VMware View Architecture Planning

View 4.6
View Manager 4.6
View Composer 2.6

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-000524-01

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

VMware View Architecture Planning

VMware View Architecture Planning provides an introduction to VMware View™, including a description of its major features and deployment options and an overview of how VMware View components are typically set up in a production environment.

This guide answers the following questions:

- Does VMware View solve the problems you need it to solve?
- Would it be feasible and cost-effective to implement a VMware View solution in your enterprise?

To help you protect your VMware View installation, the guide also provides a discussion of security features.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who need to familiarize themselves with the components and capabilities of VMware View. With this information, architects and planners can determine whether VMware View satisfies the requirements of their enterprise for efficiently and securely delivering Windows desktops and applications to their end users. The example architecture helps planners understand the hardware requirements and setup effort required for a large-scale VMware View deployment.

Introduction to VMware View 1

With VMware View, IT departments can run virtual desktops in the datacenter and deliver desktops to employees as a managed service. End users gain a familiar, personalized environment that they can access from any number of devices anywhere throughout the enterprise or from home. Administrators gain centralized control, efficiency, and security by having desktop data in the datacenter.

This chapter includes the following topics:

Advantages of Using VMware View

When you manage enterprise desktops with VMware View, the benefits include increased reliability, security, hardware independence, and convenience.

Reliability and Security

Virtual desktops can be centralized by integrating with VMware vSphere and virtualizing server, storage, and networking resources. Placing desktop operating systems and applications on a server in the datacenter provides the following advantages:

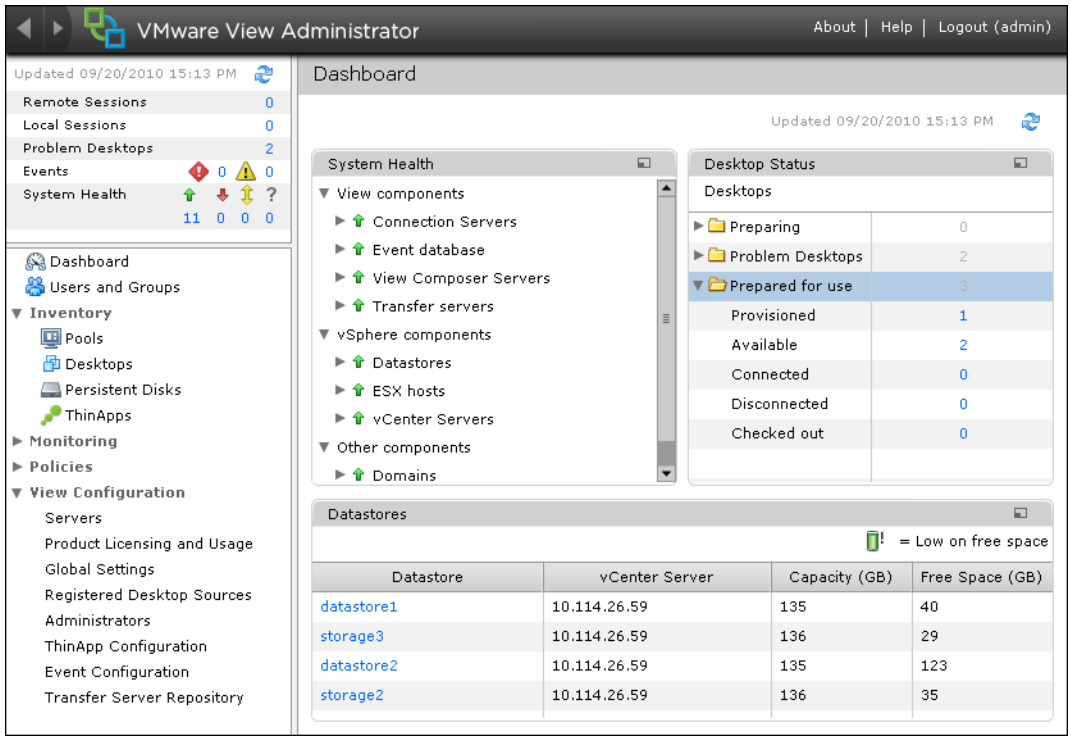
- Access to data can easily be restricted. Sensitive data can be prevented from being copied onto a remote employee's home computer.
- Data backups can be scheduled without considering when end users' systems might be turned off.
- Virtual desktops that are hosted in a datacenter experience little or no downtime. Virtual machines can reside on high-availability clusters of VMware servers.

Virtual desktops can also connect to back-end physical systems and Windows Terminal Services servers.

Convenience

The unified management console is built for scalability on Adobe Flex, so that even the largest View deployments can be efficiently managed from a single View Manager interface. Wizards and dashboards enhance the workflow and facilitate drilling down to see details or change settings. Figure 1-1 provides an example of the browser-based user interface for View Administrator.

Figure 1-1. Administrative Console for View Manager Showing the Dashboard View



Another feature that increases convenience is the VMware remote display protocol PCoIP. PCoIP (PC-over-IP) display protocol delivers an end-user experience equal to the current experience of using a physical PC:

- On LANs, the display is faster and smoother than traditional remote displays.
- On WANs, the display protocol can compensate for an increase in latency or a reduction in bandwidth, ensuring that end users can remain productive regardless of network conditions.

Manageability

Provisioning desktops for end users is a quick process. No one is required to install applications one by one on each end user's physical PC. End users connect to a virtual desktop complete with applications. End users can access their same virtual desktop from various devices at various locations.

Using VMware vSphere to host virtual desktops provides the following benefits:

- Administration tasks and management chores are reduced. Administrators can patch and upgrade applications and operating systems without touching a user's physical PC.
- Storage management is simplified. Using VMware vSphere, you can virtualize volumes and file systems to avoid managing separate storage devices.

Hardware Independence

Virtual machines are hardware-independent. Because a View desktop runs on a server in the datacenter and is only accessed from a client device, a View desktop can use operating systems that might not be compatible with the hardware of the client device.

For example, although Windows Vista can run only on Vista-enabled PCs, you can install Windows Vista in a virtual machine and use that virtual machine on a PC that is not Vista-enabled. Virtual desktops run on PCs, Macs, thin clients, and PCs that have been repurposed as thin clients.

VMware View Features

Features included in VMware View support usability, security, centralized control, and scalability.

The following features provide a familiar experience for the end user:

- Print from a virtual desktop to any local or networked printer that is defined on the client device, or use the location-based printing feature to map to printers that are physically near the client system. The virtual printer feature solves compatibility issues and does not require you to install additional print drivers in a virtual machine.
- Use multiple monitors. With PCoIP multiple-monitor support, you can adjust the display resolution and rotation separately for each monitor.
- Access USB devices and other peripherals that are connected to the local device that displays your virtual desktop.

VMware View offers the following security features, among others:

- Use RSA SecurID two-factor authentication or smart cards to log in.
- Use SSL tunneling to ensure that all connections are completely encrypted.
- Use VMware High Availability to host desktops and to ensure automatic failover.

The following features provide centralized administration and management:

- Use Microsoft Active Directory to manage access to virtual desktops and to manage policies.
- Use the Web-based administrative console to manage virtual desktops from any location.
- Use a template, or master image, to quickly create and provision pools of desktops.
- Send updates and patches to virtual desktops without affecting user settings, data, or preferences.

Scalability features depend on the VMware virtualization platform to manage both desktops and servers:

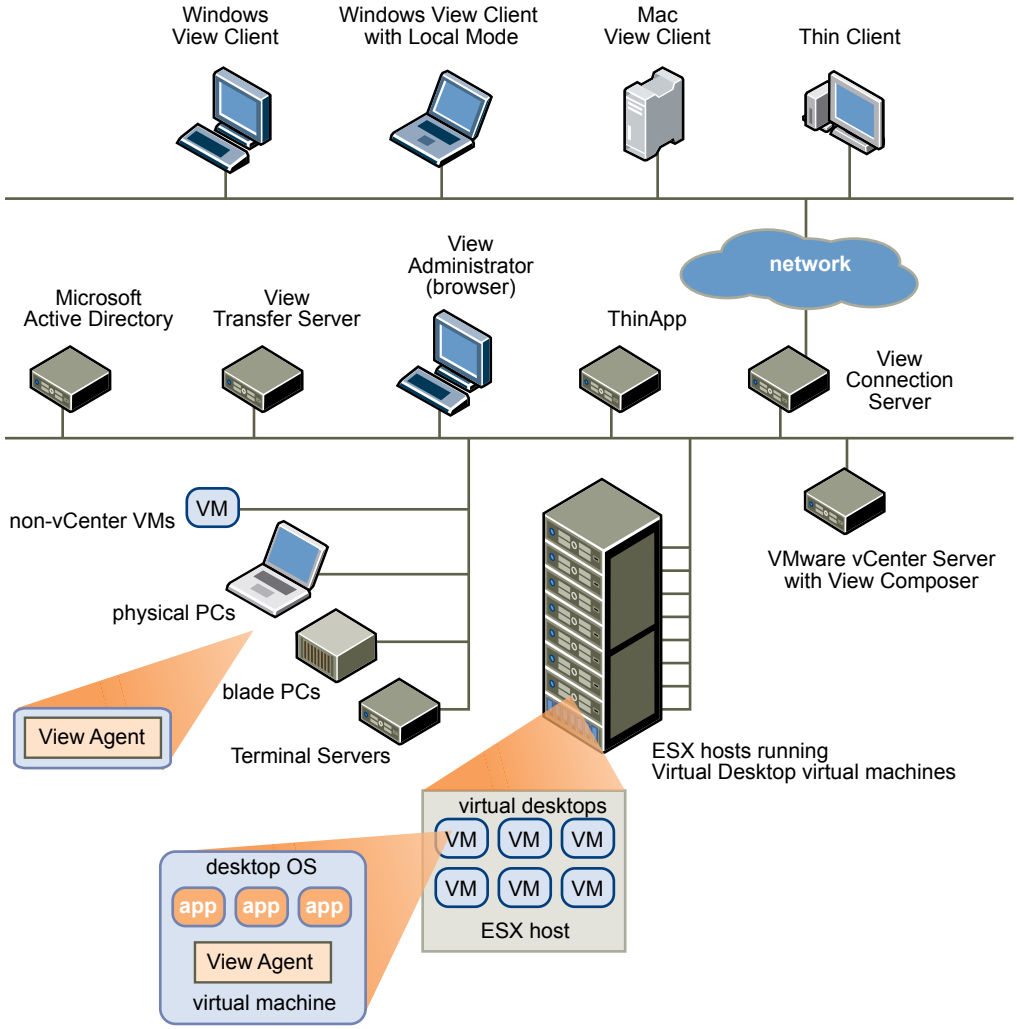
- Integrate with VMware vSphere to achieve cost-effective densities, high levels of availability, and advanced resource allocation control for your virtual desktops.
- Configure View Connection Server to broker connections between end users and the virtual desktops that they are authorized to access.
- Use View Composer to quickly create desktop images that share virtual disks with a master image. Using linked clones in this way conserves disk space and simplifies the management of patches and updates to the operating system.

How the VMware View Components Fit Together

End users start View Client to log in to View Connection Server. This server, which integrates with Windows Active Directory, provides access to a virtual desktop hosted in a VMware vSphere environment, a blade or physical PC, or a Windows Terminal Services server.

Figure 1-2 shows the relationship between the major components of a VMware View deployment.

Figure 1-2. High-Level Example of a VMware View Environment



Client Devices

A major advantage of using VMware View is that desktops follow the end user regardless of device or location. Users can access their personalized virtual desktop from a company laptop, their home PC, a thin client device, or a Mac or iPad.

From the iPad and from Mac and Windows laptops and PCs, end users open View Client to display their View desktop. Thin client devices use View thin client software and can be configured so that the only application that users can launch directly on the device is View Thin Client. Repurposing a legacy PC into a thin client desktop can extend the life of the hardware by three to five years. For example, by using VMware View on a thin desktop, you can use a newer operating system such as Windows Vista on older desktop hardware.

View Connection Server

This software service acts as a broker for client connections. View Connection Server authenticates users through Windows Active Directory and directs the request to the appropriate virtual machine, physical or blade PC, or Windows Terminal Services server.

View Connection Server provides the following management capabilities:

- Authenticating users
- Entitling users to specific desktops and pools

- Assigning applications packaged with VMware ThinApp to specific desktops and pools
- Managing local and remote desktop sessions
- Establishing secure connections between users and desktops
- Enabling single sign-on
- Setting and applying policies

Inside the corporate firewall, you install and configure a group of two or more View Connection Server instances. Their configuration data is stored in an embedded LDAP directory and is replicated among members of the group.

Outside the corporate firewall, in the DMZ, you can install and configure View Connection Server as a security server. Security servers in the DMZ communicate with View Connection Servers inside the corporate firewall. Security servers ensure that the only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. Users can access only the desktop resources that they are authorized to access.

Security servers offer a subset of functionality and are not required to be in an Active Directory domain. You install View Connection Server in a Windows Server 2008 server, preferably on a VMware virtual machine.

View Client

The client software for accessing View desktops runs either on an iPad or Windows or Mac PC as a native application or on a thin client if you have View Client for Linux.

After logging in, users select from a list of virtual desktops that they are authorized to use. Authorization can require Active Directory credentials, a UPN, a smart card PIN, or an RSA SecurID token.

An administrator can configure View Client to allow end users to select a display protocol. Protocols include PCoIP, Microsoft RDP, and HP RGS for View desktops that are hosted on HP Blades. The speed and display quality of PCoIP rival that of a physical PC.

View Client with Local Mode (formerly called Offline Desktop) is a version of View Client that has been extended to allow end users to download virtual machines and use them on their local systems regardless of whether they have a network connection.

Features differ according to which View Client you use. This guide focuses on View Client for Windows and View Client for Mac. The following types of clients are not described in detail in this guide:

- Details about View Client for iPad. See *Using VMware View Client for iPad*.
- View Client for Linux, available only through certified partners.
- Various third-party clients, available only through certified partners.
- View Open Client, which supports the VMware partner certification program. View Open Client is not an official View client and is not supported as such.

View Portal

From a Windows PC or laptop, end users can open a Web browser and use View Portal to download, install, update, and start the Windows-based View Client. As of View 4.5, View Portal installs the full View Client for Windows, with or without Local Mode.

To use View Portal, end users open an Internet Explorer browser and enter the URL of a View Connection Server instance. View Portal provides a link for downloading the installer for the full View Client for Windows.

View Agent

You install the View Agent service on all virtual machines, physical systems, and Terminal Service servers that you use as sources for View desktops. This agent communicates with View Client to provide features such as connection monitoring, virtual printing, and access to locally connected USB devices.

If the desktop source is a virtual machine, you first install the View Agent service on that virtual machine and then use the virtual machine as a template or as a parent of linked clones. When you create a pool from this virtual machine, the agent is automatically installed on every virtual desktop.

You can install the agent with an option for single sign-on. With single sign-on, users are prompted to log in only when they connect to View Connection Server and are not prompted a second time to connect to a virtual desktop.

View Administrator

This Web-based application allows administrators to configure View Connection Server, deploy and manage View desktops, control user authentication, and troubleshoot end user issues.

When you install a View Connection Server instance, the View Administrator application is also installed. This application allows administrators to manage View Connection Server instances from anywhere without having to install an application on their local computer.

View Composer

You install this software service on a vCenter Server instance that manages virtual machines. View Composer can then create a pool of linked clones from a specified parent virtual machine. This strategy reduces storage costs by up to 90 percent.

Each linked clone acts like an independent desktop, with a unique host name and IP address, yet the linked clone requires significantly less storage because it shares a base image with the parent.

Because linked-clone desktop pools share a base image, you can quickly deploy updates and patches by updating only the parent virtual machine. End users' settings, data, and applications are not affected. As of View 4.5, you can also use linked-clone technology for View desktops that you download and check out to use on local systems.

vCenter Server

This service acts as a central administrator for VMware ESX/ESXi servers that are connected on a network. vCenter Server, formerly called VMware VirtualCenter, provides the central point for configuring, provisioning, and managing virtual machines in the datacenter.

In addition to using these virtual machines as sources for View desktop pools, you can use virtual machines to host the server components of VMware View, including Connection Server instances, Active Directory servers, and vCenter Server instances.

You can install View Composer on the same server as vCenter Server to create linked-clone desktop pools. vCenter Server then manages the assignment of the virtual machines to physical servers and storage and manages the assignment of CPU and memory resources to virtual machines.

You install vCenter Server in a Windows Server 2003 or 2008 server, preferably on a VMware virtual machine.

View Transfer Server

This software manages and streamlines data transfers between the datacenter and View desktops that are checked out for use on end users' local systems. View Transfer Server is required to support desktops that run View Client with Local Mode (formerly called Offline Desktop).

Several operations use View Transfer Server to send data between the View desktop in vCenter Server and the corresponding local desktop on the client system.

- When a user checks in or checks out a desktop, View Manager authorizes and manages the operation. View Transfer Server transfers the files between the datacenter and the local desktop.
- View Transfer Server synchronizes local desktops with the corresponding desktops in the datacenter by replicating user-generated changes to the datacenter.

  Replications occur at intervals that you specify in local-mode policies. You can also initiate replications in View Administrator. You can set a policy that allows users to initiate replications from their local desktops.
- View Transfer Server distributes common system data from the datacenter to local clients. View Transfer Server downloads View Composer base images from the Transfer Server repository to local desktops.

Integrating and Customizing VMware View

To enhance the effectiveness of VMware View in your organization, you can use several interfaces to integrate VMware View with external applications or to create administration scripts that you can run from the command line or in batch mode.

Integrating View with Business Intelligence Software

You can configure VMware View to record events to a Microsoft SQL Server or Oracle database.

- End-user actions such as logging in and starting a desktop session.
- Administrator actions such as adding entitlements and creating desktop pools.
- Alerts that report system failures and errors.
- Statistical sampling such as recording the maximum number of users over a 24-hour period.

You can use business intelligence reporting engines such as Crystal Reports, IBM Cognos, MicroStrategy 9, and Oracle Enterprise Performance Management System to access and analyze the event database.

For more information, see the *VMware View Integration* document.

Using View PowerCLI to Create Administration Scripts

Windows PowerShell is a command-line and scripting environment that is designed for Microsoft Windows. PowerShell uses the .NET object model and provides administrators with management and automation capabilities. As with any other console environment, you work with PowerShell by running commands, which are called cmdlets in PowerShell.

The View PowerCLI provides an easy-to-use PowerShell interface to VMware View. You can use the View PowerCLI cmdlets to perform various administration tasks on View components.

- Create and update desktop pools.
- Add datacenter resources to a full virtual machine or linked-clone pool.
- Perform rebalance, refresh, or recompose operations on linked-clone desktops.
- Sample the usage of specific desktops or desktop pools over time.

- Query the event database.
- Query the state of View services.

You can use the cmdlets in conjunction with the vSphere PowerCLI cmdlets, which provide an administrative interface to the VMware vSphere product.

For more information, see the *VMware View Integration* document.

Modifying LDAP Configuration Data in View

When you use View Administrator to modify the configuration of VMware View, the appropriate LDAP data in the repository is updated. VMware View stores its configuration information in an LDAP compatible repository. For example, if you add a desktop pool, VMware View stores information about users, user groups, and entitlements in LDAP.

You can use VMware and Microsoft command tools to export and import LDAP configuration data in LDAP Data Interchange Format (LDIF) files from and into VMware View. These commands are for advanced administrators who want to use scripts to update configuration data without using View Administrator or View PowerCLI.

You can use LDIF files to perform a number of tasks.

- Transfer configuration data between View Connection Server instances.
- Define a large number of View objects, such as desktop pools, and add these to your View Connection Server instances without using View Administrator or View PowerCLI.
- Back up your View configuration so that you can restore the state of a View Connection Server instance.

For more information, see the *VMware View Integration* document.

Using SCOM to Monitor View Components

You can use Microsoft System Center Operations Manager (SCOM) to monitor the state and performance of VMware View components, including View Connection Server instances and security servers and View services running on these hosts.

For more information, see the *VMware View Integration* document.

Using the vdmadmin Command to Administer View

You can use the `vdmadmin` command line interface to perform a variety of administration tasks on a View Connection Server instance. You can use `vdmadmin` to perform administration tasks that are not possible from within the View Administrator user interface or that need to run automatically from scripts.

For more information, see the *VMware View Administration* document.

Planning a Rich User Experience 2

VMware View provides the familiar, personalized desktop environment that end users expect. End users can access USB and other devices connected to their local computer, send documents to any printer that their local computer can detect, authenticate with smart cards, and use multiple display monitors.

VMware View includes many features that you might want to make available to your end users. Before you decide which features to use, you must understand the limitations and restrictions of each feature.

This chapter includes the following topics:

Feature Support Matrix

Most features, such as access to local USB devices, virtual printing, Wyse multimedia redirection (MMR), and PCoIP and Microsoft RDP display protocols, are supported on most Windows client operating systems. You must also take into consideration whether the feature is supported on the View desktop operating system.

When planning which display protocol and features to make available to your end users, use the following tables to determine which client operating systems and agent (View desktop) operating systems support the feature.

Editions of Windows Vista include Windows Vista Home, Enterprise, Ultimate, and Business. Editions of Windows 7 include Home, Professional, Enterprise, and Ultimate. For Windows Terminal Server, the edition is Standard Edition.

Table 2-1. Features Supported on Operating Systems for View Desktops (Where View Agent Is Installed)

Feature	Windows XP Home/Pro SP3, 32-bit	Windows Vista SP1, SP2, 32-bit	Windows 7, 32-bit and 64-bit	Windows 2003/2003 R2 Terminal Server SP2, 32-bit	Windows 2008 SP2/2008 R2 Terminal Server 64-bit
USB access	X	X	X		
RDP display protocol	X	X	X	X	X
PCoIP display protocol	X	X	X		
HP RGS display protocol	X	X			
Wyse MMR	X	X			
Virtual printing	X	X	X		
Smart cards	X	X	X	X	X
RSA SecurID	X	X	X	N/A	N/A
Single sign-on	X	X	X	X	X
Multiple monitors	X	X	X		With RDP 7
Local Mode	X	X	X		

Table 2-2. Features Supported on Windows Clients

Feature	Windows XP Home/Pro SP3, 32-bit	Windows Vista SP1, SP2, 32-bit	Windows 7, 32-bit and 64-bit
USB access	X	X	X
RDP display protocol	X	X	X
PCoIP display protocol	X	X	X
HP RGS display protocol	X	X	
Wyse MMR	X	X	
Virtual printing	X	X	X
Smart cards	X	X	X
RSA SecurID	X	X	X
Single sign-on	X	X	X
Multiple monitors	X	X	X
Local Mode	X	X	X

Table 2-3. Features Supported on Mac Clients

Feature	Mac OS X (10.5,6)	Mac OS X (10.6)
USB access		
RDP display protocol	X	X
PCoIP display protocol		
HP RGS display protocol		
Wyse MMR		
Virtual printing		

Table 2-3. Features Supported on Mac Clients (Continued)

Feature	Mac OS X (10.5,6)	Mac OS X (10.6)
Smart cards		
RSA SecurID	X	X
Single sign-on	X	X
Multiple monitors		
Local Mode		

In addition, several VMware partners offer thin client devices for VMware View deployments. The features that are available for each thin client device are determined by the vendor and model and the configuration that an enterprise chooses to use. For information about the vendors and models for thin client devices, see the *Thin Client Compatibility Guide*, available on the VMware Web site.

NOTE For information about which features are supported on the iPad, see *Using VMware View Client for iPad*.

Choosing a Display Protocol

A display protocol provides end users with a graphical interface to a View desktop that resides in the datacenter. You can use Microsoft RDP (Remote Desktop Protocol), HP RGS for HP physical machines, or PCoIP (PC-over-IP).

You can set policies to control which protocol is used or to allow end users to choose the protocol when they log in to a desktop.

NOTE When you check out a desktop for use on a local client system, neither of the RDP or PCoIP remote display protocols is used.

VMware View with PCoIP

PCoIP is a new high-performance remote display protocol provided by VMware. This protocol is available for View desktops that are sourced from virtual machines, Teradici clients, and physical machines that have Teradici-enabled host cards.

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 optimized for delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN. PCoIP provides the following features:

- You can use up to 4 monitors and adjust the resolution for each monitor separately, up to 2560 x 1600 resolution per display.
- You can copy and paste text between the local system and the View desktop, but you cannot copy and paste system objects such as folders and files between systems.
- PCoIP supports 32-bit color.
- PCoIP supports 128-bit encryption.
- PCoIP supports Advanced Encryption Standard (AES) encryption, which is turned on by default.
- For users outside the corporate firewall, you can use this protocol with your company's virtual private network or with View security servers.

Client hardware requirements include the following:

- 800MHz or higher processor speed
- x86-based processor with SSE2 extensions

Microsoft RDP

Remote Desktop Protocol is the same protocol many people already use to access their work computer from their home computer. RDP provides access to all the applications, files, and network resources on a remote computer.

Microsoft RDP provides the following features:

- You can use multiple monitors in span mode.
- You can copy and paste text between the local system and the View desktop, but you cannot copy and paste system objects such as folders and files between systems.
- You can configure the amount of bandwidth used by Adobe Flash content to improve the overall Web browsing experience and make other applications more responsive.
- RDP supports 32-bit color.
- RDP supports 128-bit encryption.
- You can use this protocol for making secure, encrypted connections to a View security server in the corporate DMZ.

HP RGS Protocol

RGS is a display protocol from HP that allows users to access the desktop of a remote physical computer over a standard network.

You can use HP RGS as the display protocol when connecting HP Blade PCs, HP Workstations, and HP Blade Workstations. Connections to virtual machines that run on VMware ESX/ESXi hosts are not supported.

HP RGS provides the following features:

- You can use multiple monitors in span mode.
- You can configure the amount of bandwidth used by Adobe Flash content to improve the overall Web browsing experience and make other applications more responsive.

VMware does not bundle or license HP RGS with VMware View. Contact HP to license a copy of HP RGS version 5.2.5 to use with VMware View. For information about how to install and configure HP RGS components, see the HP RGS documentation available at http://www.hp.com.

Benefits of Using View Desktops in Local Mode

With View Client with Local Mode, users can check out and download a View desktop to a local system such as a laptop. Administrators can manage these local View desktops by setting policies for the frequency of backups and contact with the server, access to USB devices, and permission to check in desktops.

For employees at remote offices with poor network connections, applications run faster on a local View desktop than on a remote desktop. Also, users can use the local version of the desktop with or without a network connection.

If a network connection is present on the client system, the desktop that is checked out continues to communicate with View Connection Server to provide policy updates, and ensure that locally cached authentication criteria is current. By default, contact is attempted every 5 minutes.

View Client with Local Mode is the fully supported feature that in earlier releases was an experimental feature called View Client with Offline Desktop.

View desktops in local mode behave in the same way as their remote desktop equivalents, yet can take advantage of local resources. Latency is eliminated, and performance is enhanced. Users can disconnect from their local View desktop and log in again without connecting to the View Connection Server. After network access is restored, or when the user is ready, the checked-out virtual machine can be backed up, rolled back, or checked in.

Local resource utilization

After a local desktop is checked out, it can take advantage of the memory and CPU capabilities of the local system. For example, memory available beyond what is required for the host and guest operating systems is usually split between the host and the local View desktop, regardless of the memory settings that are specified for the virtual machine in vCenter Server. Similarly, the local View desktop can automatically use up to two CPUs available on the local system, and you can configure the local desktop to use up to four CPUs.

Although a local desktop can take advantage of local resources, a Windows 7 or Windows Vista View desktop that is created on an ESX/ESXi 3.5 host cannot produce 3-D and Windows Aero effects. This limitation applies even when the desktop is checked out for local use on a Windows 7 or Windows Vista host. Windows Aero and 3-D effects are available only if the View desktop is created using vSphere 4.x.

Conserving datacenter resources by requiring local mode

You can reduce datacenter costs associated with bandwidth, memory, and CPU resources by requiring that View desktops be downloaded and used only in local mode. This strategy is sometimes called a bring-your-own-PC program for employees and contractors.

Check-outs

When the View desktop is checked out, a snapshot is taken in vCenter, to preserve the state of the virtual machine. The vCenter Server version of the desktop is locked so that no other users can access it. When a View desktop is locked, vCenter Server operations are disabled, including operations such as powering on the online desktop, taking snapshots, and editing the virtual machine settings. View administrators can, however, still monitor the local session and access the vCenter Server version to remove access or roll back the desktop.

Backups

During backups, a snapshot is taken on the client system, to preserve the state of the checked-out virtual machine. The delta between this snapshot and the snapshot in vCenter is replicated to vCenter and merged with the snapshot there. The View desktop in vCenter Server is updated with all new data and configurations, but the local desktop remains checked out on the local system and the lock remains in place in vCenter Server.

Rollbacks

During rollbacks, the local View desktop is discarded and the lock is released in vCenter Server. Future client connections are directed to the View desktop in vCenter Server until the desktop is checked out again.

Check-ins

When a View desktop is checked in, a snapshot is taken on the client system, to preserve the state of the virtual machine. The delta between this snapshot and the snapshot in vCenter is replicated to vCenter and merged with the snapshot there. The virtual machine in vCenter Server is unlocked. Future client connections are directed to the View desktop in vCenter Server until the desktop is checked out again.

The data on each local system is encrypted with AES. 128-bit encryption is the default, but you can configure 192-bit or 256-bit encryption. The desktop has a lifetime controlled through policy. If the client loses contact with View Connection Server, the maximum time without server contact is the period in which the user can continue to use the desktop before the user is refused access. Similarly, if user access is removed, the client system becomes inaccessible when the cache expires or after the client detects this change through View Connection Server.

View Client with Local Mode has the following limitations and restrictions:

- You must have a View license that includes the Local Mode component.
- End users cannot access their local desktop while rollbacks and check-ins are taking place.
- This feature is available only for virtual machines that are managed by vCenter Server.
- Assigning application packages created with VMware ThinApp is not supported on local desktops.
- For security reasons, you cannot access the host CD-ROM from within the View desktop.
- Also for security reasons, you cannot copy and paste text or system objects such as files and folders between the local system and the View desktop.

Accessing USB Devices Connected to a Local Computer

Administrators can configure the ability to use USB devices, such as thumb flash drives, VoIP (voice-over-IP) devices, and printers, from a View desktop. This feature is called USB redirection.

When you use this feature, most USB devices that are attached to the local client system become available from a menu in View Client. You use the menu to connect and disconnect the devices.

USB devices that do not appear in the menu, but are available in a View desktop, include smart card readers and human interface devices such as keyboards and pointing devices. The View desktop and the local computer use these devices at the same time.

This feature has the following limitations:

- When you access a USB device from a menu in View Client and use the device in a View desktop, you cannot access the device on the local computer.
- USB redirection is not supported on Windows 2000 systems or for View desktops sourced from Microsoft Terminal Servers.

Printing from a View Desktop

The virtual printing feature allows end users with View Client on Windows systems to use local or network printers from a View desktop without requiring that additional print drivers be installed in the View desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and so on.

After a printer is added on the local Windows computer, View adds that printer to the list of available printers on the View desktop. No further configuration is required. Users who have administrator privileges can still install printer drivers on the View desktop without creating a conflict with the virtual printing component.

To send print jobs to a USB printer, you can either use the USB redirection feature or use the virtual printing feature.

In addition, the location-based printing capabilities as of View 4.5 allow IT organizations to map View desktops to the printer that is closest to the endpoint client device. For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer.

Streaming Multimedia to a View Desktop

Wyse MMR (multimedia redirection) enables full-fidelity playback when multimedia files are streamed to a View desktop.

The MMR feature supports the media file formats that the client system supports, because local decoders must exist on the client. File formats include MPEG2, WMV, AVI, and WAV, among others.

This feature has the following limitations:

- For best quality, use Windows Media Player 10 or later, and install it on both the local computer, or client access device, and the View desktop.
- The Wyse MMR port, which is 9427 by default, must be added as a firewall exception in the View desktop.
- MMR is not supported on Windows 7 clients or virtual desktops.

  Although MMR is not supported on Windows 7 virtual desktops, if the Windows 7 desktop has 1GB of RAM and 2 virtual CPUs, you can use PCoIP to play 480p- and 720p-formatted videos at native resolutions. For 1080p, you might need to make the window smaller than full screen size.

Using Single Sign-On for Logging In to a View Desktop

The single-sign-on (SSO) feature allows you to configure View Manager so that end users are prompted to log in only once.

If you do not use the single-sign-on feature, end users must log in twice. They are first prompted to log in to View Connection Server and then are prompted log in to their View desktop. If smart cards are also used, end users must sign in three times because users must also log in when the smart card reader prompts them for a PIN.

This feature includes the Graphical Identification and Authentication (GINA) dynamic-link library for Windows XP and a credential provider dynamic-link library for Windows Vista.

Using Multiple Monitors with a View Desktop

Regardless of the display protocol, you can use multiple monitors with a View desktop.

If you use PCoIP, the display protocol from VMware, you can adjust the display resolution and rotation separately for each monitor. PCoIP allows a true multiple-monitor session rather than a span mode session.

A span mode remote session is actually a single-monitor session. The monitors must be the same size and resolution, and the monitor layout must fit within a bounding box. If you maximize an application window, the window spans across all monitors.

In a true multiple-monitor session, monitors can have different resolutions and sizes, and a monitor can be pivoted. If you maximize an application window, the window expands to the full screen of only the monitor that contains it.

This feature has the following limitations:

- The maximum number of monitors that you can use to display a View desktop is 10 if you use the RDP display protocol and 4 if you use PCoIP.
- If you use Microsoft RDP display protocol, you must have Microsoft Remote Desktop Connection (RDC) 6.0 or higher installed in the View desktop.
- If you use a View desktop in local mode, no remote display protocol is used. You can use multiple monitors in span mode.

Managing Desktop Pools from a Central Location

3

You can create pools that include one or hundreds of virtual desktops. As a desktop source, you can use virtual machines, physical machines, and Windows Terminal Services servers. Create one virtual machine as a base image, and VMware View can generate a pool of virtual desktops from that image. You can easily install or stream applications to pools with VMware ThinApp.

This chapter includes the following topics:

Advantages of Desktop Pools

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

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

- A physical system such as a physical desktop PC or a Windows Terminal Services server
- A virtual machine that is hosted on an ESX/ESXi host and managed by vCenter Server
- A virtual machine that runs on VMware Server or some other virtualization platform that supports View Agent

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

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

- Specify which remote display protocol to use as the default for the View desktop and whether to let end users override the default.
- Configure the display quality and bandwidth throttling of Adobe Flash animations.
- If using a virtual machine, specify whether to power off the virtual machine when it is not in use and whether to delete it altogether.

- If using vSphere 4.1, specify whether to use a Microsoft Sysprep customization specification or QuickPrep from VMware. Sysprep generates a unique SID and GUID for each virtual machine in the pool.
- Specify whether the View desktop can or must be downloaded and run on a local client system.

In addition, using desktop pools provides many conveniences.

Dedicated-assignment pools

Each user is assigned a particular View desktop and returns to the same virtual desktop at each login. Users can personalize their desktops, install applications, and store data.

Floating-assignment pools

The virtual desktop is optionally deleted and re-created after each use, offering a highly controlled environment. A floating-assignment desktop is like a computer lab or kiosk environment where each desktop is loaded with the necessary applications and all desktops have access to necessary data.

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

Reducing and Managing Storage Requirements

Using virtual desktops that are managed by vCenter Server provides all the storage efficiencies that were previously available only for virtualized servers. Using View Composer increases the storage savings because all desktops in a pool share a virtual disk with a base image.

- Managing Storage with vSphere on page 24

  VMware vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

- Reducing Storage Requirements with View Composer on page 25

  Because View Composer creates desktop images that share virtual disks with a base image, you can reduce the required storage capacity by 50 to 90 percent.

Managing Storage with vSphere

VMware vSphere lets you virtualize disk volumes and file systems so that you can manage and configure storage without having to consider where the data is physically stored.

Fibre Channel SAN arrays, iSCSI SAN arrays, and NAS arrays are widely used storage technologies supported by VMware vSphere to meet different datacenter storage needs. The storage arrays are connected to and shared between groups of servers through storage area networks. This arrangement allows aggregation of the storage resources and provides more flexibility in provisioning them to virtual machines.

With View 4.5 and later and vSphere 4.1 and later, you can now also use the following features:

- vStorage thin provisioning, which lets you start out with as little disk space as necessary and grow the disk to add space later
- Tiered storage, which allows you to distribute virtual disks in the View environment across high-performance storage and lower-cost storage tiers, to maximize performance and cost savings
- Local storage on the ESX/ESXi host for the virtual machine swap files in the guest operating system

Reducing Storage Requirements with View Composer

Because View Composer creates desktop images that share virtual disks with a base image, you can reduce the required storage capacity by 50 to 90 percent.

View Composer uses a base image, or parent virtual machine, and creates a pool of up to 512 linked-clone virtual machines. Each linked clone acts like an independent desktop, with a unique host name and IP address, yet the linked clone requires significantly less storage.

When you create a linked-clone desktop pool, a full clone is first made from the parent virtual machine. The full clone, or replica, and the clones linked to it can be placed on the same data store, or LUN (logical unit number). If necessary, you can use the rebalance feature to move the replica and linked clones from one LUN to another.

Alternatively, you can place View Composer replicas and linked clones on separate datastores with different performance characteristics. For example, you can store the replica virtual machines on a solid-state drive (SSD). Solid-state drives have low storage capacity and high read performance, typically supporting tens of thousands of I/Os per second (IOPS). You can store linked clones on traditional, spinning media-backed datastores. These disks provide lower performance, but are less expensive and provide higher storage capacity, which makes them suited for storing the many linked clones in a large pool. Tiered storage configurations can be used to cost-effectively handle intensive I/O scenarios such as simultaneous rebooting of many virtual machines or running scheduled antivirus scans.

When you create a linked-clone pool, you can also optionally configure a separate, disposable virtual disk to store the guest operating system's paging and temp files that are generated during user sessions. When the virtual machine is powered off, View Manager deletes the disposable disk. Using disposable disks can save storage space by slowing the growth of linked clones and reducing the space used by powered off virtual machines.

When you create dedicated-assignment desktop pools, View Composer can also optionally create a separate persistent virtual disk for each virtual desktop. The end user's Windows profile and application data are saved on the persistent disk. When a linked clone is refreshed, recomposed, or rebalanced, the contents of the persistent virtual disk are preserved. VMware recommends that you keep View Composer persistent disks on a separate datastore. You can then back up the whole LUN that holds persistent disks.

For more information, see the best-practices guide called *Storage Considerations for VMware View.*

Application Provisioning

With VMware View, you have several options regarding application provisioning: You can use traditional application provisioning techniques, you can distribute application packages created with VMware ThinApp, or you can deploy applications as part of a View Composer base image.

- Deploying Applications and System Updates with View Composer on page 26

  Because linked-clone desktop pools share a base image, you can quickly deploy updates and patches by updating the parent virtual machine.

- Managing VMware ThinApp Applications in View Administrator on page 26

  VMware ThinApp™ lets you package an application into a single file that runs in a virtualized application sandbox. This strategy results in flexible, conflict-free application provisioning.

- Using Existing Processes for Application Provisioning on page 27

  With VMware View, you can continue to use the application provisioning techniques that your company currently uses. Two additional considerations include managing server CPU usage and storage I/O and determining whether users are permitted to install applications.

Deploying Applications and System Updates with View Composer

Because linked-clone desktop pools share a base image, you can quickly deploy updates and patches by updating the parent virtual machine.

The recompose feature allows you to make changes to the parent virtual machine, take a snapshot of the new state, and push the new version of the image to all, or a subset of, users and desktops. You can use this feature for the following tasks:

- Applying operating system and software patches and upgrades
- Applying service packs
- Adding applications
- Adding virtual devices
- Changing other virtual machine settings, such as available memory

You can create a View Composer persistent disk that contains user settings and other user-generated data. This persistent disk is not affected by a recompose operation. When a linked clone is deleted, you can preserve the user data. When an employee leaves the company, another employee can access the departing employee's user data. A user who has multiple desktops can consolidate the user data on a single desktop.

If you want to disallow users from adding or removing software or changing settings, you can use the refresh feature to bring the desktop back to its default values. This feature also reduces the size of linked clones, which tend to grow over time.

Managing VMware ThinApp Applications in View Administrator

VMware ThinApp™ lets you package an application into a single file that runs in a virtualized application sandbox. This strategy results in flexible, conflict-free application provisioning.

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package. As of View 4.5, you can use View Administrator to distribute ThinApp applications to desktops and pools.

After you create a virtualized application with ThinApp, you can choose to either stream the application from a shared file server or install the application on the virtual desktops. If you configure the virtualized application for streaming, you must address the following architectural considerations:

- Access for specific user groups to specific application repositories, where the application package is stored
- Storage configuration for the application repository
- Network traffic generated by streaming, which depends largely on the type of application

For streamed applications, users launch the applications by using a desktop shortcut.

If you assign a ThinApp package so that it is installed on a virtual desktop, the architectural considerations are similar to those that you address when you use traditional MSI-based software provisioning. Storage configuration for the application repository is a consideration both for streamed applications and for ThinApp packages installed in virtual desktops.

NOTE Assigning application packages created with VMware ThinApp is not supported for View desktops that are downloaded and used in local mode.

Using Existing Processes for Application Provisioning

With VMware View, you can continue to use the application provisioning techniques that your company currently uses. Two additional considerations include managing server CPU usage and storage I/O and determining whether users are permitted to install applications.

If you push applications out to large numbers of virtual desktops at exactly the same time, you might see significant spikes in CPU usage and storage I/O. These peak workloads can have noticeable effects on desktop performance. As a best practice, schedule application updates to occur during off-peak hours and stagger updates to desktops if possible. You must also verify that your storage solution is designed to support such workloads.

If your company allows users to install applications, you can continue your current policies, but you cannot take advantage of View Composer features such as refreshing and recomposing the desktop. With View Composer, if an application is not virtualized or otherwise included in the user's profile or data settings, that application is discarded whenever a View Composer refresh, recompose, or rebalance operation occurs. In many cases, this ability to tightly control which applications are installed is a benefit. View Composer desktops are easy to support because they are kept close to a known good configuration.

If users have firm requirements for installing their own applications and having those applications persist for the lifetime of the virtual desktop, instead of using View Composer for application provisioning, you can create full persistent desktops and allow users to install applications.

Using Active Directory GPOs to Manage Users and Desktops

VMware View includes many Group Policy administrative (ADM) templates for centralizing the management and configuration of View components and View desktops.

After you import these templates into Active Directory, you can use them to set policies that apply to the following groups and components:

- All systems regardless of which user logs in
- All users regardless of the system they log in to
- View Connection Server configuration
- View Client configuration
- View Agent configuration

After a GPO is applied, properties are stored in the local Windows registry of the specified component.

You can use GPOs to set all the policies that are available from the View Administrator user interface (UI). You can also use GPOs to set policies that are not available from the UI. For a complete list and description of the settings available through ADM templates, see the *VMware View Administration* document.

Architecture Design Elements and Planning Guidelines

4

A typical VMware View architecture design uses a building block strategy to achieve scalability. Each building block definition can vary, based on hardware configuration, View and vSphere software versions used, and other environment-specific design factors.

This chapter describes a validated example building block that consists of components that support up to 2,000 virtual desktops using vSphere 4.1. The overall deployment integrates 5 of these building blocks for a total of 10,000 virtual desktops in what is termed a "pod."

This architecture provides a standard, scalable design that you can adapt to your enterprise environment and special requirements. This chapter includes key details about requirements for memory, CPU, storage capacity, network components, and hardware to give IT architects and planners a practical understanding of what is involved in deploying a VMware View solution.

This chapter includes the following topics:

Virtual Machine Requirements

When you plan the specifications for View desktops, the choices that you make regarding RAM, CPU, and disk space have a significant effect on your choices for server and storage hardware and expenditures.

- Estimating Memory Requirements for Virtual Desktops on page 31

  RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs and total storage capacity needed, determining the correct memory allocation is crucial to planning your desktop deployment.

- Estimating CPU Requirements for Virtual Desktops on page 33

  When estimating CPU, you must gather information about the average CPU utilization for various types of workers in your enterprise. In addition, calculate that another 10 to 25 percent of processing power is required for virtualization overhead and peak periods of usage.

- Choosing the Appropriate System Disk Size on page 33

  When allocating disk space, provide only enough space for the operating system, applications, and additional content that users might install or generate. Usually this amount is smaller than the size of the disk that is included on a physical PC.

Planning Based on Types of Workers

For many configuration elements, including RAM, CPU, and storage sizing, requirements depend largely on the type of worker who uses the virtual desktop and on the applications that must be installed.

For architecture planning, workers can be categorized into several types.

Task workers	Task workers and administrative workers perform repetitive tasks within a small set of applications, usually at a stationary computer. The applications are usually not as CPU- and memory-intensive as the applications used by knowledge workers. Task workers who work specific shifts might all log in to their virtual desktops at the same time. Task workers include call center analysts, retail employees, warehouse workers, and so on.
Knowledge workers	Knowledge workers' daily tasks include accessing the Internet, using email, and creating complex documents, presentations, and spreadsheets. Knowledge workers include accountants, sales managers, marketing research analysts, and so on.
Power users	Power users include application developers and people who use graphics-intensive applications.
Employees who use desktops in local mode only	These users download and run their View desktops only on their local systems, which reduces datacenter costs associated with bandwidth, memory, and CPU resources. Scheduled replications ensure that systems and data are backed up. Administrators configure how often end users' systems must contact View Manager to avoid being locked out.
Kiosk users	These users need to share a desktop that is placed in a public place. Examples of kiosk users include students using a shared computer in a classroom, nurses at nursing stations, and computers used for job placement and recruiting. These desktops require automatic login. Authentication can be done through certain applications if necessary.

Estimating Memory Requirements for Virtual Desktops

RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs and total storage capacity needed, determining the correct memory allocation is crucial to planning your desktop deployment.

If the RAM allocation is too low, storage I/O can be negatively affected because too much memory swapping occurs. If the RAM allocation is too high, storage capacity can be negatively affected because the paging file in the guest operating system and the swap and suspend files for each virtual machine grow too large.

NOTE This topic addresses issues regarding memory allocation for remote access to View desktops. If users run View desktops in local mode, on their client systems, the amount of memory used is some proportion of that available on the client device.

You need enough memory to run the host operating system on the client computer, plus the memory required for the View desktop's operating system and for applications on the client computer and the View desktop. VMware recommends that you have 2GB or more for Windows XP and Windows Vista, and 3GB or more for Windows 7.

If you attempt to check out a desktop that is configured in vCenter Server to require more memory than the local client system can accommodate, you will not be able to check out the desktop unless you change a Windows registry setting. For instructions, see the *VMware View Administration* document.

RAM Sizing Impact on Performance

When allocating RAM, avoid choosing an overly conservative setting. Take the following considerations into account:

- Insufficient RAM allocations can cause excessive guest swapping, which can generate I/O that causes significant performance degradations and increases storage I/O load.
- VMware ESX/ESXi supports sophisticated memory resource management algorithms such as transparent memory sharing and memory ballooning, which can significantly reduce the physical RAM needed to support a given guest RAM allocation. For example, even though 2GB might be allocated to a virtual desktop, only a fraction of that number is consumed in physical RAM.
- Because virtual desktop performance is sensitive to response times, on the ESX/ESXi host, set nonzero values for RAM reservation settings. Reserving some RAM guarantees that idle but in-use desktops are never completely swapped out to disk. It can also reduce storage space consumed by ESX/ESXi swap files. However, higher reservation settings affect your ability to overcommit memory on an ESX/ESXi host and might affect VMotion maintenance operations.

RAM Sizing Impact on Storage

The amount of RAM that you allocate to a virtual machine is directly related to the size of the certain files that the virtual machine uses. To access the files in the following list, use the Windows guest operating system to locate the Windows page and hibernate files, and use the ESX/ESXi host's file system to locate the ESX/ESXi swap and suspend files.

Windows page file By default, this file is sized at 150 percent of guest RAM. This file, which is by default located at `C:\pagefile.sys`, causes thin-provisioned storage to grow because it is accessed frequently. On linked-clone virtual machines, the page file and temporary files can be redirected to a separate virtual disk that is

deleted when the virtual machines are powered off. Disposable page-file redirection saves storage, slowing the growth of linked clones and also can improve performance. Although you can adjust the size from within Windows, doing so might have a negative effect on application performance.

Windows hibernate file for laptops This file can equal 100 percent of guest RAM. You can safely delete this file because it is not needed in View deployments, even if you use View Client with Local Mode.

ESX/ESXi swap file This file, which has a `.vswp` extension, is created if you reserve less than 100 percent of a virtual machine's RAM. The size of the swap file is equal to the unreserved portion of guest RAM. For example, if 50 percent of guest RAM is reserved and guest RAM is 2GB, the ESX/ESXi swap file is 1GB. This file can be stored on the local datastore on the ESX/ESXi host or cluster.

ESX/ESXi suspend file This file, which has a `.vmss` extension, is created if you set the desktop pool logoff policy so that the virtual desktop is suspended when the end user logs off. The size of this file is equal to the size of guest RAM.

RAM Sizing for Specific Monitor Configurations When Using PCoIP

If you use PCoIP, the display protocol from VMware, the amount of extra RAM that the ESX/ESXi host requires depends in part on the number of monitors configured for end users and on the display resolution. Table 4-1 lists the amount of overhead RAM required for various configurations. The amounts of memory listed in the columns are in addition to the amount of memory required for other PCoIP functionality.

Table 4-1. PCoIP Client Display Overhead

Display Resolution Standard	Width, in Pixels	Height, in Pixels	1-Monitor Overhead	2-Monitor Overhead	4-Monitor Overhead
VGA	640	480	2.34MB	4.69MB	9.38MB
SVGA	800	600	3.66MB	7.32MB	14.65MB
720p	1280	720	7.03MB	14.65MB	28.13MB
UXGA	1600	1200	14.65MB	29.30MB	58.59MB
1080p	1920	1080	15.82MB	31.64MB	63.28MB
WUXGA	1920	1200	17.58MB	35.16MB	70.31MB
QXGA	2048	1536	24.00MB	48.00MB	96.00MB
WQXGA	2560	1600	31.25MB	62.50MB	125.00MB

When you consider these requirements, note that virtual machine configuration of allocated RAM does not change. That is, you do not need to allocate 1GB of RAM for applications and another 31MB for dual 1080p monitors. Instead, consider the overhead RAM when calculating the total physical RAM required for each ESX/ESXi host. Add the guest operating system RAM to the overhead RAM and multiply by the number of virtual machines.

RAM Sizing for Specific Workloads and Operating Systems

Because the amount of RAM required can vary widely, depending on the type of worker, many companies conduct a pilot phase to determine the correct setting for various pools of workers in their enterprise.

A good starting point is to allocate 1GB for Windows XP desktops and 32-bit Windows Vista and Windows 7 desktops and 2GB for 64-bit Windows 7 desktops. During a pilot, monitor the performance and disk space used with various types of workers and make adjustments until you find the optimal setting for each pool of workers.

Estimating CPU Requirements for Virtual Desktops

When estimating CPU, you must gather information about the average CPU utilization for various types of workers in your enterprise. In addition, calculate that another 10 to 25 percent of processing power is required for virtualization overhead and peak periods of usage.

NOTE This topic addresses issues regarding CPU requirements when accessing View desktops remotely. If users run a View desktop in local mode on their client systems, the View desktop uses the available CPUs on the client device, up to 2 CPUs.

CPU requirements vary by worker type. During your pilot phase, use a performance monitoring tool, such as Perfmon in the virtual machine, `esxtop` in ESX/ESXi, or vCenter performance monitoring tools, to understand both the average and peak CPU use levels for these groups of workers. Also use the following guidelines:

- Software developers or other power uses with high-performance needs might have much higher CPU requirements than knowledge workers and task workers. Dual virtual CPUs are recommended for compute-intensive tasks or for Windows 7 desktops that need to play 720p video using the PCoIP display protocol.
- Single virtual CPUs are generally recommended for other cases.

Because many virtual machines run on one server, CPU can spike if agents such as antivirus agents all check for updates at exactly the same time. Determine which agents and how many agents could cause performance issues and adopt a strategy for addressing these issues. For example, the following strategies might be helpful in your enterprise:

- Use View Composer to update images rather than having software management agents download software updates to each individual virtual desktop.
- Schedule antivirus and software updates to run at nonpeak hours, when few users are likely to be logged in.
- Stagger or randomize when updates occur.

As an informal initial sizing approach, to start, assume that each virtual machine requires 1/8 to 1/10 of a CPU core as the minimum guaranteed compute power. That is, plan a pilot that uses 8 to 10 virtual machines per core. For example, if you assume 8 virtual machines per core and have a 2-socket 8-core ESX/ESXi host, you can host 128 virtual machines on the server during the pilot. Monitor the overall CPU usage on the host during this period and ensure that it rarely exceeds a safety margin such as 80 percent to give enough headroom for spikes.

Choosing the Appropriate System Disk Size

When allocating disk space, provide only enough space for the operating system, applications, and additional content that users might install or generate. Usually this amount is smaller than the size of the disk that is included on a physical PC.

Because datacenter disk space usually costs more per gigabyte than desktop or laptop disk space in a traditional PC deployment, optimize the operating system image size. The following suggestions might help optimize image size:

- Remove unnecessary files. For example, reduce the quotas on temporary Internet files.
- Choose a virtual disk size that is sufficient to allow for future growth, but is not unrealistically large.
- Use centralized file shares or a View Composer persistent disk for user-generated content and user-installed applications.

The amount of storage space required must take into account the following files for each virtual desktop:

- The ESX/ESXi suspend file is equivalent to the amount of RAM allocated to the virtual machine.
- The Windows page file is equivalent to 150 percent of RAM.
- Log files take up approximately 100MB for each virtual machine.
- The virtual disk, or `.vmdk` file, must accommodate the operating system, applications, and future applications and software updates. The virtual disk must also accommodate local user data and user-installed applications if they are located on the virtual desktop rather than on file shares.

  If you use View Composer, the `.vmdk` files grow over time, but you can control the amount of growth by scheduling View Composer refresh operations, setting a storage over-commit policy for View desktop pools, and redirecting Windows page and temporary files to a separate, nonpersistent disk.

You can also add 15 percent to this estimate to be sure that users do not run out of disk space.

VMware View ESX/ESXi Node

A node is a single VMware ESX/ESXi host that hosts virtual machine desktops in a VMware View deployment.

VMware View is most cost-effective when you maximize the consolidation ratio, which is the number of desktops hosted on an ESX/ESXi host. Although many factors affect server selection, if you are optimizing strictly for acquisition price, you must find server configurations that have an appropriate balance of processing power and memory.

There is no substitute for measuring performance under actual, real world scenarios, such as in a pilot, to determine an appropriate consolidation ratio for your environment and hardware configuration. Consolidation ratios can vary significantly, based on usage patterns and environmental factors. Use the following guidelines:

- As a general framework, consider compute capacity in terms of 8 to 10 virtual desktops per CPU core. For information about calculating CPU requirements for each virtual machine, see "Estimating CPU Requirements for Virtual Desktops," on page 33.
- Think of memory capacity in terms of virtual desktop RAM, host RAM, and overcommit ratio. Although you can have between 8 and 10 virtual desktops per CPU core, if virtual desktops have 1GB or more of RAM, you must also carefully consider physical RAM requirements. For information about calculating the amount of RAM required per virtual machine, see "Estimating Memory Requirements for Virtual Desktops," on page 31.

  Note that physical RAM costs are not linear and that in some situations, it can be cost-effective to purchase more smaller servers that do not use expensive DIMM chips. In other cases, rack density, storage connectivity, manageability and other considerations can make minimizing the number of servers in a deployment a better choice.
- Finally, consider cluster requirements and any failover requirements. For more information, see "Determining Requirements for High Availability," on page 42.

For information about specifications of ESX/ESXi hosts in vSphere, see the *VMware vSphere Configuration Maximums* document.

Desktop Pools for Specific Types of Workers

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

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

Stateless desktop images Stateless architectures have many advantages, such as being easier to support, allowing View Composer based image management, and having lower storage costs. Other benefits include a limited need to back up the linked-clone virtual machines and easier, less expensive disaster recovery and business continuity options.

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

You create stateless desktop images by using View Composer and creating floating-assignment pools of linked-clone virtual machines. You create stateful desktop images by creating dedicated-assignment pools of full virtual machines. Some storage vendors have cost-effective storage solutions for stateful desktop images. These vendors often have their own best practices and provisioning utilities. Using one of these vendors might require that you create a manual dedicated-assignment pool.

- Pools for Task Workers on page 36

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

- Pools for Knowledge Workers and Power Users on page 36

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

- Pools for Mobile Users on page 37

  These users can check out a View desktop and run it locally on their laptop or desktop even without a network connection.

- Pools for Kiosk Users on page 38

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

Pools for Task Workers

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

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

- Create an automated pool so that desktops can be created when the pool is created or can be generated on demand based on pool usage.
- Use floating assignment so that users log in to any available desktop. This setting reduces the number of desktops required if everyone does not need to be logged in at the same time.
- Create View Composer linked-clone desktops so that desktops share the same base image and use less storage space in the datacenter than full virtual machines.
- Determine what action, if any, to take when users log off. Disks grow over time. You can conserve disk space by refreshing the desktop to its original state when users log off. You can also set a schedule for periodically refreshing desktops. For example, you can schedule desktops to refresh daily, weekly, or monthly.

Pools for Knowledge Workers and Power Users

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

Because power users and knowledge workers, such as accountants, sales managers, marketing research analysts, need to be able to create and retain documents and settings, you create dedicated-assignment desktops for them. For knowledge workers do not need user-installed applications except for temporary use, you can create stateless desktop images and save all their personal data outside of the virtual machine, on a file server or in an application database. For other knowledge workers and for power users, you can create stateful desktop images. Use the following pool settings:

- Use dedicated assignment so that each knowledge worker or power user logs in to the same desktop every time.
- Use vStorage thin provisioning so that at first, each desktop uses only as much storage space as the disk needs for its initial operation.
- If knowledge workers do not need user-installed applications except for temporary use, you can create View Composer linked-clone desktops. These stateless desktop images share the same base image and use less storage space than full virtual machines.
- If you use View Composer linked-clone desktops, either implement a roaming or virtual profile based solution to store user data centrally or configure a persistent disk for the desktop. Keep in mind, however, that after you refresh or recompose a desktop, the centrally stored data and persistent disk are retained, but the disk that contains the operating system and applications is not retained.
- For power users and knowledge workers who need to install their own applications, which adds data to the operating system disk, create full virtual machine desktops. These users need stateful desktop images.

Pools for Mobile Users

These users can check out a View desktop and run it locally on their laptop or desktop even without a network connection.

View Client with Local Mode provides benefits for both end users and IT administrators. For administrators, local mode allows View security policies to extend to laptops that have previously been unmanaged. Administrators can retain tight control over the applications that run on the View desktop and can centrally manage the desktop just as they do remote View desktops. With local mode, all the benefits of VMware View can also extend to remote or branch offices that have slow or unreliable networks.

For end users, benefits include the flexibility of continuing to use their own computers online or offline. The View desktop is automatically encrypted and can easily be synchronized with an image in the datacenter for purposes of disaster recovery.

General Recommendations

Local mode users might need to access their desktop applications and data from their laptop when no network connection is available. In addition, they might need this data to be regularly and automatically backed up to the datacenter in the event that the laptop is ever lost, damaged, or stolen. To provide these capabilities, you can use the following pool settings.

- When creating a virtual machine to base the pool on, configure the minimum amount of RAM and virtual CPUs required by the guest operating system. Desktops that run in local mode adjust the amount of memory and processing power they use based on that available from the client computer.
- Create an automated pool so that desktops can be created when the pool is created or can be generated on demand based on pool usage.
- Use dedicated assignment because local mode users need to log in to the same desktop every time.
- Create View Composer linked-clone desktops so that desktops share the same base image and use less storage space in the datacenter than full virtual machines.
- If you want the provisioning process to generate a unique local computer SID and GUID for each linked clone in the pool, select a Sysprep customization specification when you create the pool. Sysprep creates new SIDs and GUIDs during the initial provisioning and after recompose operations. Because you are not likely to recompose local mode pools, the SIDs and GUIDs are not likely to change.
- Include in the pool only desktops that are intended to be used in local mode. Local mode virtual machines can be placed on datastores with lower IOPS requirements than storage intended to support large numbers of remote View desktops.

Additional Recommendations Targeting Minimal Capital Expenditure

You can reduce the number of ESX/ESXi hosts required for your local mode pool if you increase the number of virtual machines per ESX/ESXi host. An ESX/ESXi 4.1 host can accommodate up to 500 virtual machines if most are not powered on at the same time, as is frequently the case for local mode pools.

Use the following recommendations to reduce the amount of bandwidth and I/O operations required by each virtual machine and maximize the number of virtual machines on an ESX/ESXi host.

- Set a View policy so that end users must use their View desktops in local mode only. With this setting, the virtual machines in the datacenter remain locked and powered off.
- Set local mode policies so that end users cannot initiate desktop rollbacks, data backups, or check-ins to the datacenter.
- Do not schedule automatic backups.

- Do not turn on SSL for provisioning or downloading local mode desktops.
- If the performance of View Connection Server is affected by the number of local desktops, set the heartbeat interval to be less frequent. The heartbeat lets View Connection Server know that the local desktop has a network connection. The default interval is five minutes.

Pools for Kiosk Users

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

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

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

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

- Create an automated pool so that desktops can be created when the pool is created or can be generated on demand based on pool usage.
- Use floating assignment so that users can access any available desktop in the pool.
- Create View Composer linked-clone desktops so that desktops share the same base image and use less storage space in the datacenter than full virtual machines.
- Institute a refresh policy so that the desktop is refreshed frequently, such as at every user logoff.
- Use an Active Directory GPO (group policy object) to configure location-based printing, so that the desktop uses the nearest printer. For a complete list and description of the settings available through Group Policy administrative (ADM) templates, see the *VMware View Administration* document.
- Use a GPO if you want to override the default policy that enables connecting local USB devices to the desktop when the desktop is launched or when USB devices are plugged in to the client computer.

Desktop Virtual Machine Configuration

Because the amount of RAM, CPU, and disk space that virtual desktops require depend on the guest operating system, separate configuration examples are provided for Windows XP, Windows Vista, and Windows 7 virtual desktops.

The example settings for virtual machines such as memory, number of virtual processors, and disk space are VMware View-specific.

The guidelines listed in Table 4-2 are for a standard Windows XP virtual desktop running in remote mode.

Table 4-2. Desktop Virtual Machine Example for Windows XP

Item	Example
Operating system	32-bit Windows XP (with the latest service pack)
RAM	1GB (512MB low end, 2GB high end)
Virtual CPU	1
System disk capacity	16GB (8GB low end, 40GB high end)
User data capacity (as a persistent disk)	5GB (starting point)
Virtual SCSI adapter type	LSI Logic Parallel (not the default)
Virtual network adapter	Flexible (the default)

The amount of system disk space required depends on the number of applications required in the base image. VMware has validated a setup that included 8GB of disk space. Applications included Microsoft Word, Excel, PowerPoint, Adobe Reader, Internet Explorer, McAfee Antivirus, and PKZIP.

The amount of disk space required for user data depends on the role of the end user and organizational policies for data storage. If you use View Composer, this data is kept on a persistent disk.

The guidelines listed in Table 4-3 are for a standard Windows Vista virtual desktop running in remote mode.

Table 4-3. Desktop Virtual Machine Example for Windows Vista

Item	Example
Operating system	32-bit Windows Vista (with the latest service pack)
RAM	1GB
Virtual CPU	1
System disk capacity	20GB (standard)
User data capacity (as a persistent disk)	5GB (starting point)
Virtual SCSI adapter type	LSI Logic Parallel (the default)
Virtual network adapter	E1000 (the default)

The guidelines listed in Table 4-4 are for a standard Windows 7 virtual desktop running in remote mode.

Table 4-4. Desktop Virtual Machine Example for Windows 7, on an ESX/ESXi 4.1 Host

Item	Example
Operating system	32-bit Windows 7
RAM	1GB
Virtual CPU	1
System disk capacity	20GB (slightly less than standard)
User data capacity (as a persistent disk)	5GB (starting point)
Virtual SCSI adapter type	LSI Logic SAS (the default)
Virtual network adapter	E1000 (the default)

vCenter and View Composer Virtual Machine Configuration and Desktop Pool Maximums

You install both vCenter Server and View Composer on the same virtual machine. Because this virtual machine is a server, it requires much more memory and processing power than a desktop virtual machine.

View Composer can create and provision up to 512 desktops per pool. View Composer can also perform a recompose operation on up to 512 desktops at a time.

Although you can install vCenter Server and View Composer on a physical machine, this example uses a virtual machine with the specifications listed in Table 4-5. The ESX/ESXi host for this virtual machine can be part of a VMware HA cluster to guard against physical server failures.

This example assumes that you are using VMware View with vSphere 4.1 and vCenter Server 4.1.

Table 4-5. vCenter Server Virtual Machine Example and Pool Size Maximum

Item	Example
Operating system	64-bit Windows Server 2008 R2 Enterprise
RAM	4 GB
Virtual CPU	2
System disk capacity	40GB
Virtual SCSI adapter type	LSI Logic SAS (the default for Windows Server 2008)
Virtual network adapter	E1000 (the default)
Maximum View Composer pool size	512 desktops

IMPORTANT Place the database to which vCenter and View Composer connect on a separate virtual machine. For guidance about database sizing, see the *vCenter Server 4.x Database Sizing Calculator for Microsoft SQL Server* at http://www.vmware.com/support/vsphere4/doc/vsp_4x_db_calculator.xls.

View Connection Server Maximums and Virtual Machine Configuration

When you install View Connection Server, the View Administrator user interface is also installed. This server requires more memory and processing resources than a vCenter Server instance.

View Connection Server Configuration

Although you can install View Connection Server on a physical machine, this example uses a virtual machine with the specifications listed in Table 4-6. The ESX/ESXi host for this virtual machine can be part of a VMware HA cluster to guard against physical server failures.

Table 4-6. Connection Server Virtual Machine Example

Item	Example
Operating system	64-bit Windows Server 2008 R2
RAM	10GB
Virtual CPU	4
System disk capacity	40GB
Virtual SCSI adapter type	LSI Logic SAS (the default for Windows Server 2008)
Virtual network adapter	E1000 (the default)
1 NIC	1 Gigabit

View Connection Server Cluster Design Considerations

You can deploy multiple replicated View Connection Server instances in a group to support load balancing and high availability. Groups of replicated instances are designed to support clustering within a LAN-connected single-datacenter environment. VMware does not recommend using a group of replicated View Connection Server instances across a WAN due to the communication traffic needed between the grouped instances. In scenarios where a View deployment needs to span datacenters, create a separate View deployment for each datacenter.

Maximum Connections for View Connection Server

Table 4-7 provides information about the tested limits regarding the number of simultaneous connections that a VMware View deployment can accommodate.

This example assumes that you are using VMware View with vSphere 4.1 and vCenter Server 4.1. It also assumes that View Connection Server is running on a 64-bit Windows Server 2008 R2 Enterprise operating system.

Table 4-7. View Desktop Connections

Connection Servers per Deployment	Connection Type	Maximum Simultaneous Connections
1 Connection Server	Direct connection, RDP or PCoIP; Tunneled connection, RDP; PCoIP Secure Gateway connection	2,000
7 Connection Servers (5 + 2 spares)	Direct connection, RDP or PCoIP	10,000
1 Connection Server	Unified Access to physical PCs	100
1 Connection Server	Unified Access to terminal servers	200

PCoIP Secure Gateway connections are required if you use security servers for PCoIP connections from outside the corporate network. Tunneled connections are required if you use security servers for RDP connections from outside the corporate network and for USB and multimedia redirection (MMR) acceleration with a PCoIP Secure Gateway connection.

View Transfer Server Virtual Machine Configuration and Storage

View Transfer Server is required to support desktops that run View Client with Local Mode (formerly called Offline Desktop). This server requires less memory than View Connection Server.

View Transfer Server Configuration

You must install View Transfer Server on a virtual rather than a physical machine and the virtual machine must be managed by the same vCenter Server instance as the local desktops that it will manage. Table 4-8 lists the virtual machine specifications for a View Transfer Server instance.

Table 4-8. View Transfer Server Virtual Machine Example

Item	Example
Operating system	64-bit Windows Server 2008 R2
RAM	4GB
Virtual CPU	2
System disk capacity	20GB
Virtual SCSI adapter type	LSI Logic Parallel (not the default, which is SAS)

Table 4-8. View Transfer Server Virtual Machine Example (Continued)

Item	Example
Virtual network adapter	E1000 (the default)
1 NIC	1 Gigabit

Storage and Bandwidth Requirements for View Transfer Server

Several operations use View Transfer Server to send data between the View desktop in vCenter Server and the corresponding local desktop on the client system. When a user checks in or checks out a desktop, View Transfer Server transfers the files between the datacenter and the local desktop. View Transfer Server also synchronizes local desktops with the corresponding desktops in the datacenter by replicating user-generated changes to the datacenter.

If you use View Composer linked-clones for local desktops, 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. The faster your network storage disks are, the better performance will be. For information about determining the size of base image files, see the *VMware View Administration* document.

Each Transfer Server instance can theoretically accommodate 60 concurrent disk operations, although network bandwidth will likely be saturated at a lower number. VMware tested 20 concurrent disk operations, such as 20 clients downloading a local desktop at the same time, over a 1GB per second network connection.

vSphere Clusters

VMware View deployments can use VMware HA clusters to guard against physical server failures. Because of View Composer limitations, the cluster must contain no more than 8 servers, or nodes.

VMware vSphere and vCenter provide a rich set of features for managing clusters of servers that host View desktops. The cluster configuration is also important because each View desktop pool must be associated with a vCenter resource pool. Therefore, the maximum number of desktops per pool is related to the number of servers and virtual machines that you plan to run per cluster.

In very large VMware View deployments, vCenter performance and responsiveness can be improved by having only one cluster object per datacenter object, which is not the default behavior. By default, VMware vCenter creates new clusters within the same datacenter object.

Determining Requirements for High Availability

VMware vSphere, through its efficiency and resource management, lets you achieve industry-leading levels of virtual machines per server. But achieving a higher density of virtual machines per server means that more users are affected if a server fails.

Requirements for high availability can differ substantially based on the purpose of the desktop pool. For example, a stateless desktop image (floating-assignment) pool might have different recovery point objective (RPO) requirements than a stateful desktop image (dedicated-assignment) pool. For a floating-assignment pool, an acceptable solution might be to have users log in to a different desktop if the desktop they are using becomes unavailable.

In cases where availability requirements are high, proper configuration of VMware HA is essential. If you use VMware HA and are planning for a fixed number of desktops per server, run each server at a reduced capacity. If a server fails, the capacity of desktops per server is not exceeded when the desktops are restarted on a different host.

For example, in an 8-host cluster, where each host is capable of running 128 desktops, and the goal is to tolerate a single server failure, make sure that no more than 128 * (8 - 1) = 896 desktops are running on that cluster. You can also use VMware DRS (Distributed Resource Scheduler) to help balance the desktops among all 8 hosts. You get full use of the extra server capacity without letting any hot-spare resources sit idle. Additionally, DRS can help rebalance the cluster after a failed server is restored to service.

You must also make sure that storage is properly configured to support the I/O load that results from many virtual machines restarting at once in response to a server failure. Storage IOPS has the most effect on how quickly desktops recover from a server failure.

Example: Cluster Configuration Example

The settings listed in Table 4-9 are VMware View-specific. For information about limits of HA clusters in vSphere, see the *VMware vSphere Configuration Maximums* document.

Table 4-9. HA Cluster Example

Item	Example
Nodes (ESX/ESXi hosts)	8 (including 1 hot spare)
Cluster type	DRS (Distributed Resource Scheduler)/HA
Networking component	Standard ESX/ESXi 4.1 cluster network
Switch ports	80

Networking requirements depend on the type of server, the number of network adapters, and the way in which vMotion is configured.

VMware View Building Blocks

A 2,000-user building block consists of physical servers, a VMware vSphere infrastructure, VMware View servers, shared storage, and 2,000 virtual machine desktops. You can include up to five building blocks in a View pod.

Table 4-10. Example of a LAN-Based View Building Block

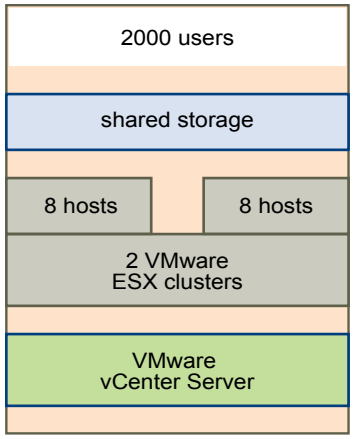
Item	Example
vSphere clusters	2 or more (with up to 8 ESX/ESXi hosts in each cluster)
80-port network switch	1
Shared storage system	1
vCenter Server with View Composer	1 (can be run in the block itself)
Database	MS SQL Server or Oracle database server (can be run in the block itself)
VLANs	3 (a 1Gbit Ethernet network for each: management network, storage network, and VMotion network)

With vCenter 4.1, which has a limit of 10,000 virtual machines per vCenter, you might be able to use vCenter Servers that manage virtual desktops in multiple building blocks. At the time this document was written, VMware had not yet validated such an approach in conjunction with VMware View. Testing of vCenter Server 4.1 with VMware View 4.5 and 4.6 was limited to testing 2,000 virtual desktops with one vCenter Server.

If you have only one building block in a pod, use two View Connection Server instances for redundancy.

Figure 4-1 shows the components of a View building block.

Figure 4-1. VMware View Building Block



Shared Storage for View Building Blocks

Storage design considerations are one of the most important elements of a successful View architecture. The decision that has the greatest architectural impact is whether to use View Composer desktops, which use linked-clone technology.

The external storage system that VMware vSphere uses can be a Fibre Channel or iSCSI SAN (storage area network), or an NFS (Network File System) NAS (network-attached storage). The ESX/ESXi binaries, virtual machine swap files, and View Composer replicas of parent virtual machines are stored on this system.

From an architectural perspective, View Composer creates desktop images that share a base image, which can reduce storage requirements by 50 percent or more. You can further reduce storage requirements by setting a refresh policy that periodically returns the desktop to its original state and reclaims space that is used to track changes since the last refresh operation.

You can also reduce operating system disk space by using View Composer persistent disks or a shared file server as the primary repository for the user profile and user documents. Because View Composer lets you separate user data from the operating system, you might find that only the persistent disk needs to be backed up or replicated, which further reduces storage requirements. For more information, see "Reducing Storage Requirements with View Composer," on page 25.

NOTE Whether to use a separate, dedicated storage component for each building block is a decision you can make during a pilot phase. The main consideration is I/Os per second (IOPS). You might experiment with a tiered-storage strategy across multiple building blocks to maximize performance and cost savings.

For more information, see the best-practices guide called *Storage Considerations for VMware View*.

Storage Bandwidth Considerations

Although many elements are important to designing a storage system that supports a VMware View environment, from a server configuration perspective, planning for proper storage bandwidth is essential. You must also consider the effects of port consolidation hardware.

VMware View environments can occasionally experience I/O storm loads, during which all virtual machines undertake an activity at the same time. I/O storms can be triggered by guest-based agents such as antivirus software or software-update agents. I/O storms can also be triggered by human behavior, such as when all employees log in at nearly the same time in the morning.

You can minimize these storm workloads through operational best practices, such as staggering updates to different virtual machines. You can also test various log-off policies during a pilot phase to determine whether suspending or powering off virtual machines when users log off causes an I/O storm. By storing View Composer replicas on separate, high-performance datastores, you can speed up intensive, concurrent read operations to contend with I/O storm loads.

In addition to determining best practices, VMware recommends that you provide bandwidth of 1Gbps per 100 virtual machines, even though average bandwidth might be 10 times less than that. Such conservative planning guarantees sufficient storage connectivity for peak loads.

Network Bandwidth Considerations

For display traffic, many elements can affect network bandwidth, such as protocol used, monitor resolution and configuration, and the amount of multimedia content in the workload. Concurrent launches of streamed applications can also cause usage spikes.

Because the effects of these issues can vary widely, many companies monitor bandwidth consumption as part of a pilot project. As a starting point for a pilot, plan for 150 to 200Kbps of capacity for a typical knowledge worker.

With the PCoIP display protocol, if you have an enterprise LAN with 100Mb or a 1Gb switched network, your end users can expect excellent performance under the following conditions:

- Two monitors (1920x1080)
- Heavy use of Microsoft Office applications
- Heavy use of Flash-embedded Web browsing
- Frequent use of multimedia with limited use of full screen mode
- Frequent use of USB-based peripherals
- Network-based printing

This information was excerpted from the information guide called *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*.

WAN Support and PCoIP

For wide-area networks (WANs), you must consider bandwidth constraints and latency issues. The PCoIP display protocol provided by VMware adapts to varying latency and bandwidth conditions.

If you use the RDP display protocol, you must have a WAN optimization product to accelerate applications for users in branch offices or small offices. With PCoIP, many WAN optimization techniques are built into the base protocol.

- WAN optimization is valuable for TCP-based protocols such as RDP because these protocols require many handshakes between client and server. The latency of these handshakes can be quite large. WAN accelerators spoof replies to handshakes so that the latency of the network is hidden from the protocol. Because PCoIP is UDP-based, this form of WAN acceleration is unnecessary.
- WAN accelerators also compress network traffic between client and server, but this compression is usually limited to 2:1 compression ratios. PCoIP is able to provide compression ratios of up to 100:1 for images and audio.

The following examples show how PCoIP can be expected to perform in various WAN scenarios:

Work from home

A user with a dedicated cable or DSL connection with 4-8MB download and less than 300ms latency can expect excellent performance under the following conditions:

- Two monitors (1920x1080)
- Microsoft Office applications
- Light use of Flash-embedded Web browsing
- Periodic use of multimedia
- Light printing with a locally connected USB printer

Mobile user

A user with a dedicated 3G connection with 5-500Kb download and less than 300ms latency can expect adequate bandwidth and tolerable latency under the following conditions:

- Single monitor
- Microsoft Office applications
- Light use of Flash-embedded Web browsing
- Light printing with a locally connected USB printer

Encourage mobile users to use local applications to access multimedia content.

Branch or remote office

Plan for 3 concurrent active users per 1Mb of bandwidth. Users at an office that has a 20Mb dedicated site-to-site UDP-based VPN with less than 200ms latency can expect acceptable performance under the following conditions:

- Two monitors (1920x1080)
- Microsoft Office applications
- Light use of Flash-embedded Web browsing
- Light printing with a locally connected USB printer

This information was excerpted from the information guide called *PCoIP Display Protocol: Information and Scenario-Based Network Sizing Guide*.

For information about setting up VPNs for using PCoIP, see the following solutions overviews, available on the VMware Web site:

- *VMware View and Juniper Networks SA Servers SSL VPN Solution*
- *VMware View and F5 BIG-IP SSL VPN Solution*
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution*

VMware View Pod

A VMware View pod integrates five 2,000-user building blocks into a View Manager installation that you can manage as one entity.

A pod is a unit of organization determined by VMware View scalability limits. Table 4-11 lists the components of a View pod.

Table 4-11. Example of a VMware View Pod

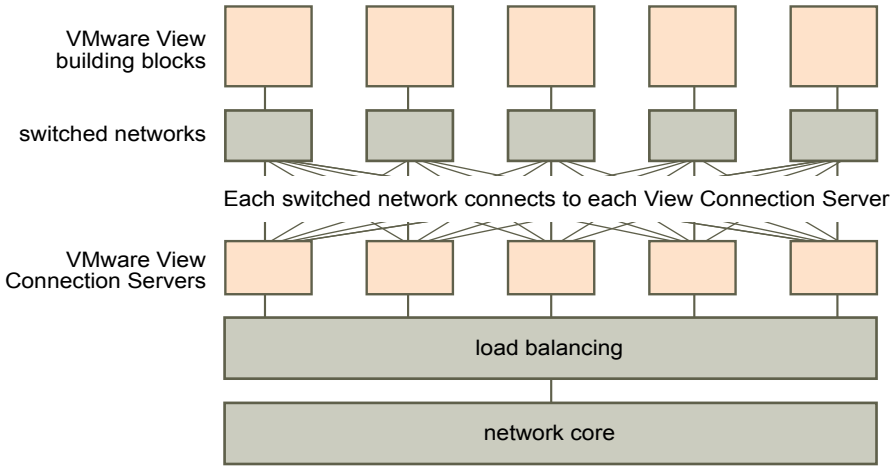
Item	Number
View building blocks	5
View Connection Servers	7 (1 for each building block and 2 spares)
10Gb Ethernet module	1
Modular networking switch	1
Load-balancing module	1
VPN for WAN	1 (optional)

The network core load balances incoming requests across View Connection Server instances. Support for a redundancy and failover mechanism, usually at the network level, prevents the load balancer from becoming a single point of failure. For example, the Virtual Router Redundancy Protocol (VRRP) communicates with the load balancer to add redundancy and failover capability.

If a View Connection Server instance fails or becomes unresponsive during an active session, users do not lose data. Desktop states are preserved in the virtual machine desktop so that users can connect to a different View Connection Server instance and their desktop session resumes from where it was when the failure occurred.

Figure 4-2 shows how all the components can be integrated into one manageable entity.

Figure 4-2. Pod Diagram for 10,000 View Desktops



Planning for Security Features 5

VMware View offers strong network security to protect sensitive corporate data. For added security, you can integrate VMware View with certain third-party user-authentication solutions, use a security server, and implement the restricted entitlements feature.

This chapter includes the following topics:

Understanding Client Connections

View Client and View Administrator communicate with a View Connection Server host over secure HTTPS connections.

The initial View Client connection, which is used for user authentication and View desktop selection, is created when a user opens View Client and provides an IP address or domain name for the View Connection Server or security server host. The View Administrator connection is created when an administrator types the View Administrator URL into a Web browser.

A default server SSL certificate is generated during View Connection Server installation. By default, clients are presented with this certificate when they visit a secure page such as View Administrator.

You can use the default certificate for testing, but you should replace it with your own certificate as soon as possible. The default certificate is not signed by a commercial Certificate Authority (CA). Use of noncertified certificates can allow untrusted parties to intercept traffic by masquerading as your server.

- Client Connections Using the PCoIP Secure Gateway on page 50

  When clients connect to a View desktop with the PCoIP display protocol from VMware, View Client can make a second connection to the PCoIP Secure Gateway component on a View Connection Server instance or a security server. This connection provides the required level of security and connectivity when accessing View desktops from the Internet.

- Tunneled Client Connections with Microsoft RDP on page 51

  When users connect to a View desktop with the Microsoft RDP display protocol, View Client can make a second HTTPS connection to the View Connection Server host. This connection is called the tunnel connection because it provides a tunnel for carrying RDP data.

- Direct Client Connections on page 51

  Administrators can configure View Connection Server settings so that View desktop sessions are established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server host. This type of connection is called a direct client connection.

- View Client with Local Mode Client Connections on page 52

  View Client with Local Mode offers mobile users the ability to check out View desktops onto their local computer.

Client Connections Using the PCoIP Secure Gateway

When clients connect to a View desktop with the PCoIP display protocol from VMware, View Client can make a second connection to the PCoIP Secure Gateway component on a View Connection Server instance or a security server. This connection provides the required level of security and connectivity when accessing View desktops from the Internet.

As of View 4.6, security servers include a PCoIP Secure Gateway component. The PCoIP Secure Gateway connection offers the following advantages:

- The only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user.
- Users can access only the desktop resources that they are authorized to access.
- This connection supports PCoIP, which is an advanced remote desktop protocol that makes more efficient use of the network by encapsulating video display packets in UDP instead of TCP.
- PCoIP is secured by AES-128 encryption.
- No VPN is required, as long as PCoIP is not blocked by any networking component. For example, someone trying to access their View desktop from inside a hotel room might find that the proxy the hotel uses is not configured to allow inbound traffic on TCP port 4172 and both inbound and outbound traffic on UDP port 4172.

  For more information, see “Firewall Rules for DMZ-Based Security Servers,” on page 60.

Security servers with PCoIP support run on Windows Server 2008 R2 and take full advantage of the 64-bit architecture. This security server can also take advantage of Intel processors that support AES New Instructions (AESNI) for highly optimized PCoIP encryption and decryption performance.

Tunneled Client Connections with Microsoft RDP

When users connect to a View desktop with the Microsoft RDP display protocol, View Client can make a second HTTPS connection to the View Connection Server host. This connection is called the tunnel connection because it provides a tunnel for carrying RDP data.

The tunnel connection offers the following advantages:

- RDP data is tunneled through HTTPS and is encrypted using SSL. This powerful security protocol is consistent with the security provided by other secure Web sites, such as those that are used for online banking and credit card payments.
- A client can access multiple desktops over a single HTTPS connection, which reduces the overall protocol overhead.
- Because VMware View manages the HTTPS connection, the reliability of the underlying protocols is significantly improved. If a user temporarily loses a network connection, the HTTP connection is reestablished after the network connection is restored and the RDP connection automatically resumes without requiring the user to reconnect and log in again.

In a standard deployment of View Connection Server instances, the HTTPS secure connection terminates at the View Connection Server. In a DMZ deployment, the HTTPS secure connection terminates at a security server. See "Preparing to Use a Security Server," on page 57 for information on DMZ deployments and security servers.

Clients that use the PCoIP display protocol can use the tunnel connection for USB redirection and multimedia redirection (MMR) acceleration, but for all other data, PCoIP uses the PCoIP Secure Gateway on a security server. For more information, see "Client Connections Using the PCoIP Secure Gateway," on page 50.

Clients that use the PCoIP or HP RGS display protocols do not use the tunnel connection.

Direct Client Connections

Administrators can configure View Connection Server settings so that View desktop sessions are established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server host. This type of connection is called a direct client connection.

With direct client connections, an HTTPS connection can still be made between the client and the View Connection Server host for users to authenticate and select View desktops, but the second HTTPS connection (the tunnel connection) is not used.

Clients that use the HP RGS display protocol always use direct client connections. HP RGS clients cannot use a tunnel connection or a PCoIP Secure Gateway connection.

Direct PCoIP connections include the following built-in security features:

- PCoIP supports Advanced Encryption Standard (AES) encryption, which is turned on by default.
- The hardware implementation of PCoIP uses both AES and IP Security (IPsec).
- PCoIP works with third-party VPN clients.

For clients that use the Microsoft RDP display protocol, direct client connections are appropriate only if your deployment is inside a corporate network. With direct client connections, RDP traffic is sent unencrypted over the connection between the client and the View desktop virtual machine.

View Client with Local Mode Client Connections

View Client with Local Mode offers mobile users the ability to check out View desktops onto their local computer.

View Client with Local Mode supports both tunneled and nontunneled communications for LAN-based data transfers. With tunneled communications, all traffic is routed through the View Connection Server host, and you can specify whether to encrypt communications and data transfers. With nontunneled communications, unencrypted data is transferred directly between the local desktop on the client system and the View desktop virtual machine in vCenter Server.

Local data is always encrypted on the user's computer, regardless of whether you configure tunneled or nontunneled communications.

The data disk stored locally on client systems is encrypted using a default encryption strength of AES-128. The encryption keys are stored encrypted on the client system with a key derived from a hash of the user's credentials (username and password or smart card and PIN). On the server side, the key is stored in View LDAP. Whatever security measures you use to protect View LDAP on the server also protect the local mode encryption keys stored in LDAP.

NOTE You can change the encryption key cipher from AES-128 to AES-192 or AES-256.

The desktop has a lifetime controlled through policy. If the client loses contact with View Connection Server, the maximum time without server contact is the period in which the user can continue to use the desktop before the user is refused access. On the client side, this expiration policy is stored in a file that is encrypted by a key that is built into the application. This built-in key prevents users who have access to the password from circumventing the expiration policy.

Choosing a User Authentication Method

VMware View uses your existing Active Directory infrastructure for user authentication and management. For added security, you can integrate VMware View with RSA SecurID and smart card authentication solutions.

- Active Directory Authentication on page 53

  Each View Connection Server instance is joined to an Active Directory domain, and users are authenticated against Active Directory for the joined domain. Users are also authenticated against any additional user domains with which a trust agreement exists.

- RSA SecurID Authentication on page 53

  RSA SecurID provides enhanced security with two-factor authentication, which requires knowledge of the user's PIN and token code. The token code is only available on the physical SecurID token.

- Smart Card Authentication on page 53

  A smart card is a small plastic card that is embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. A smart card is also referred to as a Common Access Card (CAC).

- Log In as Current User Feature on page 54

  When View Client users select the **Log in as current user** check box, the credentials that they provided when logging in to the client system are used to authenticate to the View Connection Server instance and to the View desktop. No further user authentication is required.

Active Directory Authentication

Each View Connection Server instance is joined to an Active Directory domain, and users are authenticated against Active Directory for the joined domain. Users are also authenticated against any additional user domains with which a trust agreement exists.

For example, if a View Connection Server instance is a member of Domain A and a trust agreement exists between Domain A and Domain B, users from both Domain A and Domain B can connect to the View Connection Server instance with View Client.

Similarly, if a trust agreement exists between Domain A and an MIT Kerberos realm in a mixed domain environment, users from the Kerberos realm can select the Kerberos realm name when connecting to the View Connection Server instance with View Client.

View Connection Server determines which domains are accessible by traversing trust relationships, starting with the domain in which the host resides. For a small, well-connected set of domains, View Connection Server can quickly determine a 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 desktops.

Administrators can use the `vdmadmin` command-line interface to configure domain filtering, which limits the domains that a View Connection Server instance searches and that it displays to users. See the *VMware View Administration* document for more information.

Policies, such as restricting permitted hours to log in and setting the expiration date for passwords, are also handled through existing Active Directory operational procedures.

RSA SecurID Authentication

RSA SecurID provides enhanced security with two-factor authentication, which requires knowledge of the user's PIN and token code. The token code is only available on the physical SecurID token.

Administrators can enable individual View Connection Server instances for RSA SecurID authentication by installing the RSA SecurID software on the View Connection Server host and modifying View Connection Server settings.

When users log in through a View Connection Server instance that is enabled for RSA SecurID authentication, they are first required to authenticate with their RSA user name and passcode. If they are not authenticated at this level, access is denied. If they are correctly authenticated with RSA SecurID, they continue as normal and are then required to enter their Active Directory credentials.

If you have multiple View Connection Server instances, you can configure RSA SecurID authentication on some instances and a different user authentication method on others. For example, you can configure RSA SecurID authentication only for users who access View desktops remotely over the Internet.

VMware View is certified through the RSA SecurID Ready program and supports the full range of SecurID capabilities, including New PIN Mode, Next Token Code Mode, RSA Authentication Manager, and load balancing.

Smart Card Authentication

A smart card is a small plastic card that is embedded with a computer chip. Many government agencies and large enterprises use smart cards to authenticate users who access their computer networks. A smart card is also referred to as a Common Access Card (CAC).

Smart card authentication is supported by the Windows-based View Client and View Client with Local Mode only. It is not supported by View Administrator.

Administrators can enable individual View Connection Server instances for smart card authentication. Enabling a View Connection Server instance to use smart card authentication typically involves adding your root certificate to a truststore file and then modifying View Connection Server settings.

Client connections that use smart card authentication must be SSL enabled. Administrators can enable SSL for client connections by setting a global parameter in View Administrator.

To use smart cards, client machines must have smart card middleware and a smart card reader. To install certificates on smart cards, you must set up a computer to act as an enrollment station.

To use smart cards with local desktops, you must select a 1024-bit or 2048-bit key size during smart card enrollment. Certificates with 512-bit keys are not supported for local desktops. By default, View Connection Server uses AES-128 to encrypt the virtual disk file when users check in and check out a local desktop. You can change the encryption key cipher to AES-192 or AES-256.

Log In as Current User Feature

When View Client users select the **Log in as current user** check box, the credentials that they provided when logging in to the client system are used to authenticate to the View Connection Server instance and to the View desktop. No further user authentication is required.

To support this feature, user credentials are stored on both the View Connection Server instance and on the client system.

- On the View Connection Server instance, user credentials are encrypted and stored in the user session along with the username, domain, and optional UPN. The credentials are added when authentication occurs and are purged when the session object is destroyed. The session object is destroyed when the user logs out, the session times out, or authentication fails. The session object resides in volatile memory and is not stored in View LDAP or in a disk file.
- On the client system, user credentials are encrypted and stored in a table in the Authentication Package, which is a component of View Client. The credentials are added to the table when the user logs in and are removed from the table when the user logs out. The table resides in volatile memory.

Administrators can use View Client group policy settings to control the availability of the **Log in as current user** check box and to specify its default value. Administrators can also use group policy to specify which View Connection Server instances accept the user identity and credential information that is passed when users select the **Log in as current user** check box in View Client.

The Log in as current user feature has the following limitations and requirements:

- If smart card authentication is set to Required on a View Connection Server instance, smart card users who select the **Log in as current user** check box must still reauthenticate with their smart card and PIN when logging in to the View desktop.
- Users cannot check out a desktop for use in local mode if they selected the **Log in as current user** check box when they logged in.
- The time on the system where the client logs in and the time on the View Connection Server host must be synchronized.
- If the default **Access this computer from the network** user-right assignments are modified on the client system, they must be modified as described in VMware Knowledge Base (KB) article 1025691.

Restricting View Desktop Access

You can use the restricted entitlements feature to restrict View desktop access based on the View Connection Server instance that a user connects to.

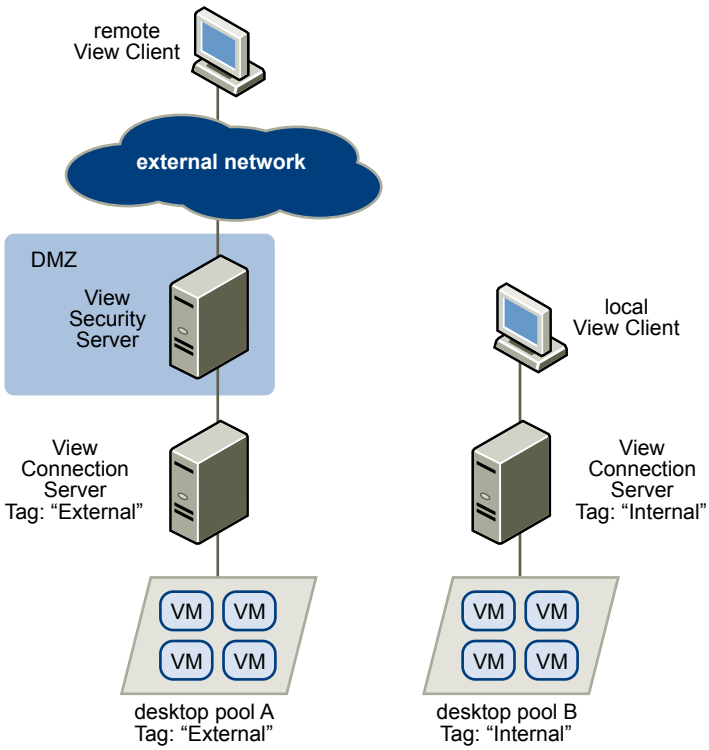
With restricted entitlements, you assign one or more tags to a View Connection Server instance. Then, when configuring a desktop pool, you select the tags of the View Connection Server instances that you want to be able to access the desktop pool. When users log in through a tagged View Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

For example, your VMware View deployment might include two View Connection Server instances. The first instance supports your internal users. The second instance is paired with a security server and supports your external users. To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

- Assign the tag "Internal" to the View Connection Server instance that supports your internal users.
- Assign the tag "External" to the View Connection Server instance that is paired with the security server and supports your external users.
- Assign the "Internal" tag to the desktop pools that should be accessible only to internal users.
- Assign the "External" tag to the desktop pools that should be accessible only to external users.

External users cannot see the desktop pools tagged as Internal because they log in through the View Connection Server tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the View Connection Server tagged as Internal. Figure 5-1 illustrates this configuration.

Figure 5-1. Restricted Entitlements Example



You can also use restricted entitlements to control desktop access based on the user-authentication method that you configure for a particular View Connection Server instance. For example, you can make certain desktop pools available only to users who have authenticated with a smart card.

The restricted entitlements feature only enforces tag matching. You must design your network topology to force certain clients to connect through a particular View Connection Server instance.

Using Group Policy Settings to Secure View Desktops

VMware View includes Group Policy administrative (ADM) templates that contain security-related group policy settings that you can use to secure your View desktops.

For example, you can use group policy settings to perform the following tasks.

- Specify the View Connection Server instances that can accept user identity and credential information that is passed when a user selects the **Log in as current user** check box in View Client.
- Enable single sign-on for smart card authentication in View Client.
- Configure server SSL certificate checking in View Client.
- Prevent users from providing credential information with View Client command line options.
- Prevent non-View client systems from using RDP to connect to View desktops. You can set this policy so that connections must be View-managed, which means that users must use View Client to connect to View desktops.

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

Implementing Best Practices to Secure Client Systems

You should implement best practices to secure client systems.

- Make sure that client systems are configured to go to sleep after a period of inactivity and require users to enter a password before the computer awakens.
- Require users to enter a username and password when starting client systems. Do not configure client systems to allow automatic logins.
- For Mac client systems, consider setting different passwords for the Keychain and the user account. When the passwords are different, users are prompted before the system enters any passwords on their behalf. Also consider turning on FileVault protection.
- Local mode client systems might have more network access when they are running in local mode than when they are remote and connected to the intranet. Consider enforcing intranet network security policies for local mode client systems or disable network access for local mode client systems when they are running in local mode.

Assigning Administrator Roles

A key management task in a VMware View environment is to determine who can use View Administrator and what tasks those users are authorized to perform.

The authorization to perform tasks in View Administrator is governed by an access control system that consists of administrator roles and privileges. A role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool or changing a configuration setting. Privileges also control what an administrator can see in View Administrator.

An administrator can create folders to subdivide desktop pools and delegate the administration of specific desktop pools to different administrators in View Administrator. An administrator configures administrator access to the resources in a folder by assigning a role to a user on that folder. Administrators can only access the resources that reside in folders for which they have assigned roles. The role that an administrator has on a folder determines the level of access that the administrator has to the resources in that folder.

View Administrator includes a set of predefined roles. Administrators can also create custom roles by combining selected privileges.

Preparing to Use a Security Server

A security server is a special instance of View Connection Server that runs a subset of View Connection Server functions. You can use a security server to provide an additional layer of security between the Internet and your internal network.

A security server resides within a DMZ and acts as a proxy host for connections inside your trusted network. Each security server is paired with an instance of View Connection Server and forwards all traffic to that instance. This design provides an additional layer of security by shielding the View Connection Server instance from the public-facing Internet and by forcing all unprotected session requests through the security server.

A DMZ-based security server deployment requires a few ports to be opened on the firewall to allow clients to connect with security servers inside the DMZ. You must also configure ports for communication between security servers and the View Connection Server instances in the internal network. See "Firewall Rules for DMZ-Based Security Servers," on page 60 for information on specific ports.

Because users can connect directly with any View Connection Server instance from within their internal network, you do not need to implement a security server in a LAN-based deployment.

NOTE As of View 4.6, security servers include a PCoIP Secure Gateway component so that clients that use the PCoIP display protocol can use a security server rather than a VPN.

For information about setting up VPNs for using PCoIP, see the following solutions overviews, available on the VMware Web site:

- *VMware View and Juniper Networks SA Servers SSL VPN Solution*
- *VMware View and F5 BIG-IP SSL VPN Solution*
- *VMware View and Cisco Adaptive Security Appliances (ASA) SSL VPN Solution*

Best Practices for Security Server Deployments

You should follow best practice security policies and procedures when operating a security server in a DMZ.

The *DMZ Virtualization with VMware Infrastructure* white paper includes examples of best practices for a virtualized DMZ. Many of the recommendations in this white paper also apply to a physical DMZ.

To limit the scope of frame broadcasts, the View Connection Server instances that are paired with security servers should be deployed on an isolated network. This topology can help prevent a malicious user on the internal network from monitoring communication between the security servers and View Connection Server instances.

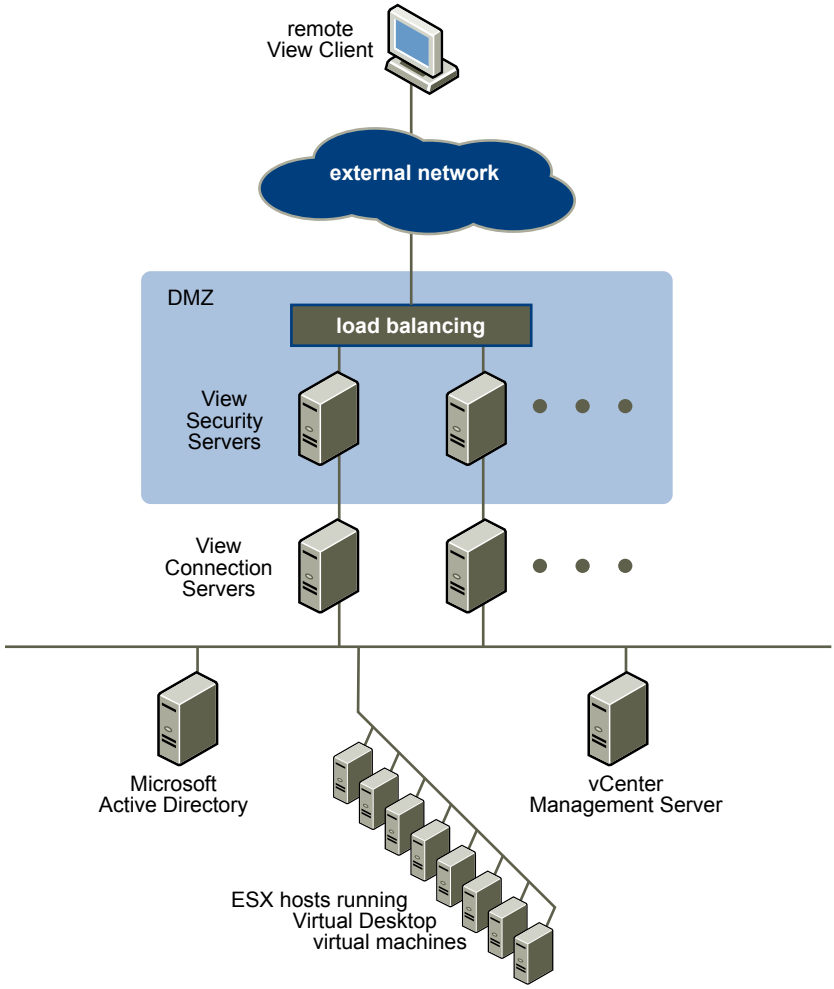
Alternatively, you might be able to use advanced security features on your network switch to prevent malicious monitoring of security server and View Connection Server communication and to guard against monitoring attacks such as ARP Cache Poisoning. See the administration documentation for your networking equipment for more information.

Security Server Topologies

You can implement several different security server topologies.

The topology illustrated in Figure 5-2 shows a high-availability environment that includes two load-balanced security servers in a DMZ. The security servers communicate with two View Connection Server instances inside the internal network.

Figure 5-2. Load-Balanced Security Servers in a DMZ

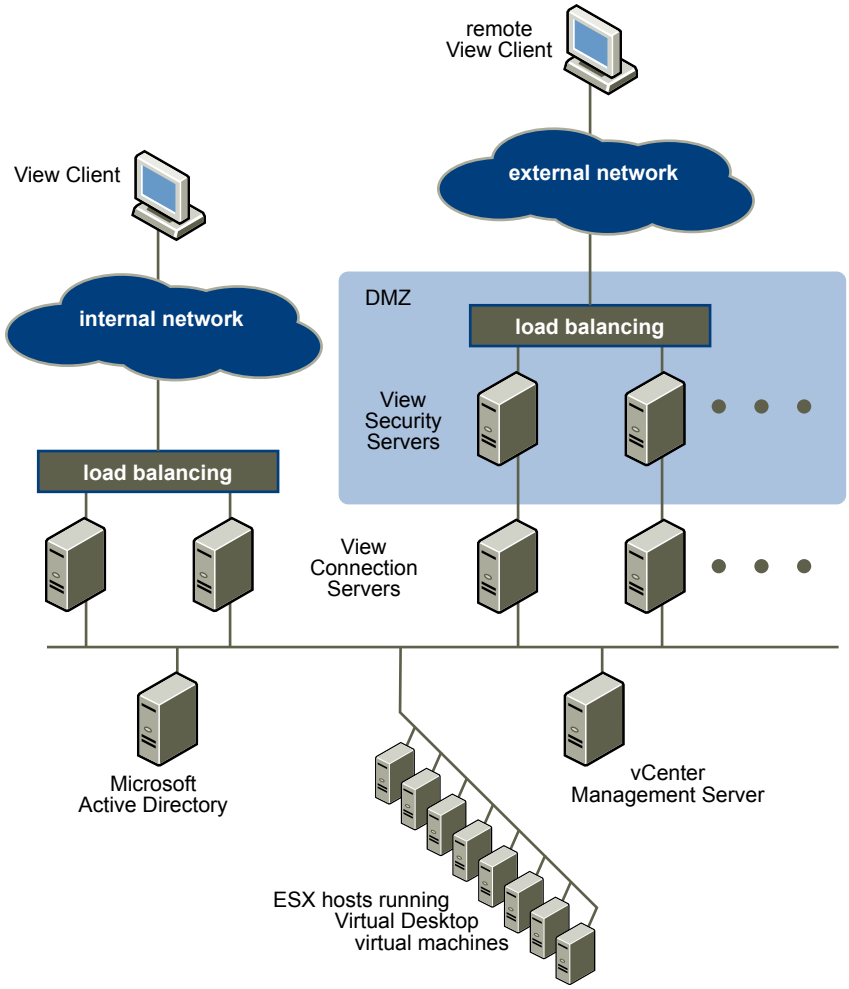


When remote users connect to a security server, they must successfully authenticate before they can access View desktops. With appropriate firewall rules on both sides of the DMZ, this topology is suitable for accessing View desktops from client devices located on the Internet.

You can connect multiple security servers to each instance of View Connection Server. You can also combine a DMZ deployment with a standard deployment to offer access for internal users and external users.

The topology illustrated in Figure 5-3 shows an environment where four instances of View Connection Server act as one group. The instances in the internal network are dedicated to users of the internal network, and the instances in the external network are dedicated to users of the external network. If the View Connection Server instances paired with the security servers are enabled for RSA SecurID authentication, all external network users are required to authenticate by using RSA SecurID tokens.

Figure 5-3. Multiple Security Servers



You must implement a hardware or software load balancing solution if you install more than one security server. View Connection Server does not provide its own load balancing functionality. View Connection Server works with standard third-party load balancing solutions.

Firewalls for DMZ-Based Security Servers

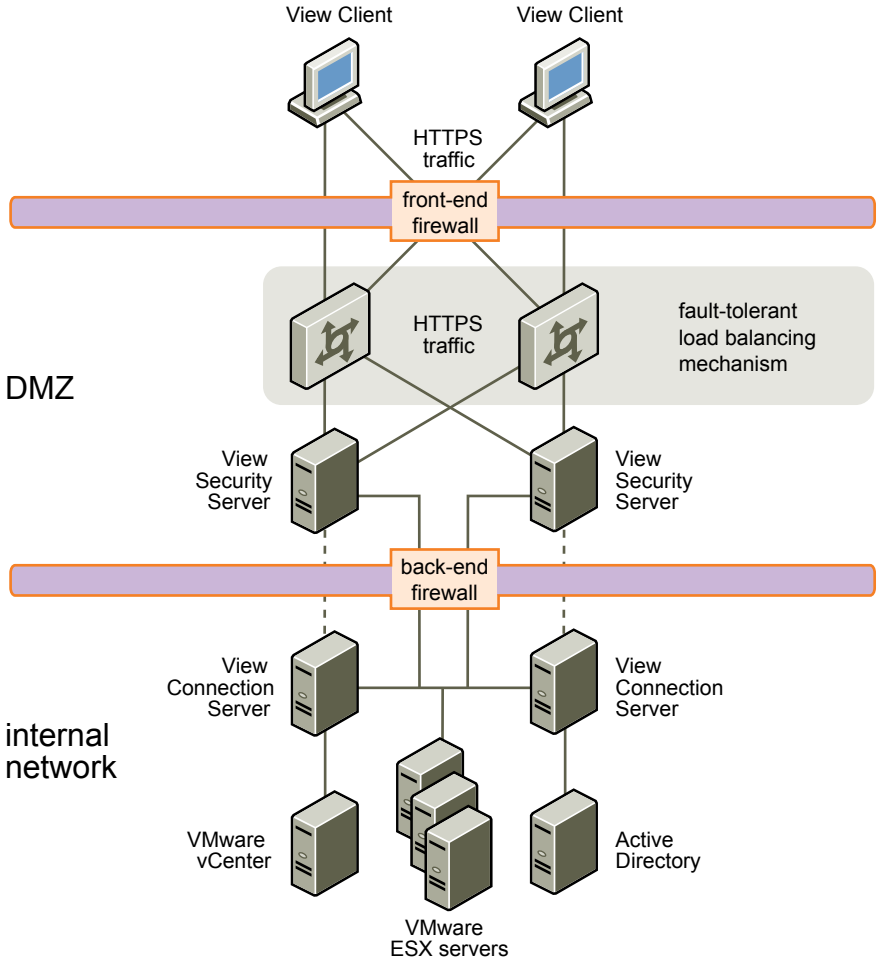
A DMZ-based security server deployment must include two firewalls.

- An external network-facing, front-end firewall is required to protect both the DMZ and the internal network. You configure this firewall to allow external network traffic to reach the DMZ.
- A back-end firewall, between the DMZ and the internal network, is required to provide a second tier of security. You configure this firewall to accept only traffic that originates from the services within the DMZ.

Firewall policy strictly controls inbound communications from DMZ services, which greatly reduces the risk of compromising your internal network.

Figure 5-4 shows an example of a configuration that includes front-end and back-end firewalls.

Figure 5-4. Dual Firewall Topology



Firewall Rules for DMZ-Based Security Servers

DMZ-based security servers require certain firewall rules on the front-end and back-end firewalls.

Front-End Firewall Rules

To allow external client devices to connect to a security server within the DMZ, the front-end firewall must allow traffic on certain TCP and UDP ports. Table 5-1 summarizes the front-end firewall rules.

Table 5-1. Front-End Firewall Rules

Source	Protocol	Port	Destination	Notes
Any	HTTP	80	Security server	External client devices use port 80 to connect to a security server within the DMZ when SSL is disabled.
Any	HTTPS	443	Security server	External client devices use port 443 to connect to a security server within the DMZ when SSL is enabled (the default).
Any	PCoIP	TCP 4172 UDP 4172	Security server	External client devices use TCP port 4172 to a security server within the DMZ when SSL is enabled and also use UDP port 4172 in both directions.

Back-End Firewall Rules

To allow a security server to communicate with each View Connection Server instance that resides within the internal network, the back-end firewall must allow inbound traffic on certain TCP ports. Behind the back-end firewall, internal firewalls must be similarly configured to allow View desktops and View Connection Server instances to communicate with each other. Table 5-2 summarizes the back-end firewall rules.

Table 5-2. Back-End Firewall Rules

Source	Protocol	Port	Destination	Notes
Security server	HTTP	80	Transfer Server	Security servers can use port 80 to download View desktop data to local mode desktops from the Transfer Server and to replicate data to the Transfer Server.
Security server	HTTPS	443	Transfer Server	If you configure View Connection Server to use SSL for local mode operations and desktop provisioning, security servers use port 443 for downloads and replication between local mode desktops and the Transfer Server.
Security server	AJP13	8009	View Connection Server	Security servers use port 8009 to transmit AJP13-forwarded Web traffic to View Connection Server instances.
Security server	JMS	4001	View Connection Server	Security servers use port 4001 to transmit Java Message Service (JMS) traffic to View Connection Server instances.
Security server	RDP	3389	View desktop	Security servers use port 3389 to transmit RDP traffic to View desktops. NOTE For USB redirection, TCP port 32111 is used alongside RDP. For MMR, TCP port 9427 is used alongside RDP.
Security server	PCoIP	TCP 4172 UDP 4172	View desktop	Security servers use TCP port 4172 to transmit PCoIP traffic to View desktops, and security servers use UDP port 4172 to transmit PCoIP traffic in both directions. For USB redirection, TCP port 32111 is used alongside PCoIP from the client to the View desktop.

TCP Ports for View Connection Server Intercommunication

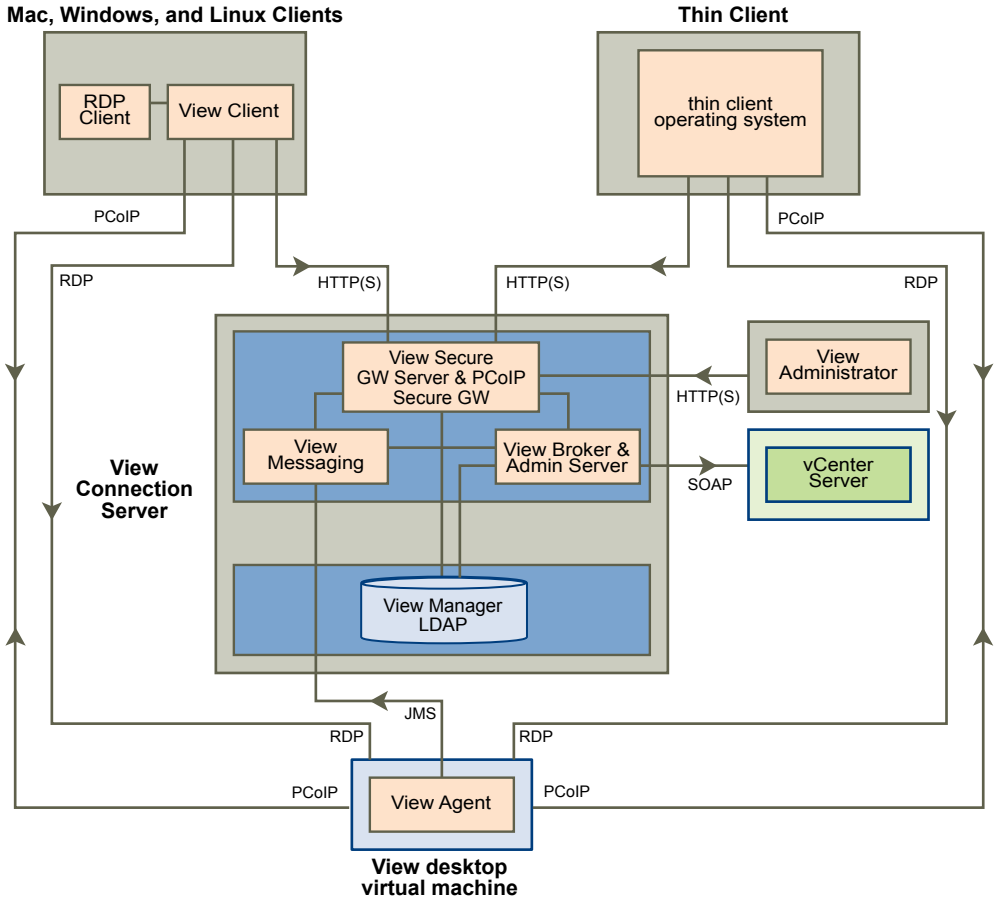
Groups of View Connection Server instances use additional TCP ports to communicate with each other. For example, View Connection Server instances use port 4100 to transmit JMS inter-router (JMSIR) traffic to each other. Firewalls are generally not used between the View Connection Server instances in a group.

Understanding VMware View Communications Protocols

VMware View components exchange messages by using several different protocols.

Figure 5-5 illustrates the protocols that each component uses for communication when a security server is not configured. That is, the secure tunnel for RDP and the PCoIP secure gateway are not turned on. This configuration might be used in a typical LAN deployment.

Figure 5-5. VMware View Components and Protocols Without a Security Server



NOTE This figure shows direct connections for clients using either PCoIP or RDP. The default setting, however, is to have direct connections for PCoIP and tunnel connections for RDP.

See Table 5-3 for the default ports that are used for each protocol.

Figure 5-6 illustrates the protocols that each component uses for communication when a security server is configured. This configuration might be used in a typical WAN deployment.

Figure 5-6. VMware View Components and Protocols with a Security Server

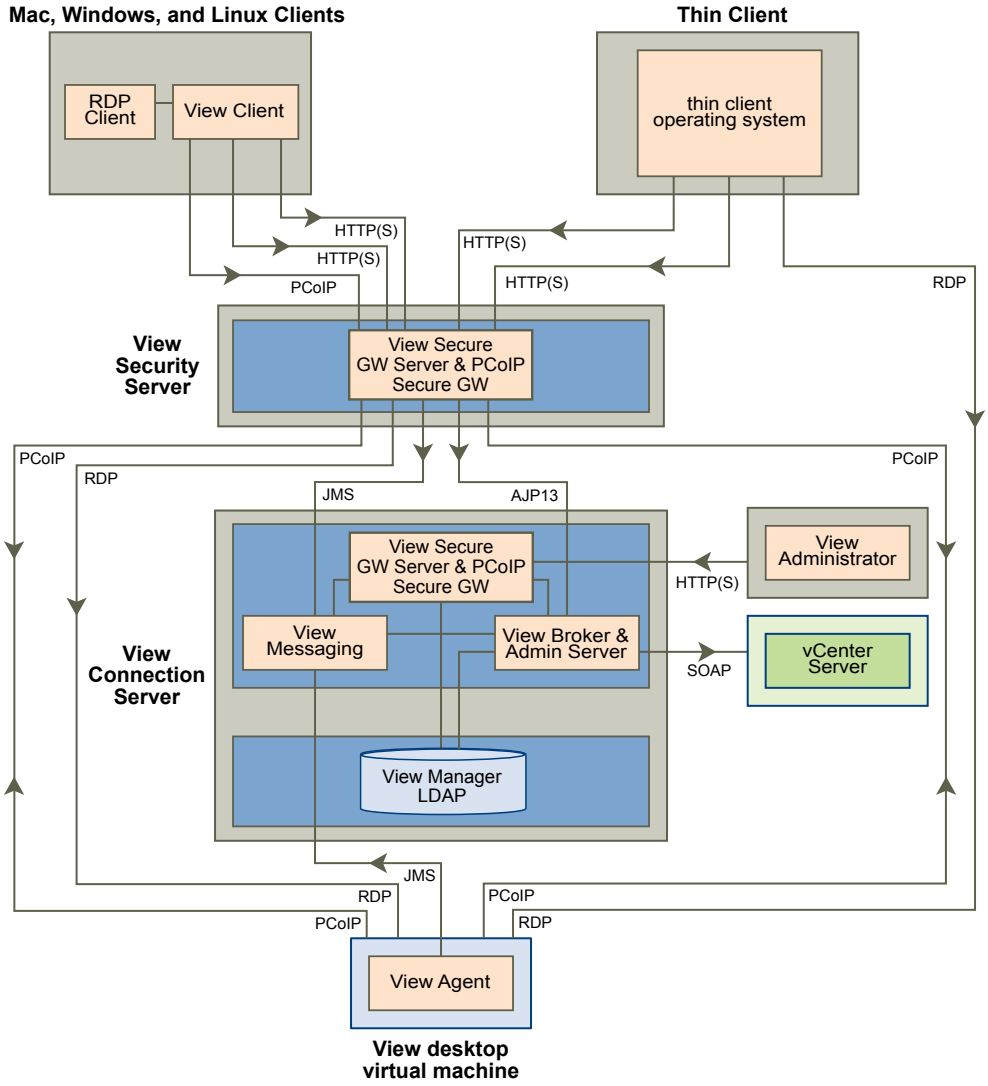


Table 5-3 lists the default ports that are used by each protocol.

Table 5-3. Default Ports

Protocol	Port
JMS	TCP port 4001
AJP13	TCP port 8009 **Note** AJP13 is used in a security server configuration only.
HTTP	TCP port 80
HTTPS	TCP port 443
RDP	TCP port 3389 For USB redirection, TCP port 32111 is used alongside RDP. For MMR, TCP port 9427 is used alongside RDP. **Note** If the View Connection Server instance is configured for direct client connections, these protocols connect directly from the client to the View desktop and are not tunneled through the View Secure GW Server component.

Table 5-3. Default Ports (Continued)

Protocol	Port
SOAP	TCP port 80 or 443
PCoIP	TCP port 4172 from View Client to the View desktop. PCoIP also uses UDP port 4172 in both directions. For USB redirection, TCP port 32111 is used alongside PCoIP from the client to the View desktop.

View Broker and Administration Server

The View Broker component, which is the core of View Connection Server, is responsible for all user interaction between VMware View clients and View Connection Server. View Broker also includes the Administration Server that is used by the View Administrator Web client.

View Broker works closely with vCenter Server to provide advanced management of View desktops, including virtual machine creation and power operations.

View Secure Gateway Server

View Secure Gateway Server is the server-side component for the secure HTTPS connection between VMware View clients and a security server or View Connection Server instance.

When you configure the tunnel connection for View Connection Server, RDP, USB, and Multimedia Redirection (MMR) traffic is tunneled through the View Secure Gateway component. When you configure direct client connections, these protocols connect directly from the client to the View desktop and are not tunneled through the View Secure Gateway Server component.

NOTE Clients that use the PCoIP display protocol can use the tunnel connection for USB redirection and multimedia redirection (MMR) acceleration, but for all other data, PCoIP uses the PCoIP Secure Gateway on a security server.

HP RGS does not use the tunnel connection at all.

View Secure Gateway Server is also responsible for forwarding other Web traffic, including user authentication and desktop selection traffic, from VMware View clients to the View Broker component. View Secure Gateway Server also passes View Administrator client Web traffic to the Administration Server component.

PCoIP Secure Gateway

As of View 4.6, security servers include a PCoIP Secure Gateway component. When the PCoIP Secure Gateway is enabled, after authentication, View clients that use PCoIP can make another secure connection to a security server. This connection allows remote clients to access View desktops from the Internet.

When you enable the PCoIP Secure Gateway component, PCoIP traffic is forwarded by a security server to View desktops. If clients that use PCoIP also use the USB redirection feature or multimedia redirection (MMR) acceleration, you can enable the View Secure Gateway component in order to forward that data.

When you configure direct client connections, PCoIP traffic and other traffic goes directly from a View client to a View desktop.

When end users such as home or mobile workers access desktops from the Internet, security servers provide the required level of security and connectivity so that a VPN connection is not necessary. The PCoIP Secure Gateway component ensures that the only remote desktop traffic that can enter the corporate data center is traffic on behalf of a strongly authenticated user. End users can access only the desktop resources that they are authorized to access.

View LDAP

View LDAP is an embedded LDAP directory in View Connection Server and is the configuration repository for all VMware View configuration data.

View LDAP contains entries that represent each View desktop, each accessible View desktop, multiple View desktops that are managed together, and View component configuration settings.

View LDAP also includes a set of View plug-in DLLs to provide automation and notification services for other VMware View components.

View Messaging

The View Messaging component provides the messaging router for communication between View Connection Server components and between View Agent and View Connection Server.

This component supports the Java Message Service (JMS) API, which is used for messaging in VMware View.

By default, RSA keys that are used for intercomponent message validation are 512 bits. The RSA key size can be increased to 1024 bits if you prefer stronger encryption.

If you want all keys to be 1024 bits, the RSA key size must be changed immediately after the first View Connection Server instance is installed and before additional servers and desktops are created. See VMware Knowledge Base (KB) article 1024431 for more information.

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 on Windows Server 2008, the installation program can optionally configure the required Windows firewall rules for you. When you install View Connection Server on Windows Server 2003, you must configure the required Windows firewall rules manually.

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

Firewall Rules for View Agent

The View Agent installation program opens certain TCP ports on the firewall. Ports are incoming unless otherwise noted.

Table 5-5. TCP Ports Opened During View Agent Installation

Protocol	Ports
RDP	3389
USB redirection	32111
MMR	9427

Table 5-5. TCP Ports Opened During View Agent Installation (Continued)

Protocol	Ports
PCoIP	4172 (TCP and UDP)
HP RGS	42966

The View Agent installation program configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.

If you instruct the View Agent installation program to not enable Remote Desktop support, it does not open ports 3389 and 32111, and you must open these ports manually.

The HP RGS Sender application is the server-side component of the HP RGS remote display protocol. HP RGS Sender uses port 42966 by default.

If you use a virtual machine template as a desktop source, firewall exceptions carry over to deployed desktops only if the template is a member of the desktop domain. You can use Microsoft group policy settings to manage local firewall exceptions. See the Microsoft Knowledge Base (KB) article 875357 for more information.

Firewall Rules for Active Directory

If you have a firewall between your VMware View environment and your Active Directory server, you must make sure that all of the necessary ports are opened.

For example, View Connection Server must be able to access the Active Directory Global Catalog and Lightweight Directory Access Protocol (LDAP) servers. If the Global Catalog and LDAP ports are blocked by your firewall software, administrators will have problems configuring user entitlements.

See the Microsoft documentation for your Active Directory server version for information about the ports that must be opened for Active Directory to function correctly through a firewall.

Firewall Rules for View Client with Local Mode

View Client with Local Mode data is downloaded and uploaded through port 902. If you intend to use View Client with Local Mode, port 902 must be accessible to your ESX/ESXi host.

Overview of Steps to Setting Up a VMware View Environment

6

Complete these high-level tasks to install VMware View and configure an initial deployment.

Table 6-1. View Installation and Setup Check List

Step	Task
1	Set up the required administrator users and groups in Active Directory. Instructions: *VMware View Installation* and vSphere documentation
2	If you have not yet done so, install and set up VMware ESX/ESXi hosts and vCenter Server. Instructions: vSphere documentation
3	If you are going to deploy linked-clone desktops, install View Composer on the vCenter Server system. Instructions: *VMware View Installation* document
4	Install and set up View Connection Server. Instructions: *VMware View Installation* document
5	If you are going to use desktops in local mode, install Transfer Server. Instructions: *VMware View Installation* document
6	Create one or more virtual machines that can be used as a template for full-clone desktop pools or as a parent for linked-clone desktop pools. Instructions: *VMware View Administration* document
7	Create a desktop pool. Instructions: *VMware View Administration* document
8	Control user access to desktops. Instructions: *VMware View Administration* document
9	Install View Client on end users' machines and have end users access their View desktops. Instructions: *VMware View Installation*
10	(Optional) Create and configure additional administrators to allow different levels of access to specific inventory objects and settings. Instructions: *VMware View Administration* document
11	(Optional) Configure policies to control the behavior of View components, desktop pools, and desktop users. Instructions: *VMware View Administration* document
12	(Optional) For added security, integrate smart card authentication and RSA SecurID solutions. Instructions: *VMware View Administration* document

Index

T

U

V

W