

VMware View Architecture Planning Guide

View 4.0

View Manager 4.0

View Composer 2.0

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

EN-000241-01

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

Copyright © 2010 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

About This Book	5	
1	Introduction to VMware View	7
Advantages of Using VMware View	7	
VMware View Features	8	
How the VMware View Components Fit Together	9	
2	Planning a Rich User Experience	15
Feature Support Matrix	15	
Choosing a Display Protocol	16	
Accessing USB Devices Connected to a Local Computer	18	
Printing from a View Desktop	18	
Streaming Multimedia to a View Desktop	19	
Using Single Sign-On for Logging In to a View Desktop	19	
Using Multiple Monitors with a View Desktop	19	
3	Managing Desktop Pools from a Central Location	21
Advantages of Desktop Pools	21	
Reducing and Managing Storage Requirements	22	
Application Provisioning	23	
Using Active Directory GPOs to Manage Users and Desktops	24	
4	Architecture Design Elements and Planning Guidelines	25
Desktop Virtual Machine Configuration	25	
vCenter and View Composer Virtual Machine Configuration and Desktop Pool Maximums	30	
Connection Server Virtual Machine Configuration and Maximums	31	
VMware View Node	32	
vSphere Clusters	33	
VMware View Building Blocks	34	
VMware View Pod	37	
5	Planning for Security Features	39
Understanding Client Connections	39	
Choosing a User Authentication Method	41	
Preparing to Use a Security Server	43	
Restricting View Desktop Access	51	
6	Overview of Steps to Setting Up a VMware View Environment	53
Index	55	

About This Book

The *VMware View Architecture Planning Guide* 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. To help you protect your VMware View installation, the book also provides a discussion of security features. 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?

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.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to <http://www.vmware.com/support/pubs>.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to <http://www.vmware.com/support>.

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to <http://www.vmware.com/support/services>.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting

Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to <http://www.vmware.com/services>.

Introduction to VMware View

VMware View lets IT departments 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,”](#) on page 7
- [“VMware View Features,”](#) on page 8
- [“How the VMware View Components Fit Together,”](#) on page 9

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

VMware View PC-over-IP 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 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. Rather than installing applications one by one on each end user's physical PC, the end user connects 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, 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. 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:

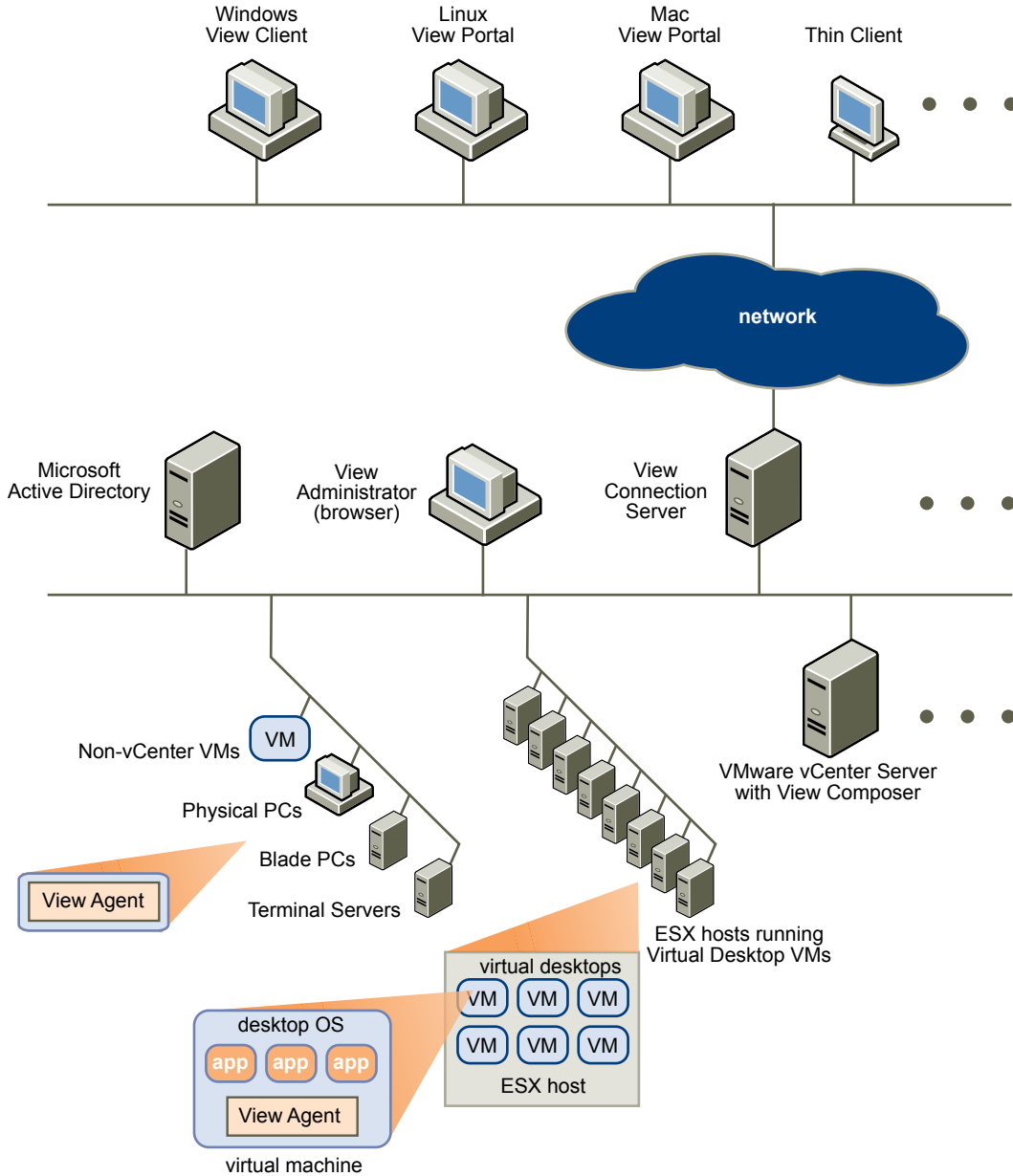
- Integrate with VMware vSphere to achieve cost-effective densities, high levels of availability, and advanced resource allocation control for your virtual desktops.
- Configure View Connection Server to broker connections between end users and the virtual desktops that they are authorized to access.
- 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 or use View Portal to log in to View Connection Server. This server, which integrates with Windows Active Directory, provides access to a virtual desktop hosted on a VMware ESX server, a blade or physical PC, or a Windows Terminal Services server.

[Figure 1-1](#) shows the relationship between the major components of a VMware View deployment.

Figure 1-1. 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.

From laptops and Windows PCs, end users open View Client to display their View desktop. From a Mac or Linux PC, end users open a Web browser and use View Portal to display their View desktop. Windows devices can also use View Portal, but some functionality is not supported.

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
- Managing 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 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 2003 server, preferably on a VMware virtual machine.

View Client

The client software for accessing View desktops runs either on a Windows PC as a native Windows 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 PCoIP display protocol is now available with VMware View 4. The speed and display quality of PCoIP rival that of a physical PC.

View Client with Offline Desktop is a version of View Client that has been extended to support the experimental Offline Desktop feature. This feature allows end users to download virtual machines and use them on their local systems.

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

- View Portal for Linux (experimental) and View Portal for Mac OS X (experimental).
- 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 Mac, Windows, or Linux PC, end users can open a Web browser and use View Portal to display their View desktop. This Web-based version of View Client installs all necessary View software on a client device, but some extensions, such as those for connecting USB devices, might not be installed.

To use View Portal, end users open a Firefox, Internet Explorer, or Safari browser and enter the URL of a View Connection Server instance. View Portal prompts users for permission to install the required View Client components. On Linux clients, View Portal requires `rdesktop` to display virtual desktops, and on Mac OS/X, View Portal requires Microsoft Remote Desktop Connection Client for Mac to display virtual desktops.

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.

vCenter Server

This service acts as a central administrator for VMware ESX 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 server, preferably on a VMware virtual machine.

Planning a Rich User Experience

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, however, you must understand the limitations and restrictions of each feature

This chapter includes the following topics:

- [“Feature Support Matrix,”](#) on page 15
- [“Choosing a Display Protocol,”](#) on page 16
- [“Accessing USB Devices Connected to a Local Computer,”](#) on page 18
- [“Printing from a View Desktop,”](#) on page 18
- [“Streaming Multimedia to a View Desktop,”](#) on page 19
- [“Using Single Sign-On for Logging In to a View Desktop,”](#) on page 19
- [“Using Multiple Monitors with a View Desktop,”](#) on page 19

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 client operating systems.

When planning which display protocol and features to make available to your end users, use [Table 2-1](#) to determine which client operating systems support the feature.

Table 2-1. Features Supported on 32-Bit Windows Clients

Feature	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1, SP2	Vista Ult SP1, SP2	Vista Ent SP2
USB access		X	X	X	X	X
RDP display protocol	X	X	X	X	X	X
PCoIP display protocol		X	X	SP2 only	SP2 only	X
HP RGS display protocol		X		X	SP2 only	X
Wyse MMR		X	X		SP1 only	

Table 2-1. Features Supported on 32-Bit Windows Clients (Continued)

Feature	Win 2000	Win XP Pro	Win XP Home	Vista Bus SP1, SP2	Vista Ult SP1, SP2	Vista Ent SP2
Virtual printing	X	X	X		SP1 only	
Offline Desktop		X				

NOTE The HP RGS and PCoIP display protocols are not available if you use the Web Portal instead of the native View Client. For information about client hardware requirements and View desktop requirements for PCoIP, see “[VMware View with PCoIP](#),” on page 17.

As [Table 2-2](#) shows, options are limited for Linux and Mac clients that are experimentally supported through Web Portal.

Table 2-2. Features That Web Portal Supports for Mac OS X and 32-Bit Linux Clients

Feature	Red Hat Ent Linux 5.1	SUSE Linux Ent Desktop 10	Ubuntu Linux 8.04	Mac OS X (10.5)	Mac OS X (10.4)
USB access					
RDP display protocol	X	X	X	X	X
PCoIP display protocol					
HP RGS display protocol					
Wyse MMR					
Virtual printing					
Offline Desktop					

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.

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 let end users choose the protocol when they log in to a desktop.

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 1920 x 1200 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.
- 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.
- PCoIP supports 32-bit color.
- PCoIP supports 128-bit encryption.
- PCoIP supports Advanced Encryption Standard (AES) encryption, which is turned on by default.
- You can use this protocol with your company's virtual private network.

PCoIP has the following limitations:

- The operating system on the View desktop must be Windows XP Professional SP 2 or 3, or Windows Vista SP 1 or 2.
- You cannot use the virtual printing feature with PCoIP.
- Using smart cards is not supported if you use PCoIP.
- Users who access their virtual desktops with View Portal cannot use PCoIP.

Client hardware requirements include the following:

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

View clients that use PCoIP can connect to View security servers, but PCoIP sessions with the virtual desktop ignore the security server. PCoIP uses the User Datagram Protocol (UDP) for streaming audio and video. Security servers support only TCP.

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 servers 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>.

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.
- If you use View Portal to access a View desktop, this feature is available only on Windows clients and then only if you first install View Client on the local Windows system with the optional USB redirection component.
- To use a USB printer in a View desktop, you must install the required print drivers in the View desktop.

Printing from a View Desktop

The virtual printing feature allows end users 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 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.

The virtual printing feature has the following limitations:

- This feature is not available if you use PCoIP.
- If you use View Portal to access a View desktop, this feature is available only on Windows clients and then only if you first install View Client on the local Windows system with the optional USB redirection component.
- This feature is not available for USB printers. To use a USB printer in a View desktop, you must install the required print drivers in the View desktop.

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 following media file formats:

- AC3
- MP3
- MPEG-1, MPEG-2, MPEG-4-part2
- WMA
- WMV 7, 8, and 9

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.

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.

SSO is implemented as an optional component that you can select when you install the View Agent on a desktop source. 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.

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.

This chapter includes the following topics:

- [“Advantages of Desktop Pools,”](#) on page 21
- [“Reducing and Managing Storage Requirements,”](#) on page 22
- [“Application Provisioning,”](#) on page 23
- [“Using Active Directory GPOs to Manage Users and Desktops,”](#) on page 24

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 server 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 vCenter 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 to all virtual desktops in a pool. The following examples show some of the settings available:

- Specify which 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.

In addition, using desktop pools provides many conveniences.

Persistent 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.

Nonpersistent pools The virtual desktop is optionally deleted and re-created after each use, offering a highly controlled environment. A nonpersistent 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 nonpersistent 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 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 22
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 22
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.

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 are 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.

When you create persistent desktop pools, View Composer also creates a separate user data disk for each virtual desktop. The end user's profile and application data are saved on the user data disk. VMware recommends that you keep user data disks on a separate datastore. You can then back up the whole LUN that holds user data disks.

Application Provisioning

With VMware View, you can use traditional application provisioning techniques, you can virtualize applications with VMware ThinApp, or you can you can deploy applications as part of a View Composer base image.

- [Deploying Applications and System Updates with View Composer](#) on page 23
Because linked-clone desktop pools share a base image, you can quickly deploy updates and patches by updating the parent virtual machine.
- [Virtualizing Applications with VMware ThinApp](#) on page 23
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 24
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

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.

Virtualizing Applications with VMware ThinApp

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.

When you create a virtualized application with ThinApp, users can either stream the application from a shared file server or copy the application to their virtual desktops. If you configure the virtualized application for streaming, you must address the following architectural considerations:

- Access for specific user groups to specific applications
- Storage configuration for the shared repository
- Network traffic generated by streaming, which depends largely on the type of application

For streamed applications, users can launch the applications directly from the shared file server, or indirectly, by using a desktop shortcut.

If you configure a ThinApp package file so that it is copied to a virtual desktop and run there, the architectural considerations are similar to those that you address when you use traditional MSI-based software provisioning.

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. 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 Object (GPO) templates for centralizing the management and configuration of View Manager 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 GPO templates, see the *View Manager Administration Guide*.

Architecture Design Elements and Planning Guidelines

4

A typical VMware View architecture design uses a building block strategy to achieve scalability. Each building block consists of components that support up to 1,000 virtual desktops. The overall design integrates 5 of these building blocks.

This architecture provides a standard, scalable design that you can adapt to your enterprise environment and special requirements. This chapter includes enough 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:

- [“Desktop Virtual Machine Configuration,”](#) on page 25
- [“vCenter and View Composer Virtual Machine Configuration and Desktop Pool Maximums,”](#) on page 30
- [“Connection Server Virtual Machine Configuration and Maximums,”](#) on page 31
- [“VMware View Node,”](#) on page 32
- [“vSphere Clusters,”](#) on page 33
- [“VMware View Building Blocks,”](#) on page 34
- [“VMware View Pod,”](#) on page 37

Desktop Virtual Machine Configuration

Virtual machines that are used as View desktops for end users do not require as much disk space and processing resources as server virtual machines.

When you create a virtual machine that is to be used as a View desktop, the choices that you make regarding RAM, CPU, and disk space have a significant effect on your choices for server hardware and expenditures.

- [Planning Based on Types of Workers](#) on page 26
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.
- [Allocating Memory to a Guest Operating System](#) on page 26
RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs, determining the correct memory allocation is crucial to planning your desktop deployment.

- [Estimating CPU Requirements for Virtual Desktops](#) on page 28
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 29
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.
- [Example Configuration for a Virtual Machine Desktop](#) on page 29
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 and Windows Vista virtual desktops.

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 those used by knowledge workers. Task workers who work specific shifts might all log in to their virtual desktop 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.

Allocating Memory to a Guest Operating System

RAM costs more for servers than it does for PCs. Because the cost of RAM is a high percentage of overall server hardware costs, 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.

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 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 server, you must set nonzero values for RAM reservation settings. Reserving some RAM guarantees that idle but in-use desktops are never completely swapped out to disk. However, higher reservation settings affect your ability to overcommit memory on an ESX server 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.

Windows page file

By default, this file is sized at 150 percent of guest RAM. This file, which is usually located at `C:\pagefile.sys`, causes linked-clone virtual machines and thin-provisioned storage to grow because it is accessed frequently. Reducing the size of the page file often reduces the size of virtual disks (`.vmdk` files) for linked clones. 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 Offline Desktop.

ESX 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 swap file is 1GB.

ESX 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 memory required depends in part on the number of monitors configured for end users and on the display resolution. [Table 4-1](#) lists the amount of memory 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.

Because you allocate RAM in increments, the table shows which increment to use. For example, a single-monitor configuration that uses VGA requires 37.03MB, but the smallest RAM increment is 64MB.

Table 4-1. PCoIP Client Display Overhead

Display Resolution Standard	Width, in Pixels	Height, in Pixels	1-Monitor Overhead (RAM Increments)	2-Monitor Overhead (RAM Increments)	4-Monitor Overhead (RAM Increments)
VGA	640	480	37.03MB (64MB)	44.06MB (64MB)	58.13MB (64MB)
SVGA	800	600	40.06MB (64MB)	51.97MB (64MB)	73.95MB (96MB)
720p	1280	720	51.09MB (64MB)	72.19MB (96MB)	114.38MB (128MB)
UXGA	1600	1200	73.95MB (96MB)	117.89MB (128MB)	205.78MB (256MB)
1080p	1920	1080	77.46MB (96MB)	124.92MB (128MB)	219.84MB (256MB)
WUXGA	1920	1200	82.73MB (96MB)	135.47MB (196MB)	240.94MB (256MB)
QXGA	2048	1536	102.00MB (128MB)	174.00MB (196MB)	318.00MB (384MB)
WQXGA	2560	1600	123.75MB (128MB)	217.50MB (256MB)	405.00MB (512MB)

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 1024MB for Windows XP desktops and 1536MB for Windows Vista 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.

CPU requirements vary by worker type. Software developers or other power users with high-performance needs might have much higher CPU requirements than knowledge workers. Knowledge workers, in turn, might have higher CPU requirements than data-entry task workers. During your pilot phase, use a performance monitoring tool, such as Perfmon, to understand both the average and peak CPU use levels for these groups of workers.

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 a sizing approach, VMware recommends that you determine how many virtual desktops can be accommodated per CPU core. A good starting point is to pilot 8 virtual machines per core. For example, if you monitor a single-core, 2.2GHz processor, physical PC and find that average CPU use is 2.79 percent, the amount of CPU is 130MHz. If you have a 2-socket quad core ESX server, you can host 64 virtual machines on the server during the pilot. Allocating 130MHz to each of the 64 virtual machines means that the total average CPU required is 8.3GHz.

In addition to the CPU required for the guest operating system and applications, you must also consider the additional processing power required for virtualizing the desktop and for utilization spikes. This overhead amounts to 10 to 25 percent of the average CPU. For this example, a conservative estimate of CPU required would be 25 percent of 8.3GHz. Therefore, the total CPU speed of the ESX server would have to be 10.38GHz.

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 VMware View user data 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 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 and setting a storage over-commit policy for View desktop pools.

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

Example Configuration for a Virtual Machine Desktop

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 and Windows Vista virtual desktops.

The example settings for virtual machines such as memory, number of virtual processors, and disk space are VMware View-specific and are based on information that was collected while validating the *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*. This architecture used VMware Infrastructure 3.5 to host and manage virtual machines. For information about limits of virtual machines in vSphere, see the *VMware vSphere Configuration Maximums* document.

The guidelines listed in [Table 4-2](#) are for a standard Windows XP virtual desktop.

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

Item	Example
Operating system	32-bit Windows XP (with the latest service pack)
RAM	1024MB (512MB low end, 2048 high end)
Virtual CPU	1
System disk capacity	16GB (8GB low end, 40GB high end)
User data capacity (either as a user data disk or as a redirected profile)	5GB (starting point)
Virtual SCSI adapter type	Use LSI Logic, which is not the default
Virtual network adapter	Use the default, which is operating system dependent

The amount of system disk space required depends on the number of applications required in the base image. The View reference architecture 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 user data disk. If you use a third-party profile management product, this data can be redirected in a Windows roaming profile to a CIFS file system.

The guidelines listed in [Table 4-3](#) are for a standard Windows Vista virtual desktop.

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

Item	Example
Operating system	32-bit Windows Vista (with the latest service pack)
RAM	1536MB (standard)
Virtual CPU	1
System disk capacity	20GB (standard)
User data capacity (either as a user data disk or as a redirected profile)	5GB (starting point)
Virtual SCSI adapter type	Use the default, which is LSI Logic
Virtual network adapter	Use the default, which is operating system dependent

vCenter and View Composer Virtual Machine Configuration and Desktop Pool Maximums

You install both vCenter 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 and View Composer on a physical machine, this example uses virtual machines with the specifications listed in [Table 4-4](#). The ESX server that hosts these virtual machines can be part of a VMware HA cluster to guard against physical server failures.

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

Item	Example
Operating system	32-bit Windows Server 2003 (with the latest service pack)
RAM	4 GB
Virtual CPU	2

Table 4-4. vCenter Virtual Machine Example and Pool Size Maximum (Continued)

Item	Example
System disk capacity	20GB
SCSI type	LSI Logic (the default for Windows Server 2003)
Network adapter	VM Network (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 http://www.vmware.com/support/vi3/doc/vc_db_calculator.xls.

Connection Server Virtual Machine Configuration and Maximums

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

View Connection Server Configuration

Although you can install View Connection Server on a physical machine, this example uses virtual machines with the specifications listed in Table 4-5. The ESX server that hosts these virtual machines can be part of a VMware HA cluster to guard against physical server failures.

Table 4-5. Connection Server Virtual Machine Example

Item	Example
Operating system	32-bit Windows Server 2003 (with the latest service pack)
RAM	4GB
Virtual CPU	2 or 4
System disk capacity	20GB
SCSI type	LSI Logic (the default for Windows Server 2003)
Network adapter	VM Network (the default)
1 NIC	1 Gigabit

Maximum Connections for View Connection Server

Table 4-6 provides information about the maximum number of simultaneous connections that a VMware View deployment can accommodate.

Table 4-6. View Desktop Connections

Connection Servers per Deployment	Connection Type	Maximum Number of Simultaneous Connections
1 Connection Server	Direct connection, RDP	2,000
5 Connection Servers	Direct connection, RDP	5,000
3 Connection Servers	Tunneled connection, RDP	2,000
1 Connection Server	Direct connection, PCoIP	2,000

Table 4-6. View Desktop Connections (Continued)

Connection Servers per Deployment	Connection Type	Maximum Number of Simultaneous Connections
1 Connection Server	Unified Access to physical PCs	100
1 Connection Server	Unified Access to terminal servers	200

Tunneled connections are required if you use security servers for RDP connections from outside the internal corporate network.

VMware View Node

A node is a single VMware ESX server that hosts virtual machine desktops in a VMware View deployment. A node can host 8 virtual machines per core and 64 virtual machines per LUN.

VMware View is most cost-effective when you maximize the number of desktops hosted on an ESX server. Although many factors affect server selection, if you are optimizing strictly for acquisition price, you must find server configurations that are not excessively limited by either CPU cores or RAM.

Generally, you can have 8 virtual machines per CPU core, but you must also consider physical RAM requirements. After you estimate how much RAM to allocate to each virtual machine, you can determine whether a given ESX server configuration is core limited or RAM limited. If a server is core limited, it has excess RAM when it runs at the maximum number of virtual machines per core. If a server is RAM limited, the physical RAM is consumed before the target number of virtual machines per core is achieved.

For information about calculating CPU requirements for each virtual machine, see [“Estimating CPU Requirements for Virtual Desktops,”](#) on page 28. For information about calculating the amount of RAM required per virtual machine, see [“Allocating Memory to a Guest Operating System,”](#) on page 26. Also consider 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.

Recommendations for ESX 3.5 node components in [Table 4-7](#) are VMware View-specific. For general information about limits of ESX hosts in vSphere, see the *VMware vSphere Configuration Maximums* document.

Table 4-7. VMware View Node Example for an ESX Server

Item	Example
ESX version	ESX 3.5 U4 or ESX 4.0 U1
Chassis type	Blade or rack
CPU	2- or 4-socket quad core
CPU speed	3.0GHz per core
RAM	128GB
Ethernet port	1 Gigabit
Virtual machines per core	8
Cores per node	8 for ESX 3.5, 16 for ESX 4.0 U1
NICs	4 (32 virtual machines per NIC)
View desktop storage density, in virtual machines per LUN	64
Fiber Channel adapter ports	0 or more

NOTE VMware View 3.x is not supported to run on vSphere 4.

vSphere Clusters

VMware View deployments can use VMware HA clusters to guard against physical server failures. Because each ESX server in a View cluster hosts more than 40 virtual machines, and 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 nonpersistent pool might have different recovery point objective (RPO) requirements than a persistent pool. For a nonpersistent 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 4-1. Cluster Configuration Example

The settings listed in [Table 4-8](#) are VMware View-specific. For information about limits of HA clusters in vSphere, see the *VMware vSphere Configuration Maximums* document.

Table 4-8. HA Cluster Example

Item	Example
Nodes (ESX servers)	8 (including 1 hot spare)
Cluster type	DRS (Distributed Resource Scheduler)/HA
Networking component	Standard ESX 3.5 or 4 cluster network
Switch ports	48 Managed GigE for ESX 3.5 or 80 for ESX 4

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 1,000-user building block consists of physical servers, a VMware vSphere infrastructure, VMware View servers, shared storage, and 1,000 virtual machine desktops. You can include up to five building blocks in a View pod.

Table 4-9. Example of a LAN-Based View Building Block

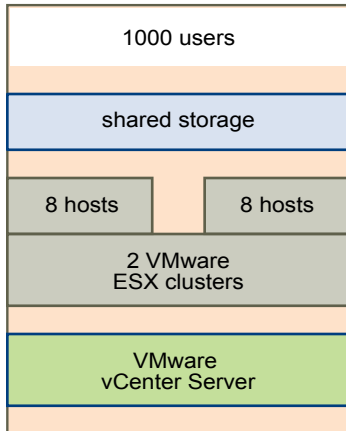
Item	Example
vSphere clusters	2 (with 8 ESX hosts in each cluster)
48-port network switch	1
Shared network storage component	1
vCenter Server with View Composer	1 (can be run in the block itself)
Database	MS 2005 SQL Server or Oracle database server (can be run in the block itself)
Shared storage component	1 (with 64 virtual machines per LUN)
Networks	3 (a 1Gbit Ethernet network for each: management network, storage network, and VMotion network)

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

This information was taken from the *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*.

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

Figure 4-1. VMware View Guiding Block



Shared Storage for View Building Blocks

Storage considerations are one of the main reasons that enterprises adopt virtualization technology. 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) or CIFS (Common Internet File System) NAS (network-attached storage). The ESX binaries, virtual machine swap files, and View Composer replicas of parent virtual machines are stored on this system.

From an architectural perspective, the decision about whether to use View Composer has the biggest impact on storage planning. 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 user data 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 user data 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 22.

Example 4-2. Storage Example

As a storage example, [Table 4-10](#) lists the storage components published in the *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*. This table provides some idea of the storage configuration required for a View building block that can accommodate 1,000 users.

Table 4-10. Example of an EMC NS20FC Storage Configuration

Item	Number
Celerra NS20FC with a CLARiiON CX3-10F back-end array	1
CLARiiON write cache	259MB
X-Blade 20 configurations	2
2.8GBz Pentium IV CPUs	2
Double-data rate RAM (266MHz)	4
Fibre Channel ports for back-end storage connectivity	2
10/100/1000 BaseT Ethernet ports	4
300GB/15K 2/4-GB Fibre Channel disks	30

Hardware Examples for View Building Blocks and Pods

The virtual infrastructure for a pod of VMware View building blocks resides on physical servers. VMware used blade server chassis to validate its building-block architecture, but you can use any type of server with the same hardware specifications.

Example 4-3. VMware View Infrastructure Hardware

Hardware similar to that shown in [Table 4-11](#) is capable of hosting infrastructure components for a View building block. Infrastructure components include virtual machine servers that host Active Directory, DNS, DHCP, View Connection Server instances, vCenter with View Composer, and the database for vCenter.

Table 4-11. Hardware Example for a Building Block with Infrastructure Components

Item	Number
16-slot blade chassis	1
Blade servers	4
Quad-core 2.66 GHz processors	4
RAM	32GB
72GB SAS drive	1
Broadcom Gb Ethernet adapters	4

Of the 4 blade servers, 2 are for load clients, 1 is for a View Connection Server instance, and 1 is for Active Directory, DNS, and DHCP.

Example 4-4. VMware View Desktop-Hosting Hardware

Hardware similar to that shown in [Table 4-12](#) is capable of hosting the virtual desktops for a View building block that accommodates 1,000 users.

Table 4-12. Hardware Example for a VMware View Building Block

Item	Number
16-slot blade chassis	1 for 2 building blocks
Blade servers	16 (8 for each cluster)
Quad-core 2.66 GHz processors	4
RAM	64GB (32GB for each cluster)
72GB SAS drive	2
Broadcom Gb Ethernet adapters	12 (6 for each cluster)
4-port gigabit uplink modules	12 (6 for each cluster)
Cisco 6500 core networking switch	1

Both the infrastructure components and the View desktops are part of VMware HA clusters to protect them from physical server failures.

This information was taken from *VMware View Reference Architecture: A Guide to Large-scale Enterprise VMware View Deployments*.

Bandwidth Considerations for a View Building Block

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

Peak Workloads

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-out policies during a pilot phase to determine whether suspending or powering off virtual machines when users log out causes an I/O storm.

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.

Display Traffic

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.

WAN Support

For wide-area networks (WANs), you must consider bandwidth constraints and latency issues.

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.

Table 4-13. Support for Small and Midsize Offices with WAN Optimization

Item	Small Office	Midsize Branch Office
Number of users	Up to 15	Up to 100
Link type	T1	10Mbps
Bandwidth	1.544Mbps	10Mbps
Latency	Up to 100ms	Up to 100ms

Users who access a View desktop with RDP display protocol from home by using a DSL or cable modem might not use a WAN optimizer. In this case, the network can accommodate 3 to 5 users.

This information was taken from the *VMware View WAN Reference Architecture*.

VMware View Pod

A VMware View pod integrates five 1,000-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 4-14](#) lists the components of a View pod.

Table 4-14. Example of a VMware View Pod

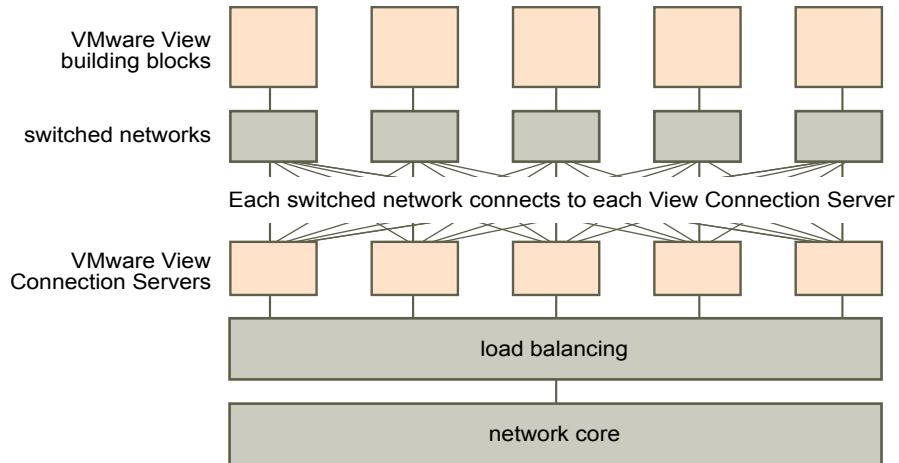
Item	Number
View building blocks	5
View Connection Servers	5 (one for each building block)
View Security Servers	2 - 5 (load-balanced in the DMZ)
10Gb Ethernet module	1
Modular core networking switch	1
Load-balancing module	1
VPN for WAN	1 (optional)
WAN accelerator if using RDP	1 (optional)

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 5,000 View Desktops



Planning for Security Features

View Manager offers strong network security to protect sensitive corporate data. For added security, you can integrate View Manager 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,”](#) on page 39
- [“Choosing a User Authentication Method,”](#) on page 41
- [“Preparing to Use a Security Server,”](#) on page 43
- [“Restricting View Desktop Access,”](#) on page 51

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 provides an IP address to View Client. The View Administrator connection is created when an administrator types the View Administrator URL into a Web browser.

View Manager includes a default self-signed SSL certificate that clients can use when they connect to a View Connection Server host. By default, clients are presented with this self-signed SSL certificate when they visit a secure page such as View Administrator.

You can use the default SSL certificate for testing. Because it is not trusted by clients and does not have the correct name for the service, you must replace the default SSL certificate. You can create your own self-signed certificate, obtain a signed certificate from a Certificate Authority (CA), or use a SSL certificate that you already have.

- [Tunneled Client Connections with Microsoft RDP](#) on page 40

When users connect to a View desktop with the Microsoft RDP display protocol, View Client makes 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 with PCoIP and HP RGS](#) on page 40

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 Offline Desktop Client Connections](#) on page 41

View Client with Offline Desktop is an experimental feature that offers mobile users the ability to check out a cloned instance of certain types of View desktops onto their local computer.

Tunneled Client Connections with Microsoft RDP

When users connect to a View desktop with the Microsoft RDP display protocol, View Client makes 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 View Manager 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 43 for information on DMZ deployments and security servers.

Clients that use the PCoIP or HP RGS display protocols do not use the tunnel connection. See [“Direct Client Connections with PCoIP and HP RGS,”](#) on page 40 for more information.

Direct Client Connections with PCoIP and HP RGS

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 is still 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.

If clients use the PCoIP or HP RGS display protocols, you must enable direct client connections.

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. See [“Tunneled Client Connections with Microsoft RDP,”](#) on page 40 for more information.

View Client with Offline Desktop Client Connections

View Client with Offline Desktop is an experimental feature that offers mobile users the ability to check out a cloned instance of certain types of View desktops onto their local computer.

View Client with Offline Desktop 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 Offline Desktop client system and the View desktop virtual machine.

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

Choosing a User Authentication Method

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

- [Active Directory Authentication](#) on page 41

Each View Connection Server instance is joined to an Active Directory domain, and users are authenticated against Active Directory for the joined domain.

- [RSA SecurID Authentication](#) on page 42

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 42

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 43

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 `vdadmin` command to configure domain filtering, which limits the domains that a View Connection Server instance or security server searches, and that it displays to users. See the *Command-Line Tool for View Manager* technical note 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 configure a different user authentication method on others. For example, you can configure RSA SecurID authentication only for users that access View desktops remotely over the Internet.

View Manager 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).

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.

Each client system that uses smart card authentication must have a Windows-compatible smart card reader and product-specific application drivers.

Smart card authentication is supported by View Client only. It is not supported by View Client with Offline Desktop, View Portal, or View Administrator.

Smart card authentication is not supported for clients that use the PCoIP display protocol.

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 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.

NOTE When smart card authentication is required, authentication fails for users who select the **Log in as current user** check box. These users must reauthenticate with their smart card and PIN when logging in to a View desktop.

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 demilitarized zone (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 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 a few 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 50 for information on specific ports.

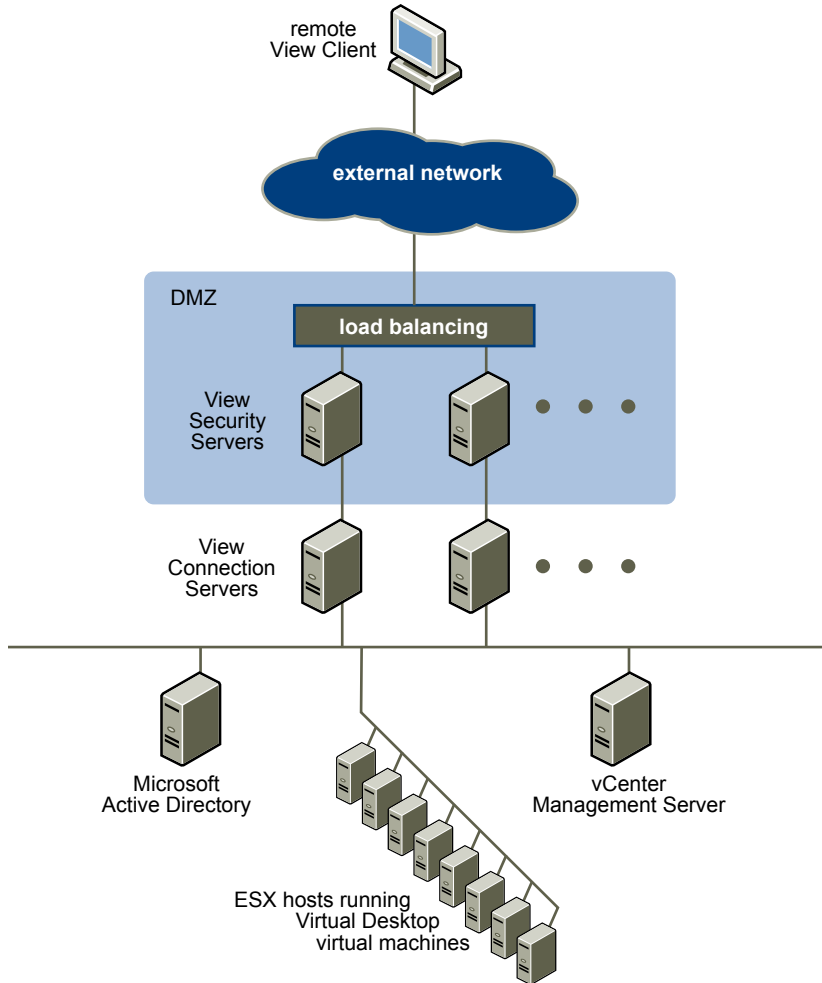
Because users can connect directly with any View Connection Server instance from within their internal network, you do not need to implement a security server in a LAN-based deployment.

View clients that use PCoIP can connect to View security servers, but PCoIP sessions with the virtual desktop ignore the security server. PCoIP uses the User Datagram Protocol (UDP) for streaming audio and video. Security servers support only TCP.

Security Server Topologies

You can implement several different security server topologies.

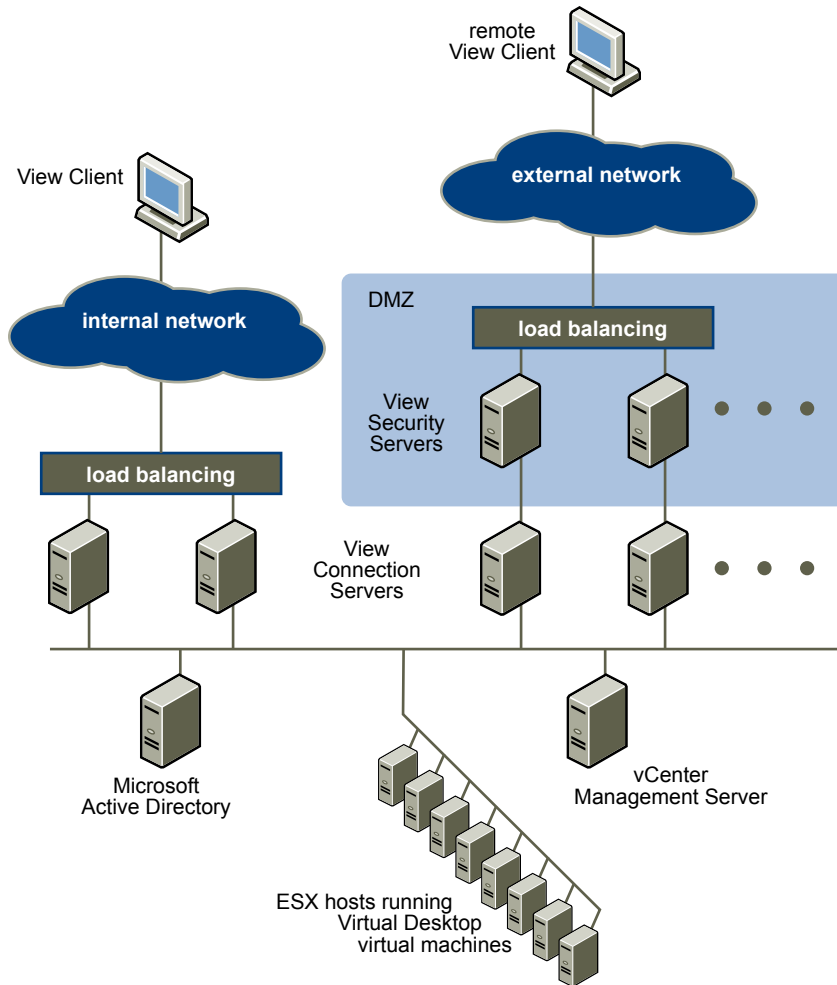
The topology illustrated in [Figure 5-1](#) shows a high-availability environment that includes two load-balanced security servers in a DMZ. The security servers communicate with two View Connection Server instances inside the internal network.

Figure 5-1. 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 5-2](#) 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 5-2. Multiple Security Servers

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

Firewalls for DMZ-Based Security Servers

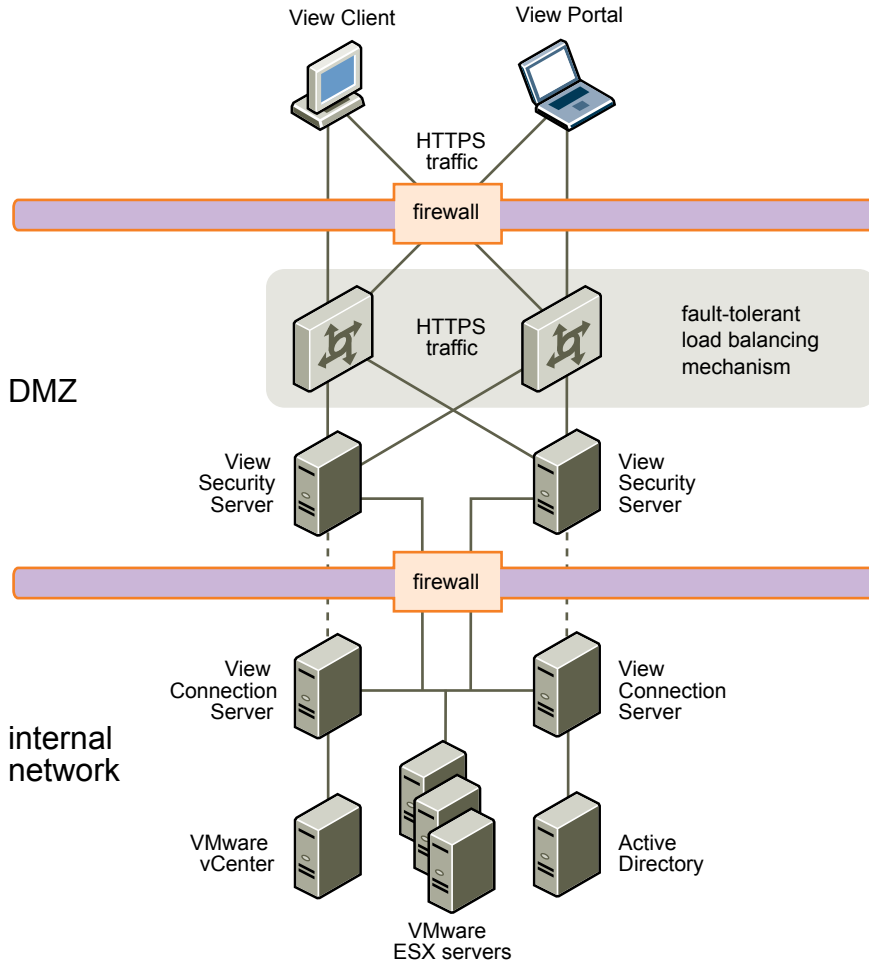
A DMZ-based security server deployment must include two firewalls.

- 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 5-3 shows an example of a configuration that includes front-end and back-end firewalls.

Figure 5-3. Dual Firewall Topology

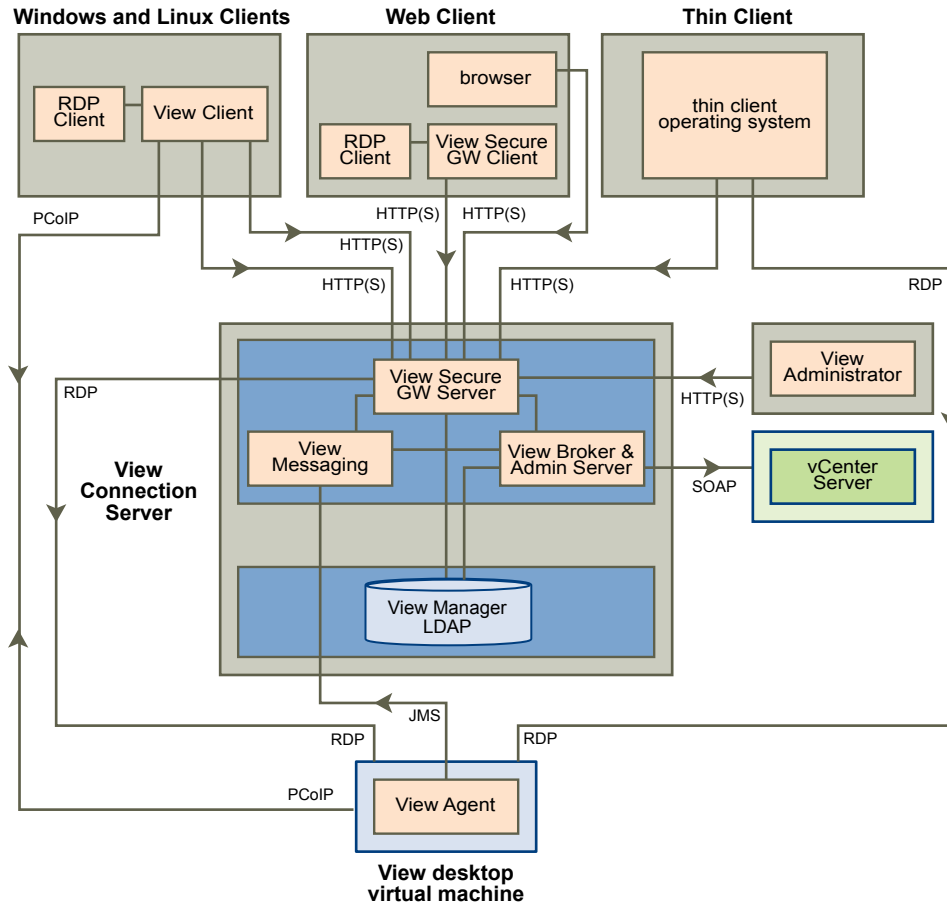


View Manager Components and Protocols

View Manager components exchange messages by using several different protocols.

Figure 5-4 illustrates the relationships between the View Manager components, including the protocols that each component uses for communication, when a security server is not configured.

Figure 5-4. View Manager Components and Protocols without a Security Server



See [Table 5-1](#) for the default ports that are used for each protocol.

[Figure 5-5](#) illustrates the relationships between the security server and all other View Manager components, including the protocols that each component uses for communication, when a security server is configured.

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

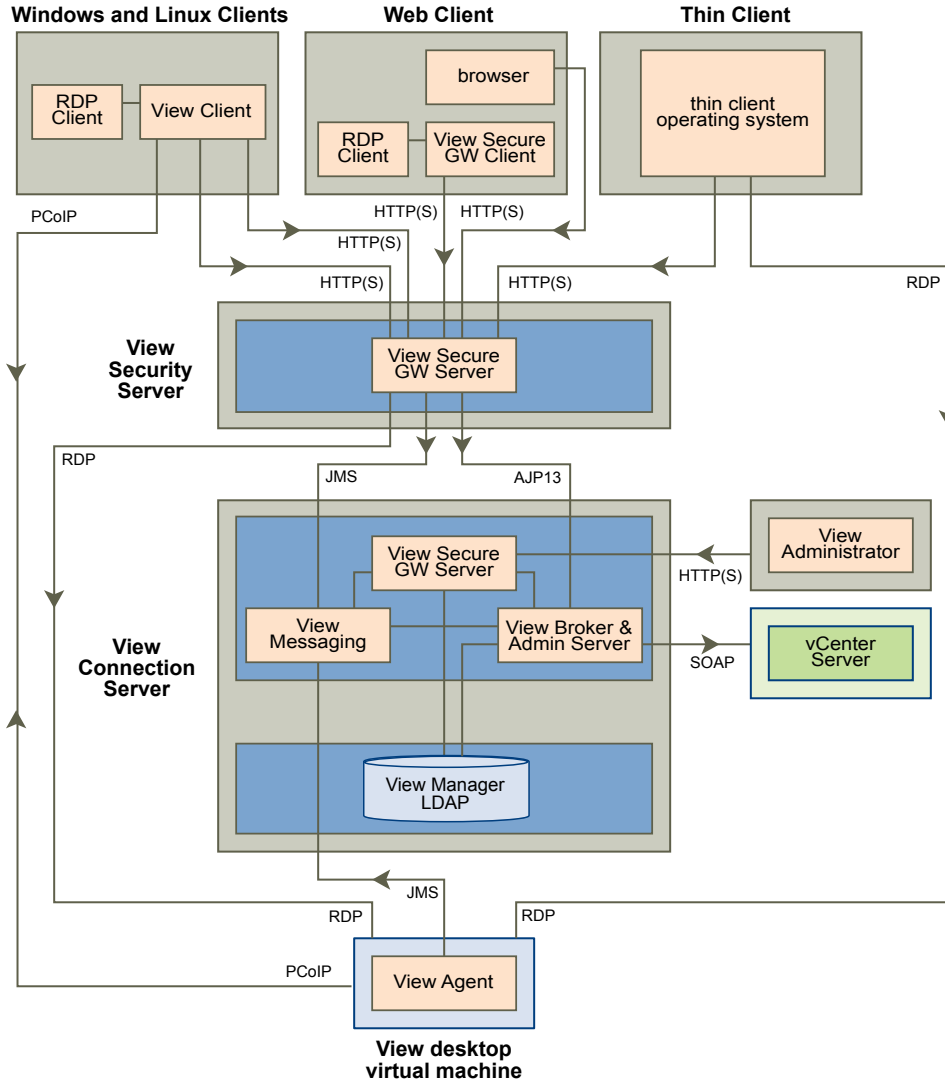


Table 5-1 lists the default ports that are used for each protocol.

Table 5-1. Default Ports

Protocol	Port
JMS	TCP port 4001
AJP13	TCP port 8009 <i>NOTE</i> 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. <i>NOTE</i> 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 5-1. Default Ports (Continued)

Protocol	Port
SOAP	TCP port 80 or 443
PCoIP	TCP port 50002 from View Client to the View desktop. PCoIP also uses UDP port 50002 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 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 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 PCoIP and HP RGS do not use the tunnel connection.

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

View LDAP

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

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

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 inbound traffic on certain TCP ports. [Table 5-2](#) summarizes the front-end firewall rules.

Table 5-2. 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).

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 5-3](#) summarizes the back-end firewall rules.

Table 5-3. Back-End Firewall Rules

Source	Protocol	Port	Destination	Notes
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.

TCP Ports for View Connection Server Communication

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 traffic to each other.

Because firewalls are generally not used between the View Connection Server instances in a group, those TCP ports are not described here.

General Firewall Rules for View Manager Components

In any firewall configuration, TCP ports must be opened to allow traffic between certain View Manager components.

See [“Firewall Rules for DMZ-Based Security Servers,”](#) on page 50 for firewall rules that are specific to security server implementations.

Firewall Rules for View Agent

Table 5-4 lists the TCP ports that are opened on the firewall by the View Agent installation program. Ports are incoming TCP ports unless otherwise noted. See “View Manager Components and Protocols,” on page 46 for information on protocol direction.

Table 5-4. TCP Ports Opened During View Agent Installation

Protocol	Ports
RDP	3389
USB redirection	32111
MMR	9427
PCoIP	50002 (TCP and UDP)
HP RGS	42966

The View Agent installer 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.

The HP RGS Sender application is the server-side component of the HP RGS remote display protocol and 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 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 Offline Desktop

View Client with Offline Desktop data is downloaded and uploaded through port 902. If you intend to use the View Client with Offline Desktop feature, this port must be accessible to your ESX host.

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.

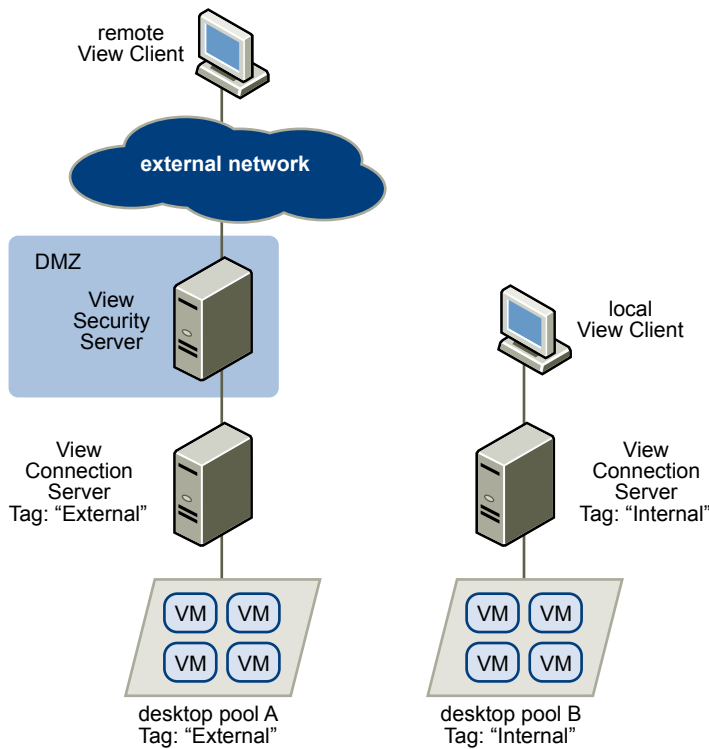
With restricted entitlements, you assign one or more tags to a View Connection Server instance. Then, when configuring a desktop or desktop pool, you select the tags of the View Connection Server instances that you want to be able to access the desktop or desktop pool. When users log in through a tagged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

For example, your 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 desktops and desktop pools that should be accessible only to internal users.
- Assign the "External" tag to the desktops and desktop pools that should be accessible only to external users.

External users cannot see the desktops and desktop pools tagged as Internal because they log in through the View Connection Server tagged as External, and internal users cannot see the desktops and desktop pools tagged as External because they log in through the View Connection Server tagged as Internal. [Figure 5-6](#) illustrates this configuration.

Figure 5-6. 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 desktops 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.

Overview of Steps to Setting Up a VMware View Environment

6

The View Installation and Setup check list shows you all the high-level tasks for creating a View deployment, tells what order to do them in, and specifies which documents provide instructions.

Table 6-1. View Installation and Setup Check List

Step	Task
1	Set up the required administrator users and groups in Active Directory. Instructions: <i>VMware View Manager Administration Guide</i> and the vSphere documentation
2	(Optional) Install and set up VMware ESX servers and vCenter Server Instructions: vSphere documentation, Documentation Roadmap
3	(Optional) Install View Composer on vCenter Server. Instructions: <i>VMware View Manager Administration Guide</i>
4	Install View Connection Server. Instructions: <i>VMware View Manager Administration Guide</i>
5	Copy the Active Directory GPO templates from the View Connection Server machine to the Active Directory server and import them. Instructions: <i>VMware View Manager Administration Guide</i>
6	Do an initial configuration of View Connection Server. Instructions: <i>VMware View Manager Administration Guide</i>
7	Create one or more virtual machines that can be used as a template for full-clone desktop pools or for as a parent for linked-clone desktop pools. Install the desired applications or VMware ThinApp applications. Instructions: vSphere documentation, Documentation Roadmap, and the <i>Windows XP Deployment Guide</i> for VMware View
8	Install View Agent on the virtual machines and physical machines you want to use as desktop sources. Instructions: <i>VMware View Manager Administration Guide</i>
9	Create an individual View desktop or a View Desktop Pool, or both. Instructions: <i>VMware View Manager Administration Guide</i>
10	Entitle users or user groups or both to desktops. Instructions: <i>VMware View Manager Administration Guide</i>
11	Set desktop policies. Instructions: <i>VMware View Manager Administration Guide</i>
12	Install View Client on end users' machines or direct them to use View Portal to install the required components. Instructions: <i>VMware View Manager Administration Guide</i>

Table 6-1. View Installation and Setup Check List (Continued)

Step	Task
13	Have end users access their View desktops. Instructions: <i>VMware View Manager Administration Guide</i>
14	Manage and monitor users and desktops. Instructions: <i>VMware View Manager Administration Guide</i>

Index

A

Active Directory **8, 24, 41**
Administration Server **49**
Adobe Flash **21**
agent, View **12**
AJP13 protocol **46, 50**
application virtualization and provisioning **23, 24**
architectural design elements **25**

B

back-end firewall
 configuring **45**
 rules **50**
bandwidth **36, 37**
base image for virtual desktops **22**
blade servers **35**
browsers, supported **12**

C

checklist for setting up VMware View **53**
client connections
 direct **40**
 tunnel **40**
clones, linked **12, 23**
cluster, vSphere **33**
communication protocols, understanding **46**
connection types
 client **39**
 direct **40**
 external client **43**
 tunnel **40**
cores, virtual machines density **28**
CPU estimates **28, 29**
credentials, user **43**

D

database sizing **30**
database types **34**
datastores **22**
demilitarized zone **43, 45**
desktop as a managed service (DAAS) **7**
desktop pools **12, 21, 22**
desktop sources **21**
diagram of a View deployment **9**
direct client connections **31, 40**

disk space allocation for virtual desktops **29**
display protocols
 defined **16**
 HP RGS **15, 18, 40**
 Microsoft RDP **15, 17, 40**
 PCoIP **40, 43**
 View PCoIP **8, 15, 17**
Distributed Resource Scheduler (DRS) **33**
DMZ **11, 43, 45**
dual-firewall topology **45**

E

encryption
 of user credentials **43**
 supported by Microsoft RDP **17**
 supported with PCoIP **17**
entitlements, restricted **51**
ESX hosts **32**

F

feature support matrix **15**
Fibre Channel SAN arrays **22**
firewalls
 back-end **45**
 front-end **45**
 rules **50**
front-end firewall
 configuring **45**
 rules **50**

G

gateway server **49**
GPOs **24**

H

HA cluster **30, 31, 33, 35**
HP RGS **15, 18, 40**

I

I/O storms **36**
iSCSI SAN arrays **22**

J

Java Message Service **49**
Java Message Service protocol **50**
JMS protocol **46, 50**

K

knowledge workers **26**

L

latency **37**

LDAP directory **11, 49**

legacy PCs **10**

linked clones **12, 22, 23, 31, 34**

Linux clients **12**

load balancing, View Connection Server **37, 43**

Log in as current user feature **19, 43**

LUNs **22**

M

Mac clients **10, 12**

media file formats supported **19**

memory allocation for virtual machines **26, 29**

messaging router **49**

Microsoft RDP **15, 17, 19, 40**

Microsoft Remote Desktop Connection Client for
Mac **12**

multimedia streaming **19**

multiple monitors **8, 17, 19**

N

NAS arrays **22**

network bandwidth **36**

nonpersistent desktop pools **21**

P

parent virtual machine **22, 23**

PCoIP **7, 8, 15, 17, 40, 43**

persistent desktop pools **21, 22**

physical PCs **31**

policies, desktop **24**

pools, desktop **12, 21, 22**

power users **26**

printing, virtual **18**

processing requirements **28**

provisioning desktops **7**

R

RAM allocation for virtual machines **26, 29**

rdesktop **12**

rebalance feature **22**

recompose feature **23**

refresh feature **23, 29**

replicas **22**

restricted entitlements **51**

RSA SecurID authentication **42**

S

scalability, planning for **25**

SCSI adapter types **29**

security features, planning **39**

security servers

implementing **43**

load balancing **43**

overview **11**

setup, VMware View **53**

shared storage **22, 34**

single sign-on (SSO) **12, 19, 43**

smart card authentication **42**

smart card readers **18, 42**

snapshots **23**

software provisioning **23, 24**

storage, reducing, with View Composer **22**

storage configurations **34**

streaming applications **23**

streaming multimedia **19**

suspend files **26, 29**

swap files **26**

T

task workers **26**

TCP ports **50**

templates, GPO **24**

terminal servers **31**

thin client support **10, 15**

ThinApp **23**

tunnel connection **31, 40**

tunneled communications **41, 49**

U

Unified Access **31**

USB devices, using with View desktops **8, 15, 18**

user authentication

Active Directory **41**

methods **41**

RSA SecurID **42**

smart cards **42**

user data disks **22**

user types **26**

V

vCenter, configuration **30**

vCenter Server **12, 21**

View Administrator **12, 24**

View Agent **12, 24**

View Broker **49**

View building block **34**

View Client **11, 24**

- View Client for Linux **11**
 - View Client with Offline Desktop, connections **41**
 - View Composer, operations **31, 34**
 - View Connection Server
 - configuration **12, 31**
 - grouping **43**
 - load balancing **43**
 - overview **11**
 - RSA SecurID authentication **42**
 - smart card authentication **42**
 - View deployment diagram **9**
 - View desktop configurations **25**
 - View Messaging **49**
 - View node configuration **32**
 - View Offline Client **15**
 - View Open Client **11**
 - View pod **35, 37**
 - View Portal **10, 12**
 - View Portal for Linux **11**
 - View Portal for Mac OS X **11**
 - View Secure Gateway Server **49**
 - virtual machine configuration
 - for vCenter **30**
 - for View Composer **30**
 - for View Connection Server **31**
 - for View desktops **25**
 - virtual printing feature **8, 15, 18**
 - virtual private networks **17, 43**
 - .vmdk files **29**
 - VMotion **33**
 - vSphere **7, 8, 22**
 - vSphere cluster **33, 34**
- ## **W**
- WAN configurations **34**
 - WAN support **37**
 - Windows page file **29**
 - worker types **25, 26, 28**
 - Wyse MMR **15, 19**

