server, the Friendly name must be **vdm**.

The Friendly name value, in both the registry and the Windows certificate store, is case sensitive.

Prerequisites

- Verify that the Window registry contains the correct subject name that is used to reach the PSG port and that matches the PSG certificate subject name or subject alternate name. See "Verify That the Server Name Matches the PSG Certificate Subject Name," on page 82.
- Verify that the certificate Friendly name is configured in the Windows local computer certificate store. See "Configure a PSG Certificate in the Windows Certificate Store," on page 83.

Procedure

1 Start the Windows Registry Editor on the View Connection Server or security server computer where the PCoIP Secure Gateway is running.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.

3 Add a new String (REG_SZ) value, `SSLCertWinCertFriendlyName`, to this registry key.

4 Modify the `SSLCertWinCertFriendlyName` value and type the certificate Friendly name to be used by the PSG.

For example: **pcoip**

If you use the same certificate as the View server, the value must be **vdm**.

5 Restart the VMware View PCoIP Secure Gateway service to make your changes take effect.

What to do next

Verify that View Client devices continue to connect to the PSG.

If you are using a security scanner for compliance testing, scan the PSG port.

(Optional) Force a CA-Signed Certificate to Be Used for Connections to the PSG

You can ensure that all View Client connections to the PSG use the CA-signed certificate for the PSG instead of the default legacy certificate. This procedure is not required to configure a CA-signed certificate for the PSG. Take these steps only if it makes sense to force the use of a CA-signed certificate in your View deployment.

In some cases, the PSG might present the default legacy certificate instead of the CA-signed certificate to a security scanner, invalidating the compliance test on the PSG port. To resolve this issue, you can configure the PSG not to present the default legacy certificate to any device that attempts to connect.

IMPORTANT Performing this procedure prevents all legacy clients from connecting to this View server over PCoIP.

Prerequisites

Verify that all client devices that connect to this View server, including thin clients, run View Client 5.2 for Windows or View Client 2.0 or later releases. You must upgrade the legacy clients.

Procedure

1 Start the Windows Registry Editor on the View Connection Server or security server computer where the PCoIP Secure Gateway is running.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.

3 Add a new String (REG_SZ) value, `SSLCertPresentLegacyCertificate`, to this registry key.

4 Set the `SSLCertPresentLegacyCertificate` value to **0**.

5 Restart the VMware View PCoIP Secure Gateway service to make your changes take effect.

View Transfer Server and SSL Certificates

You do not have to configure SSL certificates for View Transfer Server if you are installing View 5.1 or later.

A default, self-signed certificate is installed with View Transfer Server that View Connection Server uses to handle secondary connections to View clients.

When you add View Transfer Server to View, View Connection Server establishes a trust relationship with View Transfer Server. Communications between View Connection Server and View Transfer Server use Java Message Service (JMS). Messages containing sensitive data are encrypted.

When a View client requests a data transfer operation, which requires connecting to View Transfer Server, View Connection Server sends the thumbprint of the View Transfer Server certificate to the client. When the client connects to the Apache server that is associated with View Transfer Server, View Client verifies that the thumbprint passed from View Connection Server matches the certificate thumbprint on the Apache server.

Replacing the default certificate for View Transfer Server with a certificate that is signed by a CA would not significantly affect the secure communications between View Transfer Server, View Connection Server, and View clients.

In View 5.0.*x* and earlier versions, you did have to configure an SSL certificate for View Transfer Server.

If you are upgrading from View 5.0.*x* or earlier to View 5.1 or later, and you want to continue to use a certificate that is signed by a CA on the upgraded version of View Transfer Server, you must back up the certificate, upgrade View Transfer Server, and configure the signed certificate for the new View Transfer Server version.

If you configured a self-signed certificate for the old View Transfer Server, or you do not intend to use an existing CA-signed certificate on the upgraded server, you do not have to configure a certificate again. During the upgrade, a valid, self-signed certificate is installed with View Transfer Server.

For more information, see the *VMware Horizon View Upgrades* document.

Setting View Administrator to Trust a vCenter Server or View Composer Certificate

In the View Administrator dashboard, you can configure View to trust a vCenter Server or View Composer certificate that is untrusted.

VMware strongly recommends that you configure vCenter Server and View Composer to use SSL certificates that are signed by a CA. Alternatively, you can accept the thumbprint of the default certificate for vCenter Server or View Composer.

Similarly, VMware recommends that you configure SAML 2.0 authenticators to use SSL certificates that are signed by a CA. Alternatively, in the View Administrator dashboard you can configure View to trust an untrusted SAML 2.0 server certificate by accepting the thumbprint of the default certificate.

Benefits of Using SSL Certificates Signed by a CA

A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration.

You can request an SSL server certificate that is specific to a Web domain such as `www.mycorp.com`, or you can request a wildcard SSL server certificate that can be used throughout a domain such as `*.mycorp.com`. To simplify administration, you might choose to request a wildcard certificate if you need to install the certificate on multiple servers or in different subdomains. Typically, domain-specific certificates are used in secure installations, and CAs usually guarantee more protection against losses for domain-specific certificates than for wildcard certificates. If you use a wildcard certificate, you must ensure that the private key is transferrable between servers.

When you replace the default certificate with your own certificate, clients use your certificate to authenticate the server. If your certificate is signed by a CA, the certificate for the CA itself is typically embedded in the browser or is located in a trusted database that the client can access. After a client accepts the certificate, it responds by sending a secret key, which is encrypted with the public key contained in the certificate. The secret key is used to encrypt traffic between the client and the server.

Configuring View for the First Time

8

After you install the View server software and configure SSL certificates for the servers, you must take a few additional steps to set up a working View environment.

You configure user accounts for vCenter Server and View Composer, install a View license key, add vCenter Server and View Composer to your View environment, configure the PCoIP Secure Gateway and secure tunnel, and, optionally, size Windows Server settings to support your View environment.

This chapter includes the following topics:

Configuring User Accounts for vCenter Server and View Composer

To use vCenter Server with View Manager, you must configure a user account with permission to perform operations in vCenter Server. To use View Composer, you must give this vCenter Server user additional privileges. To manage desktops that are used in local mode, you must give this user privileges in addition to those that are required for View Manager and View Composer.

You also must create a domain user for View Composer in Active Directory. See "Create a User Account for View Composer," on page 21.

Where to Use the vCenter Server User and Domain User for View Composer

After you create and configure these two user accounts, you specify the user names in View Administrator.

- You specify a vCenter Server user when you add vCenter Server to View Manager.
- You specify a domain user for View Composer when you configure View Composer for vCenter Server.
- You specify the domain user for View Composer when you create linked-clone pools.

Configure a vCenter Server User for View Manager, View Composer, and Local Mode

To configure a user account that gives View Manager permission to operate in vCenter Server, you must assign a role with appropriate privileges to that user. To use the View Composer service in vCenter Server, you must give the user account additional privileges. To manage desktops that are used in local mode, you must give the user account privileges that include View Manager, View Composer, and local mode privileges.

To support View Composer, you also must make this user a local system administrator on the vCenter Server computer.

Prerequisites

- In Active Directory, create a user in the View Connection Server domain or a trusted domain. See "Creating a User Account for vCenter Server," on page 20.
- Familiarize yourself with the privileges that are required for the user account. See "View Manager Privileges Required for the vCenter Server User," on page 89.
- If you use View Composer, familiarize yourself with the additional required privileges. See "View Composer Privileges Required for the vCenter Server User," on page 90.
- If you manage local desktops, familiarize yourself with the additional required privileges. See "Local Mode Privileges Required for the vCenter Server User," on page 90.

Procedure

1 In vCenter Server, prepare a role with the required privileges for the user.

   - You can use the predefined Administrator role in vCenter Server. This role can perform all operations in vCenter Server.
   - If you use View Composer, you can create a limited role with the minimum privileges needed by View Manager and View Composer to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`View Composer Administrator`**, and select privileges for the role.

     This role must have all the privileges that both View Manager and View Composer need to operate in vCenter Server.
   - If you manage local desktops, you can create a limited role with the minimum privileges needed by View Manager, View Composer, and the local mode feature to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`Local Mode Administrator`**, and select privileges for the role.

     This role must have all the privileges that View Manager, View Composer, and the local mode feature need to operate in vCenter Server.
   - If you use View Manager without View Composer and do not manage local desktops, you can create an even more limited role with the minimum privileges needed by View Manager to perform vCenter Server operations.

     In vSphere Client, click **Home > Roles > Add Role**, enter a role name such as **`View Manager Administrator`**, and select privileges for the role.

2 In vSphere Client, right-click the vCenter Server at the top level of the inventory, click **Add Permission**, and add the vCenter Server user.

   NOTE You must define the vCenter Server user at the vCenter Server level.

3 From the drop-down menu, select the Administrator role, or the View Composer or View Manager role that you created, and assign it to the vCenter Server user.

4 If you use View Composer, on the vCenter Server computer, add the vCenter Server user account as a member of the local system Administrators group.

View Composer requires that the vCenter Server user is a system administrator on the vCenter Server computer.

What to do next

In View Administrator, when you add vCenter Server to View Manager, specify the vCenter Server user. See "Add vCenter Server Instances to View Manager," on page 93.

View Manager Privileges Required for the vCenter Server User

The vCenter Server user must have sufficient privileges to enable View Manager to operate in vCenter Server. Create a View Manager role for the vCenter Server user with the required privileges.

Table 8-1. View Manager Privileges

Privilege Group	Privileges to Enable
Folder	**Create Folder** **Delete Folder**
Virtual Machine	In **Configuration**: ■ **Add or remove device** ■ **Advanced** ■ **Modify device settings** In **Interaction**: ■ **Power Off** ■ **Power On** ■ **Reset** ■ **Suspend** In **Inventory**: ■ **Create new** ■ **Remove** In **Provisioning**: ■ **Customize** ■ **Deploy template** ■ **Read customization specifications**
Resource	**Assign virtual machine to resource pool**
Global	**Act as vCenter Server**
	The following **Host** privilege is required to implement View Storage Accelerator, which enables ESXi host caching. If you do not use View Storage Accelerator, the vCenter Server user does not need this privilege.
Host	In **Configuration**: ■ **Advanced settings**

View Composer Privileges Required for the vCenter Server User

To support View Composer, the vCenter Server user must have privileges in addition to those required to support View Manager. Create a View Composer role for the vCenter Server user with the View Manager privileges and these additional privileges.

Table 8-2. View Composer Privileges

Privilege Group	Privileges to Enable
Datastore	**Allocate space** **Browse datastore** **Low level file operations**
Virtual machine	**Inventory** (all) **Configuration** (all) **State** (all) In **Provisioning**: ■ **Clone virtual machine** ■ **Allow disk access**
Resource	**Assign virtual machine to resource pool** The following privilege is required to perform View Composer rebalance operations. **Migrate powered off virtual machine**
Global	**Enable methods** **Disable methods** **System tag** The following privilege is required to implement View Storage Accelerator, which enables ESXi host caching. If you do not use View Storage Accelerator, the vCenter Server user does not need this privilege. **Act as vCenter Server**
Network	(all)

Local Mode Privileges Required for the vCenter Server User

To manage desktops that are used in local mode, the vCenter Server user must have privileges in addition to those required to support View Manager and View Composer. Create a Local Mode Administrator role for the vCenter Server user that combines the View Manager privileges, View Composer privileges, and local mode privileges.

Table 8-3. Local Mode Privileges

Privilege Group	Privileges to Enable
Global	**Manage custom attributes** **Set custom attribute**
Host	In **Configuration**: **System management**

Configuring View Connection Server for the First Time

After you install View Connection Server, you must install a product license, add vCenter Servers and View Composer services to View Manager. You can also allow ESXi hosts to reclaim disk space on linked-clone virtual machines and configure ESXi hosts to cache virtual machine disk data.

If you install security servers, they are added to View Manager and appear in View Administrator automatically.

View Administrator and View Connection Server

View Administrator provides a management interface for View Manager.

Depending on your View deployment, you use one or more View Administrator interfaces.

- Use one View Administrator interface to manage the View components that are associated with a single, standalone View Connection Server instance or a group of replicated View Connection Server instances.

  You can use the IP address of any replicated instance to log in to View Administrator.

- You must use a separate View Administrator interface to manage the View components for each single, standalone View Connection Server instance and each group of replicated View Connection Server instances.

You also use View Administrator to manage security servers and View Transfer Server instances associated with View Connection Server.

- Each security server is associated with one View Connection Server instance.
- Each View Transfer Server instance can communicate with any View Connection Server instance in a group of replicated instances.

Log In to View Administrator

To perform initial configuration tasks, you must log in to View Administrator.

Prerequisites

Verify that you are using a Web browser supported by View Administrator. See "View Administrator Requirements," on page 9.

Procedure

1 Open your Web browser and enter the following URL, where *server* is the host name of the View Connection Server instance.

```
https://server/admin
```

NOTE You can use the IP address if you have to access a View Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance, resulting in blocked access or access with reduced security.

Your access to View Administrator depends on the type of certificate that is configured on the View Connection Server computer.

Option	Description
You configured a certificate signed by a CA for View Connection Server.	When you first connect, your Web browser displays View Administrator.
The default, self-signed certificate supplied with View Connection Server is configured.	When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click **Ignore** to continue using the current SSL certificate.

2 Log in as a user with credentials to access the View Administrators account.

You specify the View Administrators account when you install a standalone View Connection Server instance or the first View Connection Server instance in a replicated group. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the View Administrators role.

Install the View Connection Server License Key

Before you can use View Connection Server, you must enter the product license key.

The first time you log in, View Administrator displays the Product Licensing and Usage page.

After you install the license key, View Administrator displays the dashboard page when you log in.

You do not have to configure a license key when you install a replicated View Connection Server instance or a security server. Replicated instances and security servers use the common license key stored in the View LDAP configuration.

NOTE View Connection Server requires a valid license key for View 5.0. As of the release of View 4.0, the View license key is a 25-character key.

Procedure

1 If the View Configuration view is not displayed, click **View Configuration** in the left navigation pane.

2 Click **Product Licensing and Usage**.

3 On the Product Licensing table, click **Edit License** and enter the View Manager license serial number.

4 Click **OK**.

5 Verify the license expiration date.

Add vCenter Server Instances to View Manager

You must configure View Manager to connect to the vCenter Server instances in your View deployment. vCenter Server creates and manages the virtual machines that View Manager uses as desktop sources.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to View Manager separately.

View Manager connects to the vCenter Server instance using a secure channel (SSL).

Prerequisites

- Install the View Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support View Manager. To use View Composer, you must give the user additional privileges. To manage desktops that are used in local mode, you must give the user privileges in addition to those that are required for View Manager and View Composer.

  See "Configure a vCenter Server User for View Manager, View Composer, and Local Mode," on page 88.
- Verify that an SSL server certificate is installed on the vCenter Server host. In a production environment, install a valid SSL certificate that is signed by a trusted Certificate Authority (CA).

  In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to View.
- Verify that all View Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the **Trusted Root Certification Authorities > Certificates** folder in the Windows local computer certificate stores on the View Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

  See "Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store" in the *VMware Horizon View Installation* document.
- Verify that the vCenter Server instance contains ESXi hosts. If no hosts are configured in the vCenter Server instance, you cannot add the instance to View.
- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server and View Composer. See "Concurrent Operations Limits for vCenter Server and View Composer," on page 98 and "Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms," on page 99.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 In the vCenter Servers tab, click **Add**.

3 In the vCenter Server Settings server address text box, type the fully qualified domain name (FQDN) of the vCenter Server instance.

  The FQDN includes the host name and domain name. For example, in the FQDN ***myserverhost.companydomain.com***, ***myserverhost*** is the host name and ***companydomain.com*** is the domain.

  NOTE If you enter a server by using a DNS name or URL, View Manager does not perform a DNS lookup to verify whether an administrator previously added this server to View Manager by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4 Type the name of the vCenter Server user.

For example: **`domain\user`** or **`user@domain.com`**

5 Type the vCenter Server user password.

6 (Optional) Type a description for this vCenter Server instance.

7 Type the TCP port number.

The default port is 443.

8 Under Advanced Settings, set the concurrent operations limits for vCenter Server and View Composer operations.

9 Click **Next** to display the View Composer Settings page.

What to do next

Configure View Composer settings.

- If the vCenter Server instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Settings page.
- If the vCenter Server instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See "Accept the Thumbprint of a Default SSL Certificate," on page 100.

If View Manager uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Configure View Composer Settings

To use View Composer, you must configure settings that allow View Manager to connect to the View Composer service. View Composer can be installed on its own separate host or on the same host as vCenter Server.

There must be a one-to-one mapping between each View Composer service and vCenter Server instance. A View Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one View Composer service.

Prerequisites

- Your Active Directory administrator must create a domain user with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. To manage the linked-clone machine accounts in Active Directory, the domain user must have **Create Computer Objects**, **Delete Computer Objects**, and **Write All Properties** permissions.

  See "Create a User Account for View Composer," on page 21.
- Verify that you configured View Manager to connect to vCenter Server. To do so, you must complete the vCenter Server Information page in the Add vCenter Server wizard. See "Add vCenter Server Instances to View Manager," on page 93.
- Verify that this View Composer service is not already configured to connect to a different vCenter Server instance.

Procedure

1 In View Administrator, complete the vCenter Server Information page in the Add vCenter Server wizard.

   a Click **View Configuration > Servers**.

   b In the vCenter Servers tab, click **Add** and provide the vCenter Server settings.

2 On the View Composer Settings page, if you are not using View Composer, select **Do not use View Composer**.

If you select **Do not use View Composer**, the other View Composer settings become inactive. When you click **Next**, the Add vCenter Server wizard displays the Storage Settings page. The View Composer Domains page is not displayed.

3 If you are using View Composer, select the location of the View Composer host.

Option	Description
View Composer is installed on the same host as vCenter Server.	a Select **View Composer co-installed with the vCenter Server**. b Make sure that the port number is the same as the port that you specified when you installed the View Composer service on vCenter Server. The default port number is 18443.
View Composer is installed on its own separate host.	a Select **Standalone View Composer Server**. b In the View Composer server address text box, type the fully qualified domain name (FQDN) of the View Composer host. c Type the name of the View Composer user. For example: **`domain.com\user`** or **`user@domain.com`** d Type the password of the View Composer user. e Make sure that the port number is the same as the port that you specified when you installed the View Composer service. The default port number is 18443.

4 Click **Next** to display the View Composer Domains page.

What to do next

Configure View Composer domains.

- If the View Composer instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Domains page.
- If the View Composer instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See "Accept the Thumbprint of a Default SSL Certificate," on page 100.

Configure View Composer Domains

You must configure an Active Directory domain in which View Composer deploys linked-clone desktops. You can configure multiple domains for View Composer. After you first add vCenter Server and View Composer settings to View, you can add more View Composer domains by editing the vCenter Server instance in View Administrator.

Prerequisites

In View Administrator, verify that you completed the vCenter Server Information and View Composer Settings pages in the Add vCenter Server wizard.

Procedure

1 On the View Composer Domains page, click **Add** to add the domain user for View Composer account information.

2 Type the domain name of the Active Directory domain.

For example: **`domain.com`**

3 Type the domain user name, including the domain name.

For example: **`domain.com\admin`**

4 Type the account password.

5 Click **OK**.

6 To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.

7 Click **Next** to display the Storage Settings page.

What to do next

Enable virtual machine disk space reclamation and configure View Storage Accelerator for View.

Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines

In vSphere 5.1 and later, you can enable the disk space reclamation feature for View. Starting in vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones, reducing the total storage space required for linked clones.

As users interact with linked-clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with their desktops.

Disk space reclamation is especially useful for deployments that cannot take advantage of storage-saving strategies such as refresh on logoff. For example, knowledge workers who install user applications on dedicated desktops might lose their personal applications if the desktops were refreshed or recomposed. With disk space reclamation, View can maintain linked clones at close to the reduced size they start out with when they are first provisioned.

This feature has two components: space-efficient disk format and space reclamation operations.

In a vSphere 5.1 or later environment, when a parent virtual machine is virtual hardware version 9 or later, View creates linked clones with space-efficient OS disks, whether or not space reclamation operations are enabled.

To enable space reclamation operations, you must use View Administrator to enable space reclamation for vCenter Server and reclaim VM disk space for individual desktop pools. The space reclamation setting for vCenter Server gives you the option to disable this feature on all desktop pools that are managed by the vCenter Server instance. Disabling the feature for vCenter Server overrides the setting at the desktop pool level.

The following guidelines apply to the space reclamation feature:

- It operates only on space-efficient OS disks in linked clones.
- It does not affect View Composer persistent disks.
- It works only with vSphere 5.1 or later and only on desktops that are virtual hardware version 9 or later.
- It does not operate on full-clone desktops.
- It operates on virtual machines with SCSI controllers. IDE controllers are not supported.
- It operates on Windows XP and Windows 7 desktops only. It does not operate on Windows 8 desktops.

View Composer Array Integration is not supported in pools that contain virtual machines with space-efficient disks. View Composer Array Integration uses vStorage APIs for Array Integration (VAAI) native NFS snapshot technology to clone virtual machines.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.

  In an ESXi cluster, verify that all the hosts are version 5.1 with download patch ESXi510-201212001 or later.

Procedure

1 In View Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.

   a Select **View Configuration > Servers**.

   b In the vCenter Servers tab, click **Add**.

   c Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.

2 On the Storage Settings page, make sure that **Enable space reclamation** is selected.

   Space reclamation is selected by default if you are performing a fresh installation of View 5.2 or later. You must select **Enable space reclamation** if you are upgrading to View 5.2 or later from View 5.1 or an earlier release.

What to do next

On the Storage Settings page, configure View Storage Accelerator.

To finish configuring disk space reclamation in View, set up space reclamation for desktop pools.

Configure View Storage Accelerator for vCenter Server

In vSphere 5.0 and later, you can configure ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator improves View performance during I/O storms, which can take place when many desktops start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. Instead of reading the entire OS or application from the storage system over and over, a host can read common data blocks from cache.

By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your View deployment.

You enable caching on your ESXi hosts by selecting the View Storage Accelerator setting in the vCenter Server wizard in View Administrator, as described in this procedure.

Make sure that View Storage Accelerator is also configured for individual desktop pools. View Storage Accelerator is enabled for pools by default, but this feature can be disabled or enabled when you create or edit a pool. To operate on a pool, View Storage Accelerator must be enabled for vCenter Server and for the individual pool.

You can enable View Storage Accelerator on pools that contain linked clones and pools that contain full virtual machines.

View Storage Accelerator is also supported with local mode. Users can check out desktops in pools that are enabled for View Storage Accelerator. View Storage Accelerator is disabled while a desktop is checked out and reenabled after the desktop is checked in.

View Composer Array Integration is not supported in pools that are enabled for View Storage Accelerator. View Composer Array Integration uses vStorage APIs for Array Integration (VAAI) native NFS snapshot technology to clone virtual machines.

View Storage Accelerator is now qualified to work in configurations that use View replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using View Storage Accelerator with View replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. Hence, this combination is tested and supported.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.

  In an ESXi cluster, verify that all the hosts are version 5.0 or later.

- Verify that the vCenter Server user was assigned the **Global > Act as vCenter Server** privilege in vCenter Server. See the topics in the *VMware Horizon View Installation* documentation that describe View Manager and View Composer privileges required for the vCenter Server user.

Procedure

1 In View Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.

   a Select **View Configuration > Servers**.

   b In the vCenter Servers tab, click **Add**.

   c Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.

2 On the Storage Settings page, make sure that the **Enable View Storage Accelerator** check box is selected.

   This check box is selected by default.

3 Specify a default host cache size.

   The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.

   The default value is 1,024MB. The cache size must be between 100MB and 2,048MB.

4 To specify a different cache size for an individual ESXi host, select an ESXi host and click **Edit cache size**.

   a In the Host cache dialog box, check **Override default host cache size**.

   b Type a **Host cache size** value between 100MB and 2,048MB and click **OK**.

5 On the Storage Settings page, click **Next**.

6 Click **Finish** to add vCenter Server, View Composer, and Storage Settings to View.

What to do next

To configure the PCoIP Secure Gateway, secure tunnel, and external URLs for client connections, see "Configuring View Client Connections," on page 101.

To complete View Storage Accelerator settings in View, configure View Storage Accelerator for desktop pools. See "Configure View Storage Accelerator for Desktop Pools" in the *VMware Horizon View Administration* document.

Concurrent Operations Limits for vCenter Server and View Composer

When you add vCenter Server to View or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server and View Composer.

You configure these options in the Advanced Settings panel on the vCenter Server Information page.

Table 8-4. Concurrent Operations Limits for vCenter Server and View Composer

Setting	Description
Max concurrent vCenter provisioning operations	Determines the maximum number of concurrent requests that View Manager can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to full virtual machines only.
Max concurrent power operations	Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by View Manager in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see "Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms," on page 99. This setting applies to full virtual machines and linked clones.
Max concurrent View Composer maintenance operations	Determines the maximum number of concurrent View Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this View Composer instance. The default value is 12. Desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on desktops that require logoffs is 12. This setting applies to linked clones only.
Max concurrent View Composer provisioning operations	Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this View Composer instance. The default value is 8. This setting applies to linked clones only.

Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on View desktop virtual machines in a vCenter Server instance. Starting in View 5.0, this limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see "Architecture Design Elements and Planning Guidelines" in the *VMware Horizon View Architecture Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.

View waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to Horizon 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 Chapter 7, "Configuring SSL Certificates for View Servers," on page 69.

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 to Horizon View 5.1 or later, 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 2.0 authenticator for use by a View Connection Server instance. If the SAML 2.0 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 2.0 authenticator in Horizon View. After a SAML 2.0 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 2.0 authenticator. If appropriate, take the preceding steps on the SAML 2.0 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 2.0 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.

Configuring View Client Connections

View clients communicate with a View Connection Server or security server host over secure connections.

The initial View Client connection, which is used for user authentication and View desktop selection, is created over HTTPS when a user provides a domain name to View Client. If firewall and load balancing software are configured correctly in your network environment, this request reaches the View Connection Server or security server host. With this connection, users are authenticated and a desktop is selected, but users have not yet connected to View desktops.

When users connect to View desktops, by default View Client makes a second connection to the View Connection Server or security server host. This connection is called the tunnel connection because it provides a secure tunnel for carrying RDP and other data over HTTPS.

When users connect to View desktops with the PCoIP display protocol, View Client can make a further connection to the PCoIP Secure Gateway on the View Connection Server or security server host. The PCoIP Secure Gateway ensures that only authenticated users can communicate with View desktops over PCoIP.

When the secure tunnel or PCoIP Secure Gateway is disabled, View desktop sessions are established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This type of connection is called a direct connection.

Desktop sessions that use direct connections remain connected even if View Connection Server is no longer running.

Typically, to provide secure connections for external clients that connect to a security server or View Connection Server host over a WAN, you enable both the secure tunnel and the PCoIP Secure Gateway. You can disable the secure tunnel and the PCoIP Secure Gateway to allow internal, LAN-connected clients to establish direct connections to View desktops.

Certain View Client endpoints, such as thin clients, do not support the tunnel connection and use direct connections for RDP data, but do support the PCoIP Secure Gateway for PCoIP data.

You can also provide secure connections to external users who use HTML Access to connect to View desktops. The Blast Secure Gateway, enabled by default on View Connection Server and security server hosts, ensures that only authenticated users can communicate with View desktops. With HTML Access, View Client software does not have to be installed on the users' endpoint devices.

SSL is required for all client connections to View Connection Server and security server hosts.

Configure the PCoIP Secure Gateway and Secure Tunnel Connections

You use View Administrator to configure the use of the secure tunnel and PCoIP Secure Gateway. These components ensure that only authenticated users can communicate with View desktops.

Clients that use the PCoIP display protocol can use the PCoIP Secure Gateway. Clients that use the RDP display protocol can use the secure tunnel.

IMPORTANT A typical network configuration that provides secure connections for external clients includes a security server. To enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a View Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that View Connection Server instance in View Administrator.

Prerequisites

- If you intend to enable the PCoIP Secure Gateway, verify that the View Connection Server instance and paired security server are View 4.6 or later.
- If you pair a security server to a View Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is View 4.6 or later.

Procedure

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

2 In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.

3 Configure use of the secure tunnel.

Option	Description
Disable the secure tunnel	Deselect **Use secure tunnel connection to desktop**.
Enable the secure tunnel	Select **Use secure tunnel connection to desktop**.

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

Option	Description
Enable the PCoIP Secure Gateway	Select **Use PCoIP Secure Gateway for PCoIP connections to desktop**
Disable the PCoIP secure Gateway	Deselect **Use PCoIP Secure Gateway for PCoIP connections to desktop**

The PCoIP Secure Gateway is disabled by default.

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

Configure Secure HTML Access

In View Administrator, you can configure the use of the Blast Secure Gateway to provide secure HTML access to View desktops.

The Blast Secure Gateway ensures that only authenticated users can communicate with View desktops by using HTML Access. View Client does not have to be installed on users' endpoint devices.

When the Blast Secure Gateway is not enabled, client Web browsers use HTML Access to establish direct connections to View desktop virtual machines, bypassing the Blast Secure Gateway.

IMPORTANT A typical network configuration that provides secure connections for external users includes a security server. To enable or disable the Blast Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server. If external users connect directly to a View Connection Server host, you enable or disable the Blast Secure Gateway by editing that View Connection Server instance.

Prerequisites

- If users select View desktops by using the Horizon User Portal, verify that Horizon Workspace is installed and configured for use with View Connection Server and that View Connection Server is paired with a SAML 2.0 Authentication server.
- Verify that the secure tunnel is enabled. If the secure tunnel is disabled, the Blast Secure Gateway cannot be enabled.

Procedure

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

2 In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.

3 Configure use of the Blast Secure Gateway.

Option	Description
Enable the Blast Secure Gateway	Select **Use Blast Secure Gateway for HTML access to desktop**
Disable the Blast secure Gateway	Deselect **Use Blast Secure Gateway for HTML access to desktop**

The Blast Secure Gateway is enabled by default.

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

Open the Port Used by HTML Access on Security Servers

When you install View Connection Server or security server, the View server installer creates the Windows Firewall rule for the port that is used by HTML Access for client connections, but the installer leaves the rule disabled until it is actually needed. When you later install HTML Access on a View Connection Server instance, the HTML Access installer automatically enables the rule to allow communication to that port. However, on security servers, you must manually enable the rule in the Windows Firewall to allow communication to the port.

By default, HTML Access uses TCP port 8443 for client connections to the Blast Secure Gateway.

Procedure

- To open the port used by HTML Access on a View Connection Server computer, install HTML Access on that computer.

  The HTML Access installer enables the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

- To open the port for HTML Access on a security server, manually enable the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

Configuring External URLs for Secure Gateway and Tunnel Connections

To use the secure tunnel, a client system must have access to an IP address, or a fully qualified domain name (FQDN) that it can resolve to an IP address, that allows the client to reach a View Connection Server or security server host.

To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach a View Connection Server or security server host.

To use the Blast Secure Gateway, a user's endpoint device must have access to an FQDN that it can resolve to an IP address that allows the user's Web browser to reach a View Connection Server or security server host.

Using Tunnel Connections From External Locations

By default, a View Connection Server or security server host can be contacted only by tunnel clients that reside within the same network and are therefore able to locate the requested host.

Many organizations require that users can connect from an external location by using a specific IP address or client-resolvable domain name, and a specific port. This information might or might not resemble the actual address and port number of the View Connection Server or security server host. The information is provided to a client system in the form of a URL. For example:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

To use addresses like these in View Manager, you must configure the View Connection Server or security server host to return an external URL instead of the host's FQDN.

Configuring External URLs

You configure more than one external URL. The first URL allows client systems to make tunnel connections. A second URL allows client systems that use PCoIP to make secure connections through the PCoIP Secure Gateway. You must specify the PCoIP external URL as an IP address, which allows client systems to connect from an external location.

A third URL allows users to make secure connections from their Web browsers through the Blast Secure Gateway.

If your network configuration includes security servers, provide external URLs for the security servers. External URLs are not required on the View Connection Server instances that are paired with the security servers.

The process of configuring the external URLs is different for View Connection Server instances and security servers.

- For a View Connection Server instance, you set the external URLs by editing View Connection Server settings in View Administrator.
- For a security server, you set the external URLs when you run the View Connection Server installation program. You can use View Administrator to modify an external URL for a security server.

Set the External URLs for a View Connection Server Instance

You use View Administrator to configure the external URLs for a View Connection Server instance.

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this View Connection Server instance. For example, do not specify the secure tunnel external URL for this instance and the PCoIP external URL for a paired security server.

Similarly, the secure tunnel external URL and Blast external URL must be the addresses that HTML connections use to reach this View Connection Server instance. For example, do not specify the secure tunnel external URL for this instance and the Blast external URL for a paired security server.

Prerequisites

- Verify that the secure tunnel connections and the PCoIP Secure Gateway are enabled on the View Connection Server instance. See "Configure the PCoIP Secure Gateway and Secure Tunnel Connections," on page 102.
- To set the Blast external URL, verify that the Blast Secure Gateway is enabled on the View Connection Server instance. See "Configure Secure HTML Access," on page 103.

Procedure

1 In View Administrator, click **View Configuration > Servers**.

2 Select the Connection Servers tab, select a View Connection Server instance, and click **Edit**.

3 Type the secure tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable host name and port number.

For example: `https://myserver.example.com:443`

NOTE You can use the IP address if you have to access a View Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance, resulting in blocked access or access with reduced security.

---

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP External URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this View Connection Server host. You can type into the text box only if a PCoIP Secure Gateway is installed on the View Connection Server instance.

5 Type the Blast Secure Gateway external URL in the **Blast External URL** text box.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

For example: `https://myserver.example.com:8443`

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this View Connection Server host. You can type into the text box only if a Blast Secure Gateway is installed on the View Connection Server instance.

6 Click **OK**.

Modify the External URLs for a Security Server

You use View Administrator to modify the external URLs for a security server.

You initially configure these external URLs when you install a security server in the View Connection Server installation program.

The secure tunnel external URL, PCoIP external URL, and Blast external URL must be the addresses that client systems use to reach this security server. For example, do not specify the secure tunnel external URL for this security server and the PCoIP external URL for a paired View Connection Server instance.

Prerequisites

- For secure access to View desktops over PCoIP, verify that the security server version is View 4.6 or later.
- For secure HTML access to View desktops, verify that the security server version is View 5.2 or later.
- Verify that the secure tunnel connections and the PCoIP Secure Gateway are enabled on the View Connection Server instance that is paired with this security server. See "Configure the PCoIP Secure Gateway and Secure Tunnel Connections," on page 102.
- To set the Blast external URL, verify that the Blast Secure Gateway is enabled on the View Connection Server instance that is paired with this security server. See "Configure Secure HTML Access," on page 103.

Procedure

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

2 Select the Security Servers tab, select the security server, and click **Edit**.

The **Edit** button is unavailable if the security server is not upgraded to View Connection Server 4.6 or later.

3 Type the Secure Tunnel external URL in the **External URL** text box.

The URL must contain the protocol, client-resolvable security server host name and port number.

For example: `https://view.example.com:443`

NOTE You can use the IP address if you have to access a security server when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the security server, resulting in blocked access or access with reduced security.

---

4 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

Specify the PCoIP external URL as an IP address with the port number 4172. Do not include a protocol name.

For example: `10.20.30.40:4172`

The URL must contain the IP address and port number that a client system can use to reach this security server. You can type into the text box only if a PCoIP Secure Gateway is installed on the security server.

5 Type the Blast Secure Gateway external URL in the **Blast External URL** text box.

The URL must contain the HTTPS protocol, client-resolvable host name, and port number.

For example: `https://myserver.example.com:8443`

By default, the URL includes the FQDN of the secure tunnel external URL and the default port number, 8443. The URL must contain the FQDN and port number that a client system can use to reach this security server. You can type into the text box only if a Blast Secure Gateway is installed on the security server.

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

View Administrator sends the updated external URLs to the security server. You do not need to restart the security server service for the changes to take effect.

Replacing Default Ports for View Services

During installation, View services are set up to listen on certain network ports by default. In certain organizations, these ports must be changed to comply with organization policies or to avoid contention. You can change the default ports that are used by View Connection Server, security server, PCoIP Secure Gateway, View Composer, and View Transfer Server services.

Changing ports is an optional setup task. Use the default ports if your deployment does not require you to change them.

For a list of the default TCP and UDP ports that are used by View servers, see "View TCP and UDP Ports" in the *VMware Horizon View Security* document.

Replace the Default HTTP Ports or NICs for View Connection Server Instances and Security Servers

You can replace the default HTTP ports or NICs for a View Connection Server instance or security server by editing the `locked.properties` file on the View server computer. Your organization might require you to perform these tasks to comply with organization policies or to avoid contention.

The default SSL port is 443. The default non-SSL port is 80.

The port that is specified in the secure tunnel External URL does not change as a result of changes that you make to ports in this procedure. Depending on your network configuration, you might have to change the secure tunnel External URL port as well.

If the View server computer has multiple NICs, the computer listens on all NICs by default. You can select one NIC to listen on the configured port by specifying the IP address that is bound to that NIC.

During installation, View configures the Windows firewall to open the required default ports. If you change a port number or the NIC on which it listens, you must manually reconfigure your Windows firewall to open the updated ports so that View Client devices can connect to the View server.

Prerequisites

Verify that the port that is specified in the External URL for this View Connection Server instance or security server will continue to be valid after you change ports in this procedure.

Procedure

1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server computer.

   For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

   The properties in the `locked.properties` file are case sensitive.

2 Add the `serverPort` or `serverPortNonSsl` property, or both properties, to the `locked.properties` file.

   For example:

```
serverPort=4443
serverPortNonSsl=8080
```

3 (Optional) If the View server computer has multiple NICs, select one NIC to listen on the configured ports.

Add the `serverHost` and `serverHostNonSsl` properties to specify the IP address that is bound to the designated NIC.

For example:

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

Typically, both the SSL and non-SSL listeners are configured to use the same NIC. However, if you use the `serverProtocol=http` property to off-load SSL for client connections, you can set the `serverHost` property to a separate NIC to provide SSL connections to systems that are used to launch View Administrator.

If you configure SSL and non-SSL connections to use the same NIC, the SSL and non-SSL ports must not be the same.

4 Restart the View Connection Server service or security server service to make your changes take effect.

What to do next

If necessary, manually configure your Windows firewall to open the updated ports.

Replace the Default Ports or NICs for the PCoIP Secure Gateway on View Connection Server Instances and on Security Servers

You can replace the default ports or NICs that are used by a PCoIP Secure Gateway service that runs on a View Connection Server instance or security server. Your organization might require you to perform these tasks to comply with organization policies or to avoid contention.

For client-facing TCP and UDP connections, the PCoIP Secure Gateway listens on port 4172 by default. For UDP connections to View desktops, the PCoIP Secure Gateway listens on port 55000 by default.

The port that is specified in the PCoIP External URL does not change as a result of changes that you make to ports in this procedure. Depending on your network configuration, you might have to change the PCoIP External URL port as well.

If the computer on which the PCoIP Secure Gateway is running has multiple NICs, the computer listens on all NICs by default. You can select one NIC to listen on the configured ports by specifying the IP address that is bound to that NIC.

Prerequisites

Verify that the port that is specified in the PCoIP External URL on the View Connection Server instance or security server will continue to be valid after you change ports in this procedure.

Procedure

1 Start the Windows Registry Editor on the View Connection Server or security server computer where the PCoIP Secure Gateway is running.

2 Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` registry key.

3 Under this registry key, add one or more of the following String (`REG_SZ`) values with your updated port numbers.

For example:

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

4 (Optional) If the computer on which the PCoIP Secure Gateway is running has multiple NICs, select one NIC to listen on the configured ports.

Under the same registry key, add the following String (`REG_SZ`) values to specify the IP address that is bound to the designated NIC.

For example:

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

If you configure external and internal connections to use the same NIC, the external and internal UDP ports must not be the same.

5 Restart the VMware View PCoIP Secure Gateway service to make your changes take effect.

Replace the Default Port for View Composer

The SSL certificate that is used by the View Composer service is bound to a certain port by default. You can replace the default port by using the `SviConfig ChangeCertificateBindingPort` utility.

When you specify a new port with the `SviConfig ChangeCertificateBindingPort` utility, the utility unbinds the View Composer certificate from the current port and binds it to the new port.

During installation, View Composer configures the Windows firewall to open the required default port. If you change the port, you must manually reconfigure your Windows firewall to open the updated port and ensure connectivity to the View Composer service.

Prerequisites

Verify that the port you specify is available.

Procedure

1 Stop the View Composer service.

2 Open a command prompt on the Windows Server host where View Composer is installed.

3 Type the `SviConfig ChangeCertificateBindingPort` command.

For example:

```
sviconfig –operation=ChangeCertificateBindingPort
          –Port=port number
```

where `–port=`*`port number`* is the new port to which View Composer binds the certificate. The `–port=`*`port number`* parameter is required.

4 Restart the View Composer service to make your changes take effect.

What to do next

If necessary, manually reconfigure the Windows firewall on the View Composer server to open the updated port.

Replace the Default Ports for View Transfer Server

By default, the Apache Web server that is installed with View Transfer Server listens on port 80 or, if SSL is used, port 443. You can change the default ports by editing Apache Web server configuration files.

The default HTTP port is 80. You change the HTTP port by editing the `httpd.conf` file on the View Transfer Server computer.

The default HTTPS port is 443. You change the HTTPS port by editing the `mod_vprov.conf` file on the View Transfer Server computer.

During installation, View configures the Windows firewall to open the ports that are used by View Transfer Server by default. If you change the ports, you must manually reconfigure your Windows firewall to open the updated ports so that View Client devices can connect to the View Transfer Server instance.

Procedure

1 Stop the VMware View Transfer Server service.

2 On the View Transfer Server computer, navigate to the *install_directory*\VMware\VMware View\Server\httpd\conf directory.

The `httpd.conf` and `mod_vprov.conf` files are located in this directory.

3 Change the HTTP port.

a Open the `httpd.conf` file.

b Update the `Listen` value.

For example: **Listen 4080**

c Save the `httpd.conf` file.

4 Change the HTTPS port.

a Open the `mod_vprov.conf` file.

b Update the `Listen` value.

For example: **Listen 4443**

c Update the `Virtual Host` entry.

For example, update the entry as follows:

```
# Configure SSL
<VirtualHost_default_:4443>
  SSLEngine on
  SSLCertificateFile ./conf/server.crt
  SSLCertificateKeyFile ./conf/server.key

  <Location /vprov>
    SetHandler vprov
  </Location>
</VirtualHost>
```

d Save the `mod_vprov.conf` file.

5 Restart the VMware View Transfer Server service to make your changes take effect.

What to do next

If necessary, manually configure your Windows firewall to open the updated ports.

Sizing Windows Server Settings to Support Your Deployment

To support a large deployment of View Manager desktops, you can configure the Windows Server computers on which you install View Connection Server. On each computer, you can size the Windows page-file.

On 64-bit Windows Server 2008 computers, the ephemeral ports, TCB hash table, and Java Virtual Machine settings are sized by default. These adjustments ensure that the computers have adequate resources to run correctly with the expected user load.

By default, the system can create a maximum of approximately 16,000 ephemeral ports that run concurrently on Windows Server 2008. 16,000 ephemeral ports can support more than 2,000 concurrent client connections, the maximum supported number for a View Connection Server instance.

On Windows Server 2008 computers, you do not need to increase the maximum size of the TCB hash table. Windows Server 2008 fully tunes this value by default.

For hardware and memory requirements for View Connection Server, see "Hardware Requirements for View Connection Server," on page 8.

For hardware and memory recommendations for using View Connection Server in a large View deployment, see "View Connection Server Maximums and Virtual Machine Configuration" in *VMware Horizon View Architecture Planning*.

Sizing the Java Virtual Machine

The View Connection Server installer sizes the Java Virtual Machine (JVM) heap memory on View Connection Server computers to support a large number of concurrent View desktop sessions.

On a 64-bit Windows Server computer with at least 10GB of memory, the installer configures a JVM heap size of 2GB for the View Secure Gateway Server component. This configuration supports approximately 2,000 concurrent tunnel sessions, the maximum number that View Connection Server can support. There is no benefit in increasing the JVM heap size on a 64-bit computer with 10GB of memory.

NOTE On a 64-bit View Connection Server computer, 10GB of memory is recommended for deployments of 50 or more View desktops. Configure less than 10GB of memory for small, proof-of-concept deployments only.

If a 64-bit computer has less than 10GB of memory, the installer configures a JVM heap size of 512MB for the View Secure Gateway Server component. If the computer has the required minimum of 4GB of memory, this configuration supports approximately 500 concurrent tunnel sessions. This configuration is more than adequate to support small, proof-of-concept deployments.

If you increase a 64-bit computer's memory to 10GB to support a larger deployment, View Connection Server does not increase the JVM heap size. To adust the JVM heap size to the recommended value, reinstall View Connection Server.

IMPORTANT Do not change the JVM heap size on 64-bit Windows Server computers. Changing this value might make View Connection Server behavior unstable. On 64-bit computers, the View Connection Server installer sets the JVM heap size to accord with the physical memory. If you change the physical memory on a 64-bit View Connection Server computer, reinstall View Connection Server to reset the JVM heap size.

Configure the System Page-File Settings

You can optimize the virtual memory on the Windows Server computers on which your View Connection Server instances are installed by changing the system page-file settings.

When Windows Server is installed, Windows calculates an initial and maximum page-file size based on the physical memory installed on the computer. These default settings remain fixed even after you restart the computer.

If the Windows Server computer is a virtual machine, you can change the memory size through vCenter Server. However, if Windows uses the default setting, the system page-file size does not adjust to the new memory size.

Procedure

1 On the Windows Server computer on which View Connection Server is installed, navigate to the Virtual Memory dialog box.

By default, **Custom size** is selected. An initial and maximum page-file size appear.

2 Click **System managed size**.

Windows continually recalculates the system page-file size based on current memory use and available memory.

Adding the View Desktops Plug-in to the vSphere Web Client 9

The View Desktops plug-in lets you use the vSphere Web Client to find information about View deployments that run in your vSphere environment. You add the View Desktops plug-in to the vSphere Web Client by registering the plug-in with the vCenter Lookup Service.

In View 5.2, the View Desktops plug-in is a Tech Preview feature that lets you quickly navigate from users of virtual desktops in View to the underlying virtual machines on which those virtual desktops are based.

Use the View Desktops plug-in to troubleshoot issues with a user's desktop. If a user calls in with a problem such as a desktop that is performing slowly, you can immediately jump to the user's virtual machine on the Virtual Machines page of the vSphere Web Client and troubleshoot the issue.

This chapter includes the following topics:

Add the View Desktops Plug-in

To add the View Desktops plug-in to the vSphere Web Client, you must configure the vCenter Lookup Service and register the plug-in. To perform these tasks, you run the `regtool.cmd` utility installed with View Connection Server.

Procedure

1 View Desktops Support for View Pods and vCenter Server Services on page 114

The View Desktops plug-in supports a single pod of replicated View Connection Server instances. You cannot use the View Desktops plug-in to search for desktops that are managed by different pods of replicated View Connection Server instances.

2 View Desktops Registration Prerequisites on page 114

Before you add the View Desktops plug-in to the vSphere Web Client, you must verify that your vSphere and View environments are prepared for the registration. You also must identify user accounts with the administrator privileges required to register the plug-in.

3 Configure View to Recognize the vCenter Lookup Service on page 115

You must configure View to recognize the vCenter Lookup Service. You perform this configuration task once for all View Connection Server instances in a replicated group.

4 Register the View Desktops Plug-in on page 116

You must register the View Desktops plug-in with the vCenter Single-Sign On Service and vCenter Lookup Service.

View Desktops Support for View Pods and vCenter Server Services

The View Desktops plug-in supports a single pod of replicated View Connection Server instances. You cannot use the View Desktops plug-in to search for desktops that are managed by different pods of replicated View Connection Server instances.

Even if multiple View pods use the same vCenter Single Sign-On Service and vCenter Lookup Service, the View Desktops plug-in can support only one pod at a time.

To use the View Desktops plug-in for a different View pod, you must unregister the View Desktops plug-in on all the View Connection Server instances in the first pod and register the plug-in on the View Connection Server instances in the second pod.

Conversely, if one View pod is configured with multiple vCenter Server instances, each using its own vCenter Single Sign-On Service and vCenter Lookup Service, you can configure the View Desktops plug-in for only one vCenter Lookup Service. To use the View Desktops plug-in for a different vCenter Lookup Service, you must unregister the View Desktops plug-in on all the View Connection Server instances and remove the vCenter Lookup Service from View Connection Server (the View pod). You can then configure and register the View pod to use the new vCenter Lookup Service.

For details about unregistering and removing the plug-in, see "Remove the View Desktops Plug-in," on page 118.

View Desktops Registration Prerequisites

Before you add the View Desktops plug-in to the vSphere Web Client, you must verify that your vSphere and View environments are prepared for the registration. You also must identify user accounts with the administrator privileges required to register the plug-in.

Procedure

- Verify that the following products are installed:
  - VMware vSphere 5.1 or a later update or release
  - VMware Horizon View 5.2 or a later update or release
- Verify that the vSphere Web Client is configured and accessible.
- Verify that system clocks on your vSphere and View systems are synchronized.
- Verify that valid SSL certificates are configured on your vSphere and View servers.

  If the SSL certificate that is issued for the vCenter Lookup Service is not trusted by the View Connection Server computer on which you configure the View Desktops plug-in, you must accept the thumbpint of the vCenter Lookup Service certificate during the configuration step.
- Verify that snapshots were taken of the virtual machines on which the following vCenter Server services are installed:
  - vCenter Single Sign-On
  - vSphere Web Client

  These services might be configured on separate systems or the same system.

- Verify that you have a user with vCenter Single Sign-On (SSO) administrator privileges.

  You must provide this account when you register the View Desktops plug-in.

  a Log in to the vSphere Web Client with a user account that has vCenter SSO administrator privileges.

    For example, on a vCenter Server that runs on Windows Server, the default vCenter SSO administrator user is *Admin*@System-Domain. On a vCenter Server Virtual Appliance, the default user is root@localos.

  b Browse to **Administration > Access > SSO Users and Groups**.

    The Users tab on the vCenter Single Sign-On Users and Groups page displays the users with vCenter SSO administrator privileges. You can use any displayed user.

- Verify that you have a user with the View Administrators role or Global Configuration and Policy Administrators role. You can also use a user with the View Administrators role on an individual folder.

  You must provide this account when you configure the vCenter Lookup Service and register the View Desktops plug-in.

  You authorize a View Administrators account when you install View Connection Server. See "Install View Connection Server with a New Configuration," on page 38.

  In the View Administrator user interface, you can authorize additional users with the View Administrators role or Global Configuration and Policy Administrators role. In addition, you can authorize a user to have the View Administrators role on an individual folder. See "Manage Administrators" in the *VMware Horizon View Administration* document.

What to do next

Configure the vCenter Lookup Service.

Configure View to Recognize the vCenter Lookup Service

You must configure View to recognize the vCenter Lookup Service. You perform this configuration task once for all View Connection Server instances in a replicated group.

Prerequisites

- Verify that your vCenter Server and View environments are prepared for the registration. See "View Desktops Registration Prerequisites," on page 114.

Procedure

1 On the View Connection Server computer, navigate to the `regtool.cmd` utility, located in the following directory:

  install_directory\VMware\VMware View\Server\TechPreview\ViewAdminPlugin

2 (Optional) Set the `JAVA_HOME` environment variable to the `jre` folder.

  For example: **`set JAVA_HOME=c:\Program Files\VMware\VMware View\Server\jre`**

3 Configure the vCenter Lookup Service.

  For example:
  `regtool.cmd configureLookupService -u` ***`view-admin@domain`*** **`-ld https://`*`lookup-server`*`:7444/lookupservice/sdk`**

  view-admin@domain is the username and domain of a user with the View Administrators role.

  lookup-server@domain is the host name or IP address and domain of the computer on which the vCenter Lookup Service is installed.

4 If the SSL certificate that is issued for the vCenter Lookup Service is not trusted by the View Connection Server computer, accept the certificate thumbprint.

The following error message is displayed:

```
Error: The security certificate presented by this Lookup Service was not
issued by a trusted certificate authority. The thumbprint of the certificate is
thumbprint.
Return code: -1
```

Accept the thumbprint by using the `-lt` option and copying the thumbprint. You can copy the thumbprint that is displayed in the error message and paste it into the command line.

For example:
`regtool.cmd configureLookupService -u` *`view-admin@domain`* `-ld https://` *`lookup-server`*`:7444/lookupservice/sdk -lt` *`thumbprint`*

The *thumbprint* might look like this: `31:2A:32:50:1A:0B:34:B1:65:46:13:A8:0A:5E:F7:43:6E:A9:2C:3E`

5 At the prompt, type the View Administrators user password.

A return code of `0` indicates that the configuration was successful.

NOTE When you type the password, the following warning message might appear. You can ignore this message:

```
log4j: WARN No appenders could be found for logger
<com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl>.
log4j: WARN Please initialize the log4j system properly.
```

What to do next

Register the View Desktops plug-in.

Register the View Desktops Plug-in

You must register the View Desktops plug-in with the vCenter Single-Sign On Service and vCenter Lookup Service.

You must register the View Desktops plug-in on each View Connection Server instance in a replicated group. Repeat this procedure on each View Connection Server computer.

NOTE The `regtool.cmd register` commands in this procedure assume that your View Connection Server service uses the default port, 443. If you change the default View Connection Server port, use the `-p` *`port-number`* option with the `regtool.cmd register` command to specify the custom port number.

Prerequisites

Verify that the vCenter Lookup Service is configured for the View Desktops plug-in. See "Configure View to Recognize the vCenter Lookup Service," on page 115.

Procedure

1 On the View Connection Server computer, navigate to the `regtool.cmd` utility, located in the following directory:

`install_directory``\VMware\VMware View\Server\TechPreview\ViewAdminPlugin`

2 Register the View Desktops plug-in.

For example: **`regtool.cmd register -u` *`view-admin@domain`* `-lu` *`sso-admin@domain`***

`view-admin@domain` is the username and domain of a user with the View Administrators role.

sso_admin@domain is the username and domain of a user with vCenter SSO administrator privileges. On a vCenter Server that runs on Windows Server, the default vCenter SSO administrator user is *Admin*@System-Domain. On a vCenter Server Virtual Appliance, the default user is root@localos.

3 At the prompt, type the View Administrators user password.

4 At the prompt, type the vCenter SSO administrator user password.

A return code of 0 indicates that the configuration was successful.

NOTE When you type the password, the following warning message might appear. You can ignore this message:

```
log4j: WARN No appenders could be found for logger
<com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl>.
log4j: WARN Please initialize the log4j system properly.
```

---

5 If necessary, restart the VMware vSphere Web Client Service.

In certain cases, this service must be restarted to allow the registration to take effect.

The service resides on the vCenter Server or another computer, not on the View Connection Server computer.

6 (Optional) Verify that the View Connection Server pod, View Desktops plug-in, and View Connection Server instance were registered successfully by using the `regtool.cmd showDetails` command.

For example: **`regtool.cmd showDetails -u`** ***`view-admin@domain`***

What to do next

Log in to the vSphere Web Client to verify that the View Desktops plug-in was added. See "Search for View Users in the vSphere Web Client," on page 117.

Search for View Users in the vSphere Web Client

In **View Desktops** in the vSphere Web Client, you can perform a quick search or simple search for a View user, display the desktops that are associated with that user, and examine the underlying virtual machines. After you first configure the View Desktops plug-in, perform this task to verify that the plug-in was added to the vSphere Web Client.

When you search for a View user in the vSphere Web Client, **View Desktops** displays floating desktops on which the user is logged in and dedicated desktops that are assigned to the user. Note that a floating desktop is displayed even when the session is in a disconnected state. If a user is entitled to a floating desktop pool but not logged in, no floating desktops in that pool are displayed.

This procedure uses quick search. You can also use a simple search to search for View users. In this Tech Preview, you cannot use an advanced search to search for View users.

Prerequisites

- Verify that the View Desktops plug-in was configured with the vCenter Lookup Service and registered with the vSphere Web Client. See "Configure View to Recognize the vCenter Lookup Service," on page 115 and "Register the View Desktops Plug-in," on page 116.
- Verify that you can log in to the vSphere Web Client as a user with the View Administrators role or View Administrators (Read only) role and with the vSphere Administrator privilege for the View desktop virtual machines and vCenter Server folders that store the virtual machines.

  If you search for desktops without having the vSphere Administrator privilege, the virtual machine names are displayed as disabled links and you cannot access the virtual machine information.

Procedure

1 Log in to the vSphere Web Client as a user with the View Administrators or View Administrators (read only) role and the appropriate vSphere Administrator privileges.

For example: **https://*vSphere_Web_Client_IP_address_or_FQDN*:9443/vsphere-client/**

2 In the Search box, type the username of a View user.

3 Select the username from the search results.

4 Select a desktop from the list of desktops that is associated with the user.

5 Navigate to the Virtual Machines page to see details about the underlying desktop virtual machine.

Remove the View Desktops Plug-in

To remove the View Desktops plug-in from the vSphere Web Client, you must unregister the plug-in on each View Connection Server instance in a replicated group. Next, you remove the vCenter Lookup Service configuration.

In a replicated group of View Connection Server instances, you cannot unregister the instance on which you first registered the View Desktops plug-in until all other instances are unregistered.

If you intend to perform maintenance operations on the View Connection Server instances in a replicated group, you can use the `-f` option with the `regtool.cmd removeLookUpService` command to unregister all the View Connection Server instances and remove the vCenter Lookup Service configuration in one step.

If you intend to bring down a View Connection Server instance for scheduled maintenance, you must unregister the instance from the vCenter Lookup Service before you start the maintenance procedure.

Procedure

1 On the View Connection Server computer, navigate to the `regtool.cmd` utility, located in the following directory:

install_directory\VMware\VMware View\Server\TechPreview\ViewAdminPlugin

2 Unregister View Desktops plug-in.

For example: **regtool.cmd unregister -u *view-admin@domain***

view-admin@domain is the username and domain of a user with the View Administrators role.

3 At the prompt, type the View Administrators user password.

A return code of `0` indicates that the configuration was successful.

4 Repeat the preceding steps to unregister the plug-in on all View Connection Server instances in a replicated group.

After all other instances are unregistered, unregister the plug-in on the instance on which you first performed the registration.

5 Remove the vCenter Lookup Service configuration from View Connection Server.

For example: **regtool.cmd removeLookUpService -u *view-admin@domain***

You can run this command on any View Connection Server instance in a replicated group. The command fails if the View Desktops plug-in is still registered on any View Connection Server instance.

6 At the prompt, type the View Administrators user password.

A return code of `0` indicates that the configuration was successful.

Configuring Event Reporting 10

You can create an event database to record information about View Manager events. In addition, if you use a Syslog server, you can configure View Connection Server to send events to a Syslog server or create a flat file of events written in `Syslog` format.

This chapter includes the following topics:

Add a Database and Database User for View Events

You create an event database by adding it to an existing database server. You can then use enterprise reporting software to analyze the events in the database.

The database server for the event database can reside on a View Connection Server host itself or on a dedicated server. Alternatively, you can use a suitable existing database server, such as a server that hosts a View Composer database.

NOTE You do not need to create an ODBC data source for this database.

Prerequisites

- Verify that you have a supported Microsoft SQL Server or Oracle database server on a system that a View Connection Server instance has access to. For a list of supported database versions, see "Database Requirements for View Composer," on page 10.
- Verify that you have the required database privileges to create a database and user on the database server.
- If you are not familiar with the procedure to create databases on Microsoft SQL Server database servers, review the steps in "Add a View Composer Database to SQL Server," on page 28.
- If you are not familiar with the procedure to create databases on Oracle database servers, review the steps in "Add a View Composer Database to Oracle 11g or 10g," on page 30.

Procedure

1 Add a new database to the server and give it a descriptive name such as ViewEvents.

2 Add a user for this database that has permission to create tables, views, and, in the case of Oracle, triggers and sequences, as well as permission to read from and write to these objects.

   For a Microsoft SQL Server database, do not use the Integrated Windows Authentication security model method of authentication. Be sure to use the SQL Server Authentication method of authentication.

The database is created, but the schema is not installed until you configure the database in View Administrator.

What to do next

Follow the instructions in "Configure the Event Database," on page 120.

Prepare an SQL Server Database for Event Reporting

Before you can use View Administrator to configure an event database on Microsoft SQL Server, you must configure the correct TCP/IP properties and verify that the server uses SQL Server Authentication.

Prerequisites

- Create an SQL Server database for event reporting. See "Add a Database and Database User for View Events," on page 119.
- Verify that you have the required database privileges to configure the database.
- Verify that the database server uses the SQL Server Authentication method of authentication. Do not use Windows Authentication.

Procedure

1 Open SQL Server Configuration Manager and expand **SQL Server*YYYY*Network Configuration**.

2 Select **Protocols for*server_name***.

3 In the list of protocols, right-click **TCP/IP** and select **Properties.**

4 Set the **Enabled** property to **Yes.**

5 Verify that a port is assigned or, if necessary, assign one.

   For information on the static and dynamic ports and how to assign them, see the online help for the SQL Server Configuration manager.

6 Verify that this port is not blocked by a firewall.

What to do next

Use View Administrator to connect the database to View Connection Server. Follow the instructions in "Configure the Event Database," on page 120.

Configure the Event Database

The event database stores information about View events as records in a database rather than in a log file.

You configure an event database after installing a View Connection Server instance. You need to configure only one host in a View Connection Server group. The remaining hosts in the group are configured automatically.

NOTE The security of the database connection between the View Connection Server instance and an external database is the responsibility of the administrator, although event traffic is limited to information about the health of the View environment. If you want to take extra precautions, you can secure this channel through IPSec or other means, or you can deploy the database locally on the View Connection Server computer.

You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *VMware Horizon View Integration* document.

You can also generate View events in `Syslog` format so that the event data can be accessible to third-party analytics software. You use the `vdmadmin` command with the `–I` option to record View event messages in `Syslog` format in event log files. See "Generating View Event Log Messages in Syslog Format Using the -I Option" in the *VMware Horizon View Administration* document.

Prerequisites

You need the following information to configure an event database:

- The DNS name or IP address of the database server.
- The type of database server: Microsoft SQL Server or Oracle.
- The port number that is used to access the database server. The default is 1521 for Oracle and 1433 for SQL Server. For SQL Server, if the database server is a named instance or if you use SQL Server Express, you might need to determine the port number. See the Microsoft KB article about connecting to a named instance of SQL Server, at http://support.microsoft.com/kb/265808.
- The name of the event database that you created on the database server. See "Add a Database and Database User for View Events," on page 119.
- The username and password of the user you created for this database. See "Add a Database and Database User for View Events," on page 119.

  Use SQL Server Authentication for this user. Do not use the Integrated Windows Authentication security model method of authentication.
- A prefix for the tables in the event database, for example, VE_. The prefix enables the database to be shared among View installations.

  NOTE You must enter characters that are valid for the database software you are using. The syntax of the prefix is not checked when you complete the dialog box. If you enter characters that are not valid for the database software you are using, an error occurs when View Connection Server attempts to connect to the database server. The log file indicates all errors, including this error and any others returned from the database server if the database name is invalid.

Procedure

1. In View Administrator, select **View Configuration > Event Configuration**.
2. In the **Event Database** section, click **Edit**, enter the information in the fields provided, and click **OK**.
3. (Optional) In the Event Settings window, click **Edit**, change the length of time to show events and the number of days to classify events as new, and click **OK**.

   These settings pertain to the length of time the events are listed in the View Administrator interface. After this time, the events are only available in the historical database tables.

   The Database Configuration window displays the current configuration of the event database.
4. Select **Monitoring > Events** to verify that the connection to the event database is successful.

   If the connection is unsuccessful, and error message appears. If you are using SQL Express or if you are using a named instance of SQL Server, you might need to determine the correct port number, as mentioned in the prerequisites.

In the View Administrator Dashboard, the System Component Status displays the event database server under the Reporting Database heading.

Configure Event Logging for Syslog Servers

You can generate View events in `Syslog` format so that the event data can be accessible to analytics software.

You need to configure only one host in a View Connection Server group. The remaining hosts in the group are configured automatically.

If you enable file-based logging of events, events are accumulated in a local log file. If you specify a file share, these log files are moved to that share.

- Use a local file only for quick troubleshooting during configuration, perhaps before the Events database is configured, so that you have some way to see events.

  The maximum size of the local directory for event logs, including closed log files, before the oldest files are deleted, is 300MB. The default destination of the Syslog output is `%PROGRAMDATA %\VMware\VDM\events\`.

- Use a UNC path to save log files for a long-term record of events, of if you do not have a Syslog server, or if your current Syslog server does not meet your needs.

You can alternatively use a `vdmadmin` command to configure file-based logging of events in Syslog format. See the topic about generating View event log messages in Syslog format using the `–I` option of the `vdmadmin` command, in the *VMware Horizon View Administration* document.

IMPORTANT Syslog data is sent across the network without software-based encryption, and might contain sensitive data, such as user names. VMware recommends using link-layer security, such as IPSEC, to avoid the possibility of this data being monitored on the network.

Prerequisites

You need the following information to configure View Connection Server so that events can be recorded in Syslog format or sent to a Syslog server, or both:

- If you plan to use a Syslog server to listen for the View events on a UDP port, you must have the DNS name or IP address of the Syslog server and the UDP port number. The default UDP port number is 514.
- If you plan to collect logs in a flat-file format, you must have the UNC path to the file share and folder in which to store the log files, and you must have the user name, domain name, and password of an account that has permission to write to the file share.

Procedure

1. In View Administrator, select **View Configuration > Event Configuration**.
2. (Optional) In the **Syslog** area, to configure View Connection Server to send events to a Syslog server, click **Add** next to **Send to syslog servers**, and supply the server name or IP address and the UDP port number.
3. (Optional) To enable View event log messages to be generated and stored in Syslog format, in log files, select the **Log to file: Enable** check box.

   The log files are retained locally unless you specify a UNC path to a file share.
4. (Optional) To store the View event log messages on a file share, click **Add** next to **Copy to location**, and supply the UNC path to the file share and folder in which to store the log files, along with the user name, domain name, and password of an account that has permission to write to the file share.

   An example of a UNC path is:

   ```
   \\syslog-server\folder\file
   ```

Index

W