Administration Guide

View Manager 3.0.1

vmware®

Administration Guide
Item: EN-000083-01

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

About This Book

This guide describes how to install, configure, and use VMware® View Manager, including how to install the various software components, how to deploy servers, and how to configure and connect to virtual desktops. It also describes how to set up load balancing and security, supported operating systems, and thin client devices.

This chapter includes these topics:

Intended Audience

This book is intended for anyone who wants to install, administrate, or configure View Manager. The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

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 sections describe the technical support resources 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

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.

1 Introduction

View Manager 3.0.1 is a flexible and intuitive desktop management solution that enables system administrators to rapidly provision desktops and control user access. Client software connects users to virtual desktops running on VMware Virtual Infrastructure, or to physical systems running within your network environment.

This chapter provides a brief overview of the features offered by View Manager and describes the system requirements for installing and running the software components associated with this application.

This chapter discusses the following topics:

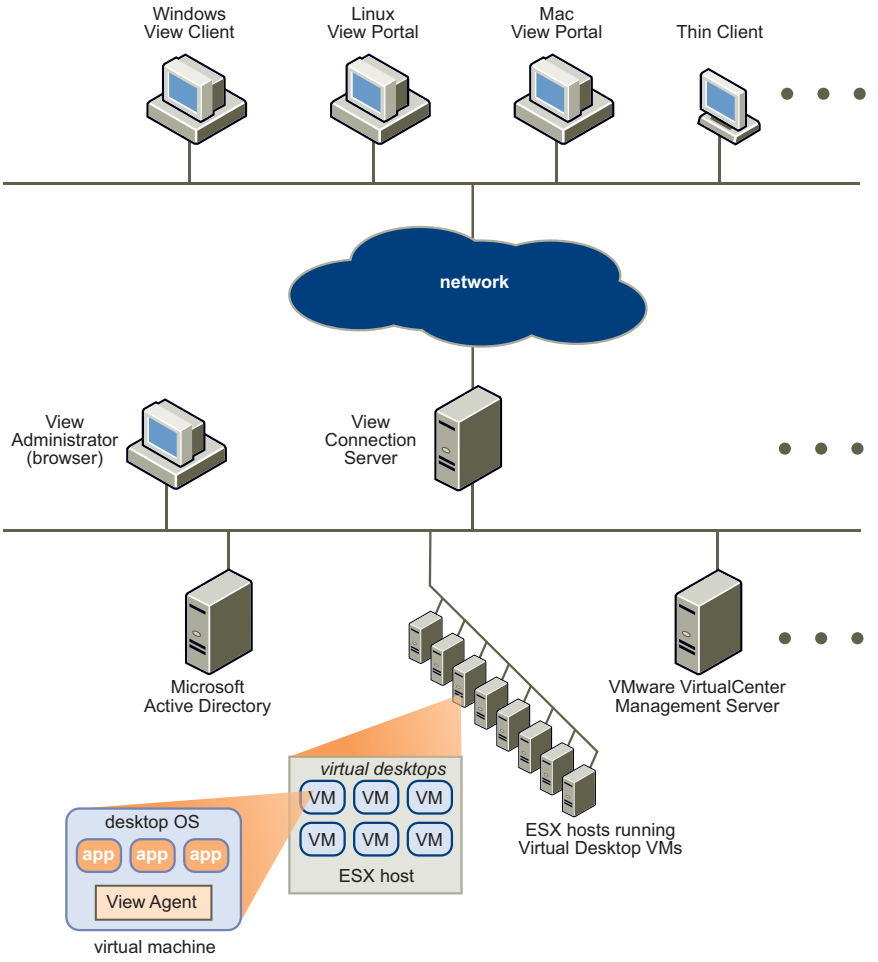
Overview of View Manager

View Manager integrates with VMware VirtualCenter in order to allow administrators to create desktops from virtual machines running on VMware ESX server and then deploy them to end-users. In addition, View Manager utilizes your existing Active Directory infrastructure for user authentication and management.

Once a desktop has been created, Web-based or locally installed client software enables authorized end-users to securely connect to centralized virtual desktops, back-end physical systems, or terminal servers.

Figure 1-1 shows a high-level view of an example View Manager environment and its main components—these components are described in more detail in later sections of this book.

Figure 1-1. Example High-Level View of a View Manager Environment



View Manager Features

The major features of View Manager are described below:

- Enterprise-class connection brokering—View Manager manages the connections between users and their virtual desktops. When users connect to View Manager, the virtual desktops they are authorized to access are displayed.
- "Smart pooling" capabilities—A range of persistent and non-persistent pooling capabilities simplifies the provisioning and management of centralized desktops.

- Flexible deployment options—View Manager components can be deployed in a variety of configurations and to different parts of the network, which improves security, scalability, and reliability. In addition, multiple VirtualCenter servers are supported, and View Manager can scale horizontally to support many virtual desktops.
- High availability—Servers can be clustered for high availability and scalability with automatic failover. These servers can also leverage industry-standard load-balancing solutions.
- Integration with Microsoft Active Directory—Connection to Active Directory allows you to locate user and user group accounts and use authentication features in order to control which users can access virtual desktops.
- Seamless integration with VMware Virtual Infrastructure (VI)—Works with VMware VirtualCenter to provide advanced virtual desktop management capabilities, such as automatic suspend and resume, which reduces the memory and processing power required to host virtual desktops.

  By leveraging the capabilities of VMware Virtual Infrastructure, desktops can run even when server hardware fails and recover quickly from unplanned outages without duplicate hardware.
- Secure access—Optional secure encapsulation capabilities allow all network connections to be encrypted.
- Support for two-factor authentication—With RSA SecurID, access control is strengthened.
- USB client device and virtual printing support—USB devices and printers can be locally connected to clients yet accessed from a virtual desktop.
- Web-based management user interface—A Web-based administrative console allows virtual desktops to be managed from any location.
- Support for non-VI systems—physical machines or terminal services systems can be also managed by View Manager, ensuring a seamless integration of existing architectures into the VDI environment.
- Scalable virtual infrastructure—linked clone technology allows multiple desktops to be deployed from a single base image. Subsequent changes to this image can be automatically proliferated amongst all desktops in linked clone pool.
- View Manager 3.0.1 is a fully internationalized product.

View Manager Components

View Manager consists of the following major components:

- View Connection Server—a software service that acts as a broker for client connections by authenticating and then directing incoming remote desktop user requests to the appropriate virtual desktop, physical desktop, or terminal server.
- View Agent—a software service that is installed on all guest virtual machines, physical systems, or terminal servers in order to allow them to be managed by View Manager. The agent provides features such as RDP connection monitoring, virtual printing, remote USB support, and single sign on.
- View Client—a locally installed software application that communicates with View Connection Server in order to allow users to connect to their desktops using the Remote Desktop Protocol (RDP).
- View Client with Offline Desktop—a version of View Client that is extended to support the Offline Desktop feature which allows users to download virtual machines and use them on their local systems.
- View Portal—a Web-based version of View Client supported by multiple operating systems and browsers.
- View Administrator—a Web application that allows View Manager administrators to configure View Connection Server, deploy and manage desktops, control user authentication, initiate and examine system events, and carry out analytical activities.
- View Composer—a software service that is installed on the VirtualCenter server in order to allow View Manager to rapidly deploy multiple linked clone desktops from a single centralized base image.

System Requirements

The following sections describe the hardware and software requirements for the major components provided as part of View Manager.

NOTE VMware includes certain "experimental features" in some of our product releases. These features are there for you to test and experiment with. We do not expect these features to be used in a production environment. However, if you do encounter any issues with an experimental feature, we are interested in any feedback you are willing to share. Please submit a support request via the normal access methods. You will receive an auto-acknowledgement of your request. We cannot, however, commit to troubleshoot, provide workarounds or provide fixes for these experimental features.

View Connection Server

View Connection Server is not supported on servers that have the Windows Terminal Server role installed. Remove the Windows Terminal Server role from any server on which you will be installing View Connection Server.

View Connection Server runs on a 32-bit or 64-bit dedicated physical or virtual server with the following specifications:

- Pentium IV 2.0Ghz processor or higher—dual processors are recommended
- 2GB RAM or higher—3GB RAM is recommended for deployments of 50 or more View Manager desktops
- One or more 10/100Mbps network interface controllers (NIC)—1Gbps NIC is recommended

---

NOTE The above specifications apply to any additional View Connection Server instances that are installed in your environment for the purposes of high availability or external access.

Supported Operating Systems

The View Connection Server can be installed on the following 32-bit operating systems:

- Windows Server 2003 R2 Standard Edition with SP2
- Windows Server 2003 Standard Edition with SP2
- Windows Server 2003 R2 Enterprise Edition with SP2
- Windows Server 2003 Enterprise Edition with SP2

Prerequisites

View Connection Server has the following prerequisites:

- A valid license key for View Manager. The following types of license are available:
  - View Manager
  - View Manager with View Composer
  - View Manager with View Composer, and Offline Desktop
- VMware Infrastructure 3.0.2 (supported) or VMware Virtual Infrastructure 3.5 (recommended). Both ESX and ESXi 3.5 are supported.

  NOTE VMware Infrastructure 3.5 U3 is required in order to use the View Composer (linked clone) and Offline Desktop features.

- Host operating systems for standard or replica View Connection Server instances are joined to an Active Directory domain. The following versions of Active Directory are supported:
  - Windows 2000 Active Directory
  - Windows 2003 Active Directory

  NOTE View Connection Server does not make nor require any schema or configuration updates to Active Directory.

- In order to apply customization specifications to standard (non-linked clone) desktop pools, Microsoft Sysprep tools must be installed on your VirtualCenter server

RSA Authentication Manager

View Connection Server has been certified with version 6.1 and 7.1 of RSA Authentication Manager. Other versions of RSA Authentication Manager that are compatible with version 6.1 are also supported.

Operating System Support for Installed Components

Table 1-1 describes the support offered by various types of Windows operating system to the locally installed components of View Manager. For each of these components, only 32-bit support is offered. Any additional environmental requirements of these components are described in subsequent sections. The columns represented in this table are:

- View Agent—refers to the View Agent service that is installed on a View Manager desktop. The entries in this column are the operating systems that can be managed by View Manager. The column is divided into two sub-columns:
  - Virtual—refers to the virtual systems supported as guests. These systems could reside within Virtual Infrastructure where they are provisioned and managed, or could exist as standalone systems within another VMware application such as VMware Server.
  - Physical—refers to the physical systems supported as alternate multiple back-ends, including terminal servers.
- View Client—refers to the View Client application. The entries in this column are the operating systems capable of installing and running this application.

- Offline Desktop—refers to the View Client for Offline Desktop application. The entries in this column are the operating systems capable of installing and running this application. For a list of the View Manager desktops that can be downloaded and used in an offline context, refer to "View Client with Offline Desktop: Supported Guests" on page 20.
- View Composer—refers to the View Composer service that runs on the VirtualCenter host system. The entries in this column are the operating systems capable of running this service.

NOTE The requirements for View Connection Server are not included in this table—refer to "View Connection Server" on page 15 for detailed information about this component.

Table 1-1. Operating System Support (32-bit) for Installed Components

Operating System	View Agent		View Client	Offline Desktop
	Virtual	Physical		
Windows 2000 Professional SP4			Yes	
Windows XP Professional SP1	Yes	Yes	Yes	
Windows XP Professional SP2	Yes	Yes	Yes	Yes
Windows XP Professional SP3	Yes	Yes	Yes	Yes
Windows XP Home SP2			Yes	
Windows XPe			Yes	
Windows Vista Home			Yes	
Windows Vista Home Premium			Yes	
Windows Vista Business	Yes	Yes	Yes	
Windows Vista Business SP1	Yes	Yes	Yes	
Windows Vista Enterprise SP1	Yes	Yes		
Windows Vista Ultimate			Yes	
Windows Vista Ultimate SP1	Yes	Yes	Yes	
Windows Server 2003 Enterprise Terminal Server		Yes		
Windows Server 2003 Enterprise Terminal Server SP2		Yes		
Windows Server 2003 SP1				

Operating System Support for Web Components

Table 1-2 describes the support offered by various types of operating system to the Web-based components of View Manager, with the specific browser and additional software requirements also provided. Any additional environmental requirements of the Web-based components are described in subsequent sections.

Table 1-2. Operating System Support for Web-Based Components (32-bit)

Operating System	View Portal	View Administrator
Windows 2000 Professional SP4		Internet Explorer 6 Internet Explorer 7 Firefox 2.0 Firefox 3.0
Windows XP Professional SP1	Internet Explorer 6 SP2 Internet Explorer 7	
Windows XP Professional SP2		
Windows XP Professional SP3		
Windows XP Home SP2		
Windows Vista Home	Internet Explorer 7	
Windows Vista Home Premium		
Windows Vista Business		
Windows Vista Business SP1		
Windows Vista Ultimate		
Windows Vista Ultimate SP1		
RHEL 5.0, Update 1	Firefox 2.0 / 3.0 Java JRE 1.5.0 or 1.6.0 rdesktop	
SLES 10 SP1		
Ubuntu 8.04		
Mac OS/X Tiger (10.4)	Safari Java JRE 1.5.0 RDC 2.0	
Mac OS/X Leopard (10.5)		

View Agent

You must have administrative privileges to install View Agent on Windows View Manager desktops.

View Composer

You cannot use the View Composer feature of View Manager to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1. For more information about View Composer, refer to Chapter 6, “View Composer,” on page 93.

Volume Licensing and Windows Vista Ultimate

Windows Vista Ultimate is not designed for broad enterprise deployment and therefore does not support volume licensing—in order to deploy desktop clones that use Windows Vista Ultimate, you must first contact Microsoft in order to determine your licensing obligations.

View Client / View Client with Offline Desktop

You must have administrative privileges to install View Client or View Client with Offline Desktop on the client desktop. In order to redirect the USB devices attached to the client system for use on the View Manager desktop, you must enable the USB redirection feature when you install either client application.

NOTE Offline Desktop is an experimental feature. Please refer to "System Requirements" on page 14 for more information about experimental features.

Remote Desktop Connection

Microsoft Remote Desktop Connection (RDC) 6.1 is recommended, RDC 5.0 and RDC 6.0 are supported—you must have at least RDC 6.0 installed in order to have multi-monitor support. RDC 6.1 can be downloaded from the following location:

http://microsoft.com/downloads/details.aspx?familyid=6E1EC93D-BDBD-4983-92F7-479E088570AD

View Client with Offline Desktop: Product Compatibility

You cannot install View Client with Offline Desktop on any system that has the following applications installed:

- VMware ACE
- VMware Player
- VMware Server
- VMware Workstation

The above applications must be uninstalled prior to installing View Client with Offline Desktop.

View Client with Offline Desktop: Supported Guests

The following 32-bit operating systems can be downloaded and used by View Client with Offline Desktop:

- Windows XP Professional SP2
- Windows XP Professional SP3

View Client and View Client with Offline Desktop: MMR

The multimedia redirection (MMR) feature redirects certain multimedia codecs running on the remote desktop to the local client for rendering of full-motion video and audio. Windows XP and XPe are the only client operating systems that support MMR on View Client and View Client with Offline Desktop. MMR supports the following media formats:

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

The recommended application to use with these files is Windows Media Player 10—this application supports MMR and should be installed on both the client and View Manager desktop.

NOTE MMR will not work correctly if the View Client video display hardware does not have overlay support.

View Portal

ActiveX controls are required for Windows users who access their desktops using View Portal on Internet Explorer 6 or higher.

Before connecting to a Windows desktop using the View Portal on a Linux system, you must install rdesktop 1.5.0. You can download rdesktop from the following location:

http://www.rdesktop.org

After you download rdesktop, follow the instructions in the `readme` file.

Mac Operating System Support

View Portal is an experimental feature on Mac OS. Please refer to "System Requirements" on page 14 for more information about experimental features.

USB Support

In order to use the USB redirection feature with View Portal, users must first install View Client on their local system. Refer to "View Client and View Portal" on page 70 for more information about this.

NOTE Windows 2000 does not support USB redirection.

Virtual Printing

View Portal does not support virtual printing.

View Composer

VMware Infrastructure 3.5 U3 is required in order to use the View Composer feature, and is supported on the following 32-bit platforms:

- Windows Server 2003 Service Pack 1
- Windows XP Professional Service Pack 2

NOTE You cannot use the View Composer feature of View Manager to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1.

SQL

A SQL database resident on—or available to—the VirtualCenter server is also required in order to store linked clone information.

NOTE If one is already present on the VirtualCenter server, View Composer can use the existing database—for example, the Microsoft SQL Server 2005 Express instance provided with VirtualCenter by default.

The requirements for each type of database supported by this feature are shown in Table 1-3.

Table 1-3. SQL Server Requirements

Database Type	Requirements
Microsoft SQL Server 2000 Standard	SP4 For Windows XP, apply MDAC 2.8 SP1 to the client Use SQL Server driver for the client
Microsoft SQL Server 2000 Enterprise	
Microsoft SQL Server 2005 Enterprise	SP1 or SP2 For Windows XP, apply MDAC 2.8 SP1 to the client Use SQL native client driver for the client
Microsoft SQL Server 2005 Express SP2	For Windows XP, apply MDAC 2.8 SP1 to the client Use SQL native client driver for the client
Oracle 9i release 2 Standard	Apply patch 9.2.0.8.0 to the server and client
Oracle 9i release 2 Enterprise	
Oracle 10g Standard Release 1 (10.1.0.3.0)	N/A
Oracle 10g Enterprise Release 1 (10.1.0.3.0)	
Oracle 10g Standard Release 2 (10.2.0.1.0)	First apply patch 10.2.0.3.0 to the client and server, then apply patch 5699495 to the client
Oracle 10g Enterprise Release 2 (10.2.0.1.0)	

Installation 2

This chapter describes how to install and backup one or more instances of View Connection Server, and also considers the different deployment scenarios you may encounter during this operation.

Before installing View Connection Server, refer to Chapter 1, "Introduction," on page 11 to view the system requirements and hardware and device support.

After installing and configuring View Connection Server, refer to "View Connection Server Backup" on page 38 for information on how to backup your View Manager configuration information.

This chapter discusses the following topics:

Overview of View Connection Server

View Connection Server communicates with VirtualCenter in order to provide advanced management of virtual desktops. This includes virtual desktop creation as part of pool management and power operations, such as automatic suspend and resume.

View Connection Server performs the following functions:

- User authentication
- User desktop entitlements with View LDAP
- Virtual desktop session management
- Coordination of the secure connection establishment, virtual desktop connection, and single sign-on
- Administration server used by View Administrator Web client
- Virtual desktop pool management

View Connection Server Instances

View Connection Server is installed on a Microsoft Windows Server 2003 system that is located on either a physical or virtual server dedicated to brokering View Manager connections. The host system must be joined to an Active Directory domain—but must not be a domain controller—and it is recommended that the host system uses a static IP address.

CAUTION Do not install View Connection Server on a platform that performs any other functions or roles—for example, do not use the same system to host VirtualCenter

The domain user account used to install View Connection Server must have administrator privileges on that server. The View Connection Server administrator also must posses administrative credentials for VirtualCenter.

The server can be installed as a either a standard, replica, or security server—the instance type is selected during the installation process.

NOTE In order to add users in an Active Directory domain other than the one in which you have installed a standard or replica View Connection Server, you must establish a two-way trust relationship between their domain and the one in which the View Connection Server is located.

View LDAP

View LDAP is an embedded Lightweight Directory Access Protocol directory that serves as the data repository for all View Manager configuration information, and uses Microsoft Active Directory Application Mode (ADAM) as its data store. ADAM is provided as part of the View Connection Server installation.

View LDAP contains the following components that are used within View Manager:

- Specific View Manager schema definitions
- Directory information tree (DIT) definitions
- Access control lists (ACLs)

View LDAP contains entries that represent the following View Manager objects:

- Virtual desktop entries that represent each accessible virtual desktop—this contains references to the Foreign Security Principal (FSP) entries of Windows users and Windows user groups in Active Directory who are authorized to use this desktop.
- Virtual desktop pool entries that represent multiple virtual desktops managed together
- Virtual machine entries that represent each virtual desktop
- View Manager component configuration entries used to store configuration settings

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

NOTE Security server instances do not contain the View LDAP component.

Preparing for Installation

View Manager uses ephemeral ports in order to establish TCP connections between the View Connection Server and the desktops it administers. An ephemeral (short-lived) port is one that is automatically created by the operating system when a program requests any available user port. The port is drawn from a predefined range (typically between 1024 and 65535) and released once it has served its purpose.

The default maximum number of ephemeral ports that can be created simultaneously on Windows 2003 Server is 5000. If you are planning to deploy View Manager into an environment where a large number (>1000) of concurrent client connections is likely, it is strongly recommended that you increase the number of available ephemeral ports.

To increase the maximum number of ephemeral ports on Windows 2003 Server

1 Start the Windows Registry Editor by entering `regedit` from a command prompt.

2 Locate the following subkey in the registry, and then click **Parameters**:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

3 On the **Edit** menu, click **New**, and then add the following registry entry:

```
Value Name: MaxUserPort
Value Type: DWORD
Value data: 65534
Valid Range: 5000–65534 (decimal)
Default: 0x1388 (5000 decimal)
```

4 Exit Registry Editor, and then restart the system.

Standard Server Installation

A standard server deployment creates a single standalone View Connection Server. This server could later become the first server instance within a replicated View Connection Server group.

When a standard server instance is created during View Connection Server installation, a new local View LDAP instance is also created. The schema definitions, DIT definition, ACLs, and so forth are loaded and the data is initialized.

NOTE Most configuration data in View LDAP is maintained from View Administrator, although View Connection Server manages some entries automatically.

To install a standard server

1 Run the following executable on the system that will host the View Connection Server, where `xxx` is the build number of the file:

```
VMware–viewconnectionserver–xxx.exe
```

The VMware Installation wizard is displayed. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Accept or change the destination folder and click **Next**.

4 Choose the **Standard** deployment option.

5 Click **Next** > **Install** > **Finish**.

Replica Server Installation

Replica servers are additional View Connection Server instances that are installed in order to provide high-availability and load balancing. When a replica server is installed, a local ADAM instance is also created and the View LDAP data on the replica server is initialized from an existing View Connection Server.

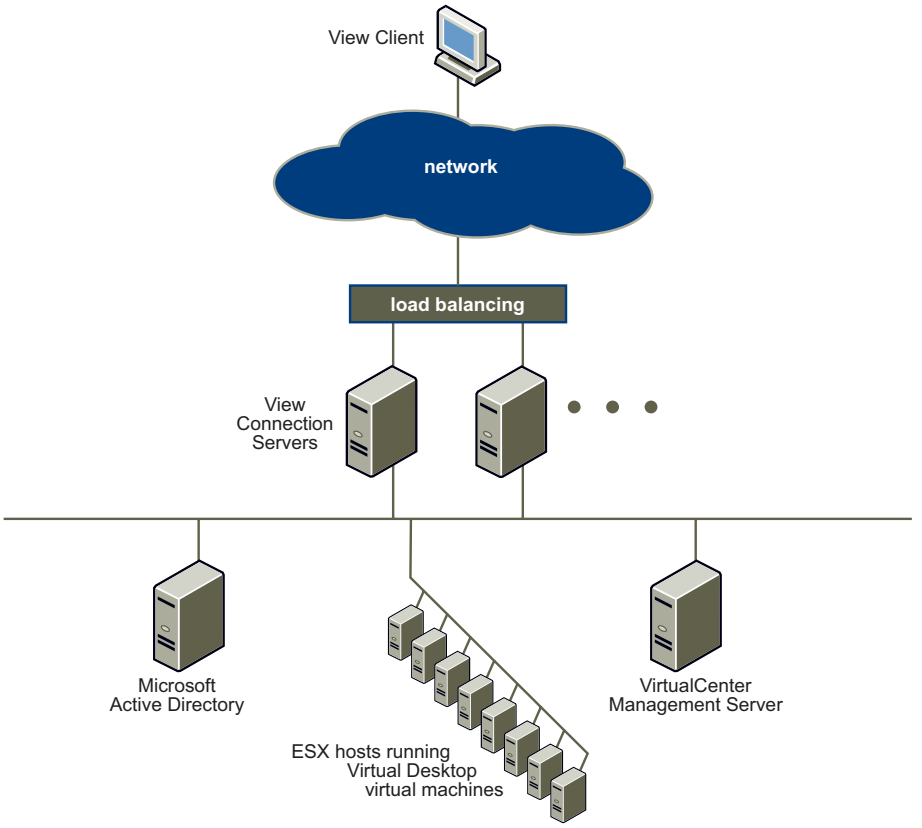
During replica installation, an agreement is established that ensures every View Connection Server in the replicated group shares the same configuration data. Whenever a change is made to View LDAP data on one system, the updated information is automatically proliferated across every other replica server within the group.

NOTE This replication functionality is provided by ADAM, which uses the same replication technology as Active Directory.

In order to install a replica, there must be at least one View Connection Server instance already present on your network. Replica servers can use either a standard server or another replica server to initialize their data. Once initialized, the behavior and functionality of the replica server is identical to that of a standard server and offers identical functionality.

In the event of server failure, the other servers in the replicated group will continue to operate. If the failed server resumes activity, its configuration data is automatically updated to reflect any changes that may have taken place during the outage. Figure 2-1 shows two instances of View Connection Server operating as a replicated group.

Figure 2-1. Multiple Replica Servers



To further enhance the high-availability and scalability requirements of your VDI environment, it is recommended that you deploy a load balancing solution—this ensures that connections are distributed evenly across each available View Connection Server, and that failed or inaccessible servers are automatically excluded from the replicated group.

NOTE View Connection Server does not provide load-balancing functionality but works with standard third-party load-balancing solutions.

To install a replica server

1 Run the following executable on the system that will host the View Connection Server, where xxx is the build number of the file:

```
VMware-viewconnectionserver-xxx.exe
```

The VMware Installation wizard is displayed. Click **Next**.

2 Accept the VMware license terms, and click **Next.**

3 Accept or change the destination folder, and click **Next**.

4 Choose the **Replica** deployment option.

5 Enter the host name or IP address of the existing View Connection Server that you want to replicate. If the target system is not part of the same domain as the main server, you will require local administrative rights on the target server to do this.

6 Click **Next > Install** > **Finish**.

Security Server Installation

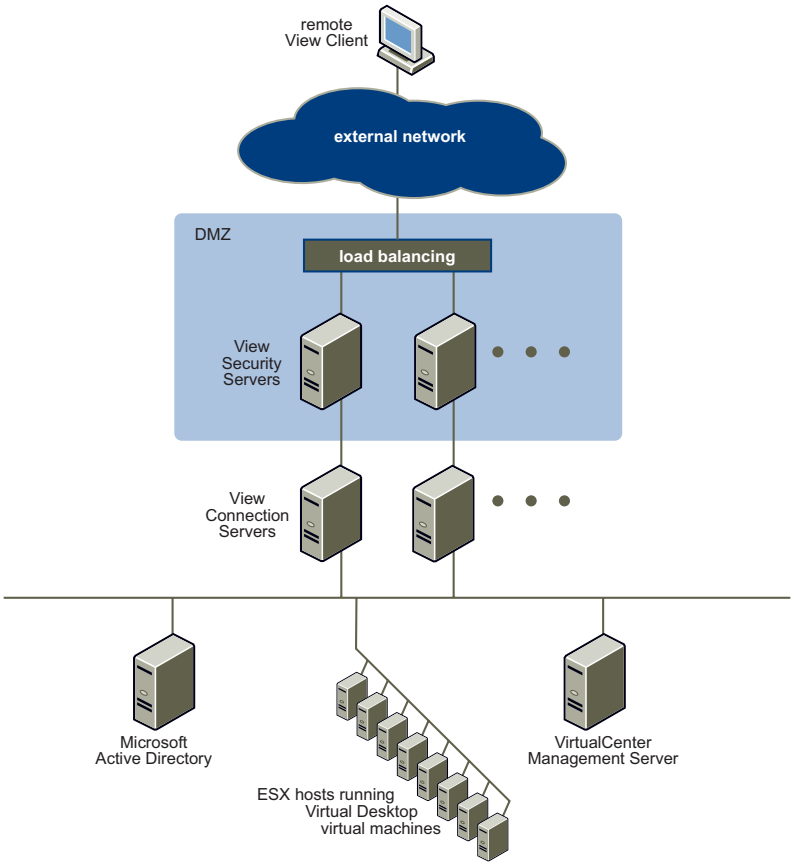
A demilitarized zone (DMZ) is a semi-protected sub-network that exists between a secure internal network and an insecure external network. Services that exist within this space are exposed to both networks and provide an entry point for external to users to access applications that reside within the secure environment.

View Connection Server security servers are installed in the DMZ in order to add an additional layer of network protection; they ensure that only authenticated users can connect to the internal network from external locations by providing a single point of access. Because the inbound communications from DMZ services can be strictly controlled through firewall policy, the risk of the internal network being compromised is greatly reduced.

NOTE In LAN-based deployments, no security servers are required as users can connect directly with any View Connection Server from within their internal network.

Figure 2-2 shows a high-availability environment comprising two load-balanced security servers in the DMZ communicating with two instances of View Connection Server—a standard server and a replica server—inside the internal network.

Figure 2-2. Multiple Security Servers



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

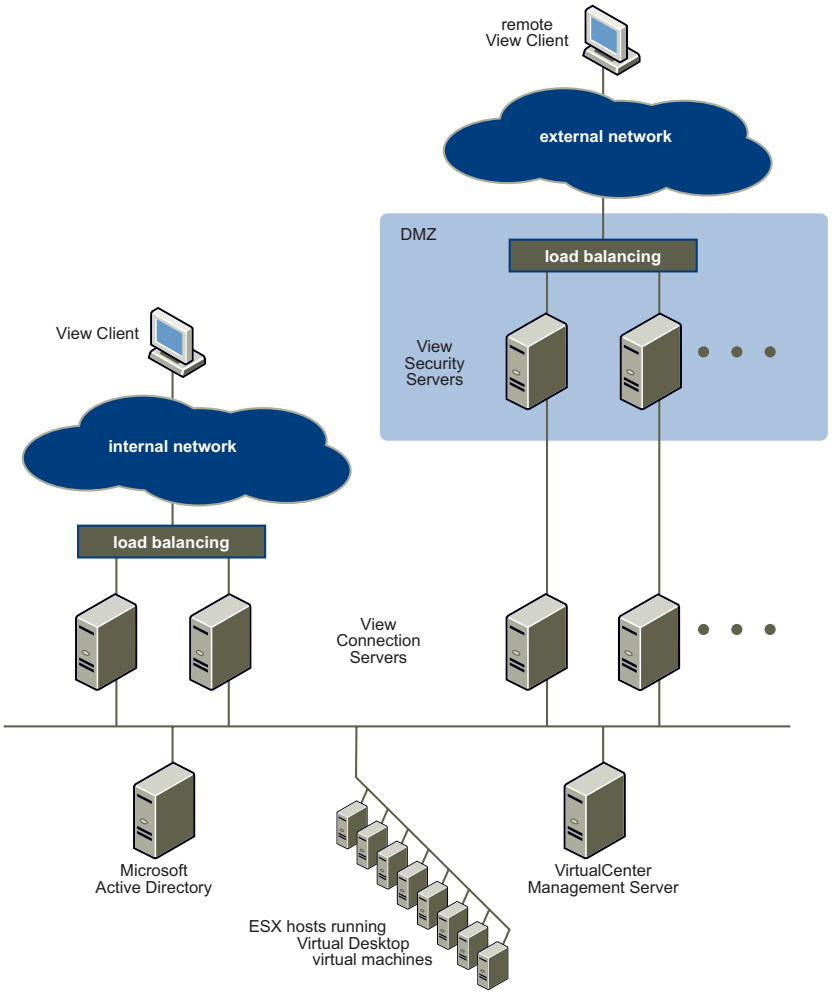
Multiple security servers can be connected to each standard or replica View Connection Server. A DMZ deployment can be combined with a standard deployment to offer access for internal users and external users.

Figure 2-3 shows an environment where four instances of View Connection Server act as one group with the servers in the internal network dedicated to the users of that network, and the servers in the external network dedicated to users of that network. The servers on the right can be enabled for RSA SecurID authentication, so that all external network users are required to authenticate using RSA SecurID tokens.

Depending on your particular server configuration, load balancing might be required. You will require either a hardware or software load-balancing solution if you have more than one security server.

NOTE View Connection Server does not provide load-balancing functionality but works with standard third-party load-balancing solutions.

Figure 2-3. DMZ Deployment with Multiple View Connection Server Instances

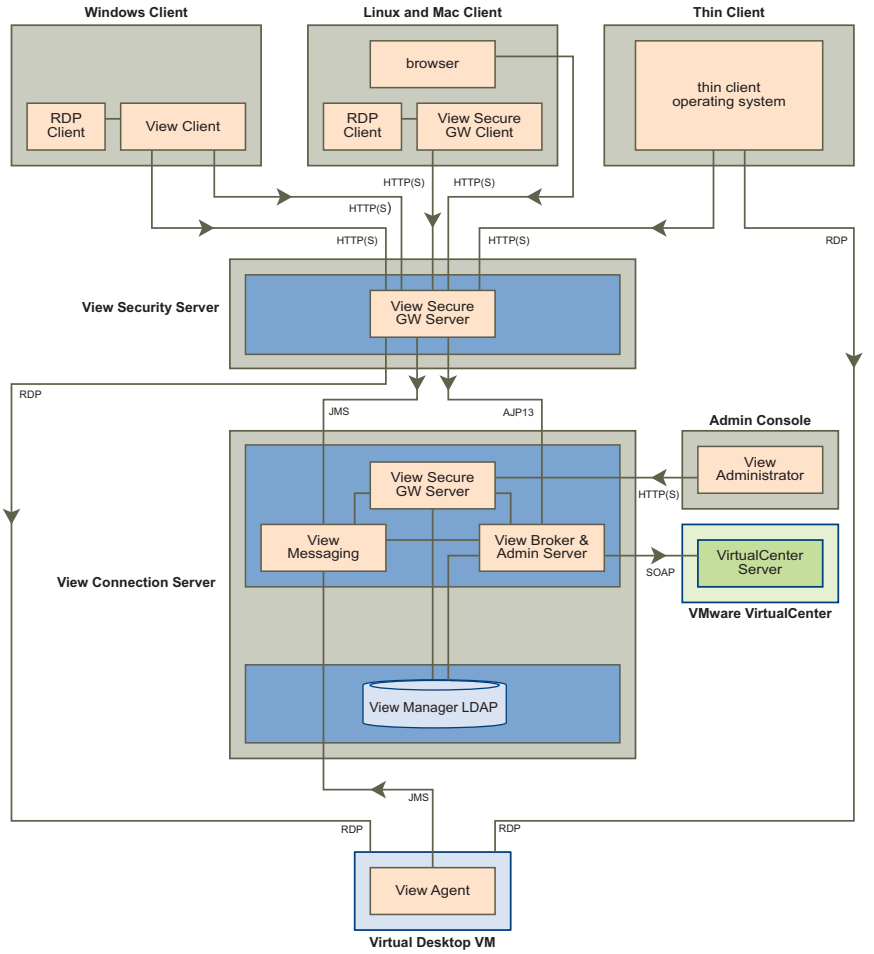


Security servers implement a subset of View Connection Server functionality, and do not need to reside in an Active Directory domain. In addition, security servers do not contain a View LDAP configuration repository and do not access any other authentication repositories, such as Active Directory or RSA Authentication Manager.

Firewall Configuration

Figure 2-4 shows a security server deployment and illustrates the relationship between the security server and all other View Manager components, including the protocols each components uses for communication.

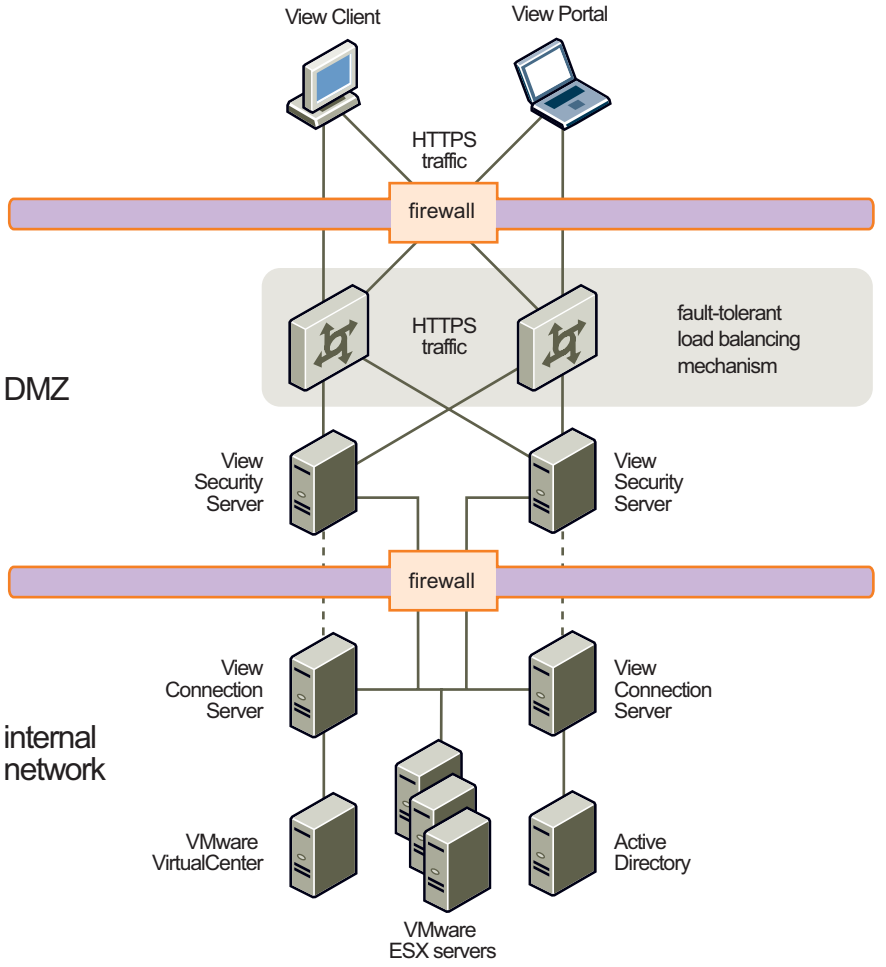
Figure 2-4. View Manager Component Diagram



The recommended security configuration for a DMZ-based security server deployment is the dual firewall. In this configuration, an external network facing "front-end" firewall protects both the DMZ and the internal network, and a "back-end" firewall between the DMZ and the internal network provides a second tier of security.

The front-end firewall is configured to allow network traffic to reach the DMZ, whereas the back-end firewall is configured to only accept traffic that originates from the services within the DMZ. This configuration is illustrated in Figure 2-5.

Figure 2-5. Example DMZ-Based Security Server Deployment



To allow external client devices to connect to a security server within the DMZ, the front-end firewall must allow inbound traffic on TCP ports 80 and 443. To allow the security server to communicate with each standard or replica server that resides within the internal network, the back-end firewall must allow inbound traffic on TCP port 8009 for AJP13-forwarded Web traffic, TCP port 4001 for Java Message Service (JMS) traffic, and TCP port 3389 for RDP traffic.

Behind the back-end firewall, internal firewalls must be similarly configured in order to allow the View Manager desktops and View Connection Server instances to communicate with each other. Port 3389 (RDP) is used for traffic originating from a standard or replica server that is directed at a guest system. Port 4001 is used for JMS traffic originating from either the View Agent component installed on each View Manager desktop or from a security server in the DMZ, and is directed at standard or replica View Connection Server instances.

The back-end and front-end firewall rules are summarized in Table 2-1.

Table 2-1. Firewall Rules

Firewall Type	TCP Port	Protocol	Source	Destination
Front-end	80	HTTP	Any	Security server
	443	HTTPS		
Back-end	3389	RDP	Security server	Any desktop virtual machine
	4001	JMS		Standard or replica server
	8009	AJP13		
	4001	JMS	Any desktop VM	

External URL

By default, the fully-qualified domain name (FQDN) of the host is required by View Client in order to establish a connection with View Connection Server. This information will not be available to clients who attempt to contact the server from outside your network environment.

Refer to "Client Connections from the Internet" on page 71 for information on how to add an external URL to a security server to make it accessible from the Internet.

Offline Desktop

If you intend to use the Offline Desktop feature, you must also ensure that port 902 is similarly accessible on your ESX / ESXi server; this port is used to establish the TCP connection through which the offline desktop data is downloaded and uploaded. Refer to Chapter 7, "Offline Desktop," on page 123 for more information about this component.

RDP

When View Agent is installed on a desktop virtual machine or an unmanaged desktop source, the application installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system—in most cases this will be port `3389`.

If an administrator subsequently changes the port number used for RDP, the associated firewall rules for both the desktop virtual machine or unmanaged desktop source and the back-end firewall must be similarly modified by the administrator.

For more information about desktop virtual machines and unmanaged desktop sources, refer "Desktop Sources" on page 50.

To install a security server

1 Run the following executable on the system that will host the security server, where `xxx` is the build number of the file:

```
VMware-viewconnectionserver-xxx.exe
```

The Installation wizard is displayed. Click **Next**.

2 Accept the license terms and click **Next.**

3 Accept or change the destination folder and click **Next**.

4 Choose **Security Server**.

5 Each security server is paired with a View Connection Server and forwards all traffic to that server. Enter the FQDN of the standard or replica server with which the security server is to communicate.

6 Click **Next** > **Install** > **Finish**.

VirtualCenter Permissions for View Manager Users

To use VirtualCenter with View Manager, administrators must have permission to carry out certain operations in VirtualCenter. These permissions are granted by creating and assigning VirtualCenter roles to a View Manager user from within VirtualCenter.

NOTE Administrative users in VirtualCenter have all the requisite permissions enabled by default.

Assign the View Manager administrator the role of administrator for a datacenter or cluster where pools will be created so that they can make the required changes.

To create the a View Manager role for VirtualCenter user

1 In VirtualCenter, click the **Administration** button.

2 If it is not already selected, click the **Roles** tab and click **Add Role**.

3 Enter a name for the role (`View Administrator`, for example).

4 In the list of **Privileges**, expand **Folder** and select **Create Folder** and **Delete Folder**.

5 Expand **Virtual Machine** and perform the following steps:

   a Expand **Inventory** and select **Create** and select **Remove**.

   b Expand **Interaction** and click **Power On**, **Power Off**, **Suspend**, and **Reset**.

   c Expand **Configuration** and select **Add new disk**, **Add or Remove Device**, **Modify Device Settings**, and **Advanced**.

   d Expand **Provisioning** and select **Customize**, **Deploy Template**, and **Read Customization Specifications**.

6 Expand **Resource** and select **Assign Virtual Machine to Resource Pool**.

7 Click **OK**. The new role appears in the list of roles.

Initial View Manager Configuration

Once you have installed one or more View Connection Server instances you must perform an initial configuration so that they are ready to carry out administrative tasks. Configuration is carried out from within View Administrator, the Web-based administrative component of View Manager.

NOTE This component is only available on standard and replica server instances.

To perform an initial configuration

1 Open a browser supported by View Administrator, and enter the following URL where `<server>` is the hostname or IP address of a standard or replica View Connection Server instance:

```
https://<server>/admin
```

NOTE View Administrator is accessed through a secure (SSL) connection. The first time you connect, your browser may present you with an intermediary page that warns you that the security certificate associated with the address is not issued by a trusted certificate authority. This is expected behavior because the default root certificate supplied with View Connection Server is self-signed.

2 Log in using the appropriate credentials. Initially, all domain users who are members of the local administrators group on the View Connection Server are allowed to login to the View Administrator—you can use the interface to change the list of View Manager administrators later.

The first time you log in, the Configuration view is shown. After you have licensed the product, the Desktop view is displayed after log in.

NOTE If the Configuration view is not shown, click the **Configuration** () button.

3 Within the Configuration view, do the following:

- Under Product Licensing, click **Edit License** and enter the View Manager license key in the field provided. Click **OK**.
- Under VirtualCenter **Servers**, click **Add** and complete the details for one or more VirtualCenter servers to use with View Manager.
  - Enter the FQDN or IP address of the VMware VirtualCenter server you want View Manager to communicate with in the **Server address** text box.

CAUTION If you enter a server using a DNS name or URL, no DNS lookup is performed to verify whether or not the server has previously been entered using its IP address. A conflict will arise if a VirtualCenter server is added with both its DNS name and its IP address.

- Enter the username of a VirtualCenter user or administrator in the **User name** text box. If you want to select a VirtualCenter user who is not an administrator but has the requisite level of authority, ensure that their role meets the criteria described in "VirtualCenter Permissions for View Manager Users" on page 36.
- Enter the password that corresponds to the username entered above in the **Password** text box.
- (Optional) Enter a description for this VirtualCenter server in the **Description** text box.
- If you will be connecting to the VirtualCenter through a secure channel (SSL) then make sure the Connect using SSL checkbox is checked. This is the default setting.
- Enter the TCP port number in the Port text box. The default is 443.

(Optional) If you click the **Advanced** button you may also configure the following settings:

- **Maximum number of concurrent provisioning operations**—This is the maximum number of virtual machines that will be simultaneously created by View Manager in VirtualCenter at any given time.
- **Maximum number of concurrent power operations**—This is the maximum number of concurrent power operations (startup, shutdown, suspend and so forth) that will take place on View Manager managed virtual machines in VirtualCenter at any given time.

Click **OK** to store the VirtualCenter settings.

- Under Administrators, click **Add** and use the form provide to grant administrative rights to the Active Directory users who you want to be able to access to View Administrator. Once you have added all the required administrators, click **OK**.

View Connection Server Backup

In order to preserve or migrate your configuration information, View Manager allows you to export and import the contents of the View LDAP repository from any standard or replica View Connection Server.

View LDAP data is exported and imported in LDAP data interchange format (LDIF), a draft Internet standard for a file format that can be used to perform batch operations against directories that conform to the LDAP standard.

Once you have completed the initial configuration of your server or replicated group, it is strongly recommended that you regularly take backups of your View Manager data using the utilities described in this section. Do not rely on replica servers to act as your backup mechanism as any data lost from one instance will be lost from all members of the replicated group when the data is harmonized.

NOTE If you have multiple instances of View Connection Server operating in a replicated group you only need to export the data from one server as all replica servers contain the same configuration data.

To export View Manager configuration data

LDIF data is exported from View Manager using the `vdmexport.exe` tool that accompanies each standard and replica View Connection Sever; the path to the executable file is:

```
C:\Program Files\VMware\View Manager\Server\bin\vdmexport.exe
```

From the command prompt on a standard or replica View Connection Server, execute the following command to create a file called `VDMConfig.LDF` that contains the exported View LDAP configuration information:

```
vdmexport > vdmconfig.ldf
```

To import View Manager configuration data

LDIF data is imported into View Manager using LDIFDE, a utility program included in Windows Server 2003 that supports batch operations based on the LDIF file format standard.

From the command prompt on a standard or replica View Connection Server, execute the following command to import a file called `VDMConfig.LDF` that contains previously exported View LDAP configuration data:

```
LDIFDE –i –f vdmconfig.ldf –s 127.0.0.1
```

View Administrator 3

View Administrator is where you perform all of the configuration, deployment, analytical, and administrative tasks related to View Manager and desktop management.

The purpose of this chapter is to give you a brief overview of the different types of view available within View Administrator and describe the features they contain. This chapter also discusses the various desktop sources and the different desktop delivery models that can be delivered.

This chapter discusses these topics:

Overview of View Administrator

The **Desktops and Pools** (), **Users and Groups** (), **Configuration** (), and **Events** () buttons are displayed at the top of the administrative interface, and these buttons allow you to navigate to the different feature areas in order to perform various tasks. This section describes the views associated with each button and the features they contain.

NOTE When you click one of these buttons in the administrative interface and select a tab on the view that is displayed, the tab background becomes white. Tabs that are not selected have a purple background.

Desktops and Pools View

The Desktops view is displayed when you log in to the administrative interface or when you click the **Desktops and Pools** button and is where you create, deploy, administer, and monitor your virtual desktops.

From here you can examine information about desktops or desktop pools and their associated users; individual desktop sources; any sessions that are active; any tasks that are scheduled; and desktop usage policies at the global, pool or user level.

The Desktops view is divided into two parts: a left-hand pane that contains an **Inventory** and a **Search** tab and a right hand pane that provides either global or pool-level information about the desktops currently available.

When the **Inventory** tab is selected, the left-hand pane provides a list of all the desktops or pools in an alphabetic list under the top-level **Desktops and Pools** entry ().

The **Desktops and Pools** entry is global in scope. When selected it changes the context of the right-hand pane to cover all the desktops available—for example, when this entry is selected the **Active Sessions** tab in the right-hand pane lists all the active sessions for all View Manager desktops.

If any desktops or desktop pools are present, they are listed beneath the **Global desktop and pool view** entry. Selecting an individual desktop () or desktop pool entry () changes the context of the right-hand pane to provide specifically about that desktop or pool. For example, when an entry in this list is selected the **Active Sessions** sub-tab in the right-hand pane lists all the active sessions for the desktops in that pool.

The tabs in the right-hand pane are described in Table 3-1. If the tab is present for both specific desktop sources and also desktop pools, this is indicated in the Context column.

Table 3-1. Desktops Pane – Tab Summary

Tab	Context	Description
Summary	Desktop or Pool	This tab provides an overview of all information associated with a desktop or desktop pool, including: General information about the pool, such as the name, type, persistence, and current activity. VirtualCenter environmental criteria, such as server name, capacity, and domain administrator. Desktop settings, such as minimum, maximum, and available number of desktops; power policy and so forth. From this tab you can click: ■ **Edit** to modify the desktop or desktop pool deployment settings ■ **Entitle** to add or remove user entitlements to or from the desktop or desktop pool ■ **Enable/Disable** to enable or disable desktop or desktop pool availability and provisioning
Desktops	Global	This tab lists all the desktops or desktops pools currently available within View Manager. From this tab you can click **Add** to deploy a new desktop or pool. In addition, you can select existing desktop or desktop pool entries from the table provided and click: ■ **Edit** to modify the desktop or desktop pool deployment settings ■ **Entitle** to add or remove user entitlements to or from the desktop or desktop pool ■ **Delete** to remove the desktop or desktop pool ■ **Enable/Disable** to enable or disable desktop or desktop pool availability and provisioning
Users and Groups	Desktop or Pool	This tab lists all users and groups entitled to use this desktop or pool. From under the **Entitlements** sub-tab, you can select and **Remove Entitlement** from any user listed in the table provided. If the selected pool uses linked clone technology for its deployment, an additional sub-tab—**Known Users**—is also displayed.

Table 3-1. Desktops Pane – Tab Summary (Continued)

Tab	Context	Description
Desktop Sources	Desktop or Pool	This tab lists all the individual virtual systems available in the selected pool. From this tab you can select existing desktop or desktop pool entries from the table provided and click: ■ **Remove** to remove individual or multiple virtual machines (either from View Manager, or from VirtualCenter and View Manager) ■ **Reset** to reset selected desktop—this action disconnects any currently connected users and restarts the system ■ **Rebalance** to redistribute the virtual machines on the datastore to ensure that space is being used optimally between logical drives ■ **Cancel Task** to terminate any tasks that have been scheduled or that are currently running against the selected virtual machines
Active Sessions	Both	This tab lists all the desktop sessions currently active, either globally or within the selected pool. The user name, start time, duration, and virtual machine address for each connected user are shown. You can select user entries from the table provided and click: ■ **Disconnect session** to disconnect the user from the desktop—this action does not log the user off, and their session will preserved once they log back in providing the **Automatic logoff after disconnect** setting specified during desktop deployment has been not been exceeded ■ **Logoff session** to log the user off and disconnects them from the current session ■ **Reset virtual machine**
Offline Sessions	Both (when Offline Desktop desktops are detected)	This tab lists all the Offline Desktop desktops currently checked out, either globally or within the selected pool. Refer to Chapter 7, "Offline Desktop," on page 123 for more information about this feature.
Global Policies	Global	This tab lists the policies that are applied to all desktops and pools at the global level.
Policies	Desktop or Pool	This tab lists the policies that are applied to the selected desktop or pool. If the Any user-level policies that have been applied are also listed in this view.

Configuration View

The Configuration view is displayed when you click the **Configuration** () button. This view contains multiple sections that allow you to analyze desktop usage, configure licensing, connections, authentication criteria and so forth. Each section is described in Table 3-2:

Table 3-2. Configuration View Overview

Section	Description
Product Licensing	This section indicates the license status of View Manager and also if additional components such as the Offline Desktop feature are provided within the license coverage. Click **Edit License** to add or modify the license serial number for View Connection Server.
Usage	This section indicates the usage information for currently active desktops, including offline desktops if the View Manager license coverage includes Offline Desktop. You can update the information displayed in the usage table by clicking **Refresh**, and reset the counter that tallies the highest number of concurrent connections by clicking **Reset Highest**.
VirtualCenter Servers	This section lists the VirtualCenter servers available for the connection server to use. You can click **Add**, **Edit**, or **Remove** to modify the connection criteria.
Registered Desktop Sources	This section provides the number of Terminal Services, standalone virtual machines, and physical desktop sources currently registered with View Connection Server.
View Servers	This section allows you to enable or disable the current View Connection Server—indicated by a check mark ()—and any replica instances of View Connection Server known to the this server. Select a server entry from the table provided and click: ■ **Enable** to allow users to connect to their clients using this server. ■ **Disable** to refuse future client connections to this server (existing client connections are not affected by this action). ■ **Edit** to modify the View Connection Server external URL or to enable or disable RSA SecurID. To specify if a direct (non-tunnelled) connection is used by client connections brokered by this View Connection Server server, select the **Direct connection to desktop** box.

Table 3-2. Configuration View Overview (Continued)

Section	Description
Global Settings	This section provides information about the global product configuration parameters that apply to all areas of the product. To change a setting, click **Edit** and then modify any of the following entries: ■ **Session timeout**—Determine how long (in minutes) users are allowed to keep sessions open after they log in to the View Connection Server. This field must contain a value, and the default is `600`. ■ **Require SSL for client connections**—Determines if SSL is used to create a secure communication channel between View Connection Server and the client. ■ **Reauthenticate after network interruption**—Determines if tunnel client user credentials must be reauthenticated after a network interruption. This setting had no effect when direct connection is being used. ■ **Message security mode**—Determines if the JMS messages passed between View Manager components are encrypted. If a security server exists in your View Manager environment and you enable this setting, you must have an appropriately configured locked.properties file resident on the security server. Refer to "Generating locked.properties Automatically" on page 74 for more information about this. ■ **Direct connection for Offline Desktop operations**—Offline Desktop (if available) supports tunneled or non-tunneled communications for LAN-based data transfers. When tunneling is enabled, all traffic is routed through the View Connection Server. When tunneling is not enabled, data transfers take place directly between the online desktop host system and the offline client. ■ **Require SSL for Offline Desktop operations**—In addition to specifying the route for communications, you can encrypt the communications and data transfers that take place between the Offline Desktop client and the View Connection Server by selecting this check box. ■ **Disable SSO for Offline Desktop operations**—Determines if single sign-on is enabled for Offline Desktop. When disabled, users must manually log in to their desktop to start their Windows sessions.

Table 3-2. Configuration View Overview (Continued)

Section	Description
Global Settings (Continued)	■ **Display a pre-login message**—if selected, Client and Web Access users see a disclaimer or login message with information or instructions entered by the administrator in the field provided. ■ **Display a warning before forced logoff**—Determines if desktop users are logged off as a result of a scheduled or immediate update event (such as a desktop refresh). In the fields provided, enter the notification message to be shown, and the amount of time after it is displayed that the user is logged off.
Administrators	This section allows you to add administrators to, or remove them from, the View Connection Server. Click **Add** to search for Active Directory users or groups in order add (or remove) them as administrators View Connection Server administrators.
Security Servers	This section allows you to add one or more security server instances to your View Manager environment. Security servers offer greater network security to environments that allow clients to access them from the Internet. Security servers operate within a DMZ and run a subset of the full View Connection Server functionality. By using a security server as an intermediary connection layer, View Manager ensures that only authenticated users can attempt a connection to the internal network from the Internet."Security Server Installation" on page 29 for more information about this.

Events View

Use the Events view to examine events generated by the actions taking place within the View Connection Server. You can enter text in the Contains field and search by type of message, the time of the message or the message text itself. You can also determine the number of days of messages to display.

You can use the information on the **Events** page for diagnosing problems or viewing activity on the server.

To search events

1 Click the arrow after **Contains** and select the columns to search (**Messages, Time, Type).**

2 From the list, choose the number of days of messages to show in the Events table and click **Done**.

3 Enter search text in the text box and click **Go**.

Search results appear in the **Events** table. Click **(more) at the end of each message to display more details about the event.**

4 Virtual Desktop Deployment

Virtual desktop deployment is the task of preparing individual or multiple virtual machines for View Manager client connections. Once deployed, prepared systems can be accessed directly or act as a template from which View Manager can create an extensible pool of cloned desktops.

This chapter covers the end-to-end requirements and procedures associated with desktop deployment, and concentrates specifically on the creation of desktops and desktop pools from virtual machines managed by VirtualCenter.

This chapter discusses the following topics:

Overview of Virtual Desktop Deployment

The procedure for deploying virtual desktops varies depending on whether you are creating an automated pool from a virtual machine template, an individual desktop instance, or a pool of manually-selected virtual desktops. However, in all of these cases a base—or guest—system must first be selected and configured for use with View Manager.

Desktop Sources

Different desktop sources have different capabilities in terms of application support and user experience. They also differ in the way they are configured and managed and the provisioning choices they offer. The desktop sources supported by View Manager:

View Manager Provisioned and VirtualCenter Managed— the desktop source is a virtual machine that is provisioned by View Manager and is managed by a VirtualCenter server. To add this desktop source the following settings must be specified by the administrator:

- VirtualCenter server which provisions and manages the virtual machines. You can only use VirtualCenter servers that are known to the View Manager server.
- Template used to provision the virtual machines.
- Location in the VirtualCenter inventory hierarchy where you want to add the virtual machines.
- Data store for the virtual machines.
- Customization specification for the virtual machines.

View Manager Non-Provisioned and VirtualCenter Managed— the desktop source is a virtual machine that is managed by a VirtualCenter server but not provisioned by View Manager. Virtual machines already exist on the VirtualCenter server. To add this desktop source the following settings must be specified by the administrator:

- VirtualCenter server which manages the virtual machines. You can only use VirtualCenter servers that are known to the View Manager server.
- Individual desktop: Select the virtual machine and add it as a desktop source.
- Desktop pool: Select multiple virtual machines and add them as desktop sources.
- If the virtual machine is already assigned to another desktop, an error appears. You must remove the desktop from previously assigned desktop pool or individual desktop.

Unmanaged Desktop Sources— the desktop source is a machine that is not managed by a VirtualCenter server. This includes virtual machines running on VMware Server and virtual machines running on other virtualization platforms that support View Agent. Blade PCs, physical PCs and Terminal Servers on which you can install View Agent are unmanaged desktop sources.

Desktop Delivery Models

Unified Access supports different desktop delivery models which characterize the way a desktop is created, entitled, delivered, and used. The desktop delivery models supported by View Manager are:

Individual Desktop – is a desktop that allows a single, pre-existing back-end source with the following characteristics:

- Entitled to many users or user groups; however, only one active user at a time.
- Not provisioned automatically.

Manual Pool – is a pool of desktop sources with the following characteristics:

- Multiple users to multiple desktop mapping; however, only one active user on a desktop at a time.
- Not provisioned automatically.
- Supports both persistent and non-persistent access modes.
- Administrator entitles entire pool to users or user groups.

Automated Pool – is a pool that contains one or more dynamically generated desktops that are automatically created and customized by View Manager from a VirtualCenter virtual machine template and have the following characteristics:

- Multiple users to multiple desktop mapping; however, only one active user on a desktop at a time. This is applicable only on VI machines.
- Provisioned automatically.
- Administrator specifies a template and a customization specification which is used to provision desktop sources.
- Supports both persistent and non-persistent access modes.
- Administrator entitles entire pool to users or user groups.

Terminal Server Pool – is a pool of terminal server (TS) desktop sources served by one or more terminal servers. A terminal server desktop source can deliver multiple desktops. A TS pool has the following characteristics:

- Pool of TS desktops served by a farm comprising of one or more terminal servers.
- Least session count based load balancing: View Manager load balances connection requests across terminal servers in a pool by choosing the pool that has the least number of active sessions on it.
- Administrator entitles entire pool to users or user groups.
- Administrators should deploy a roaming profile solution to enable user settings and personalization to be propagated to the currently accessed desktop.

Preparing the Guest System

The guest system is the virtual machine that forms the basis for every type of virtual desktop deployment. The procedure for creating a new virtual machine in exceeds the scope of this document, but the selected virtual machine must adhere to the requirements described in "System Requirements" on page 14.

NOTE Refer to the VirtualCenter documentation for more information about creating new virtual machine instances.

Once you have selected a guest system you must ensure that the following prerequisites are in place:

- The latest version of VMware Tools are installed (provided with VI 3.5).
- The networking settings (proxies, and so forth) are properly configured and that the guest system is attached to a domain.
- View Manager Agent is installed.

  NOTE For automated updating of View Agent in large environments, VMware recommends using standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software.

- You have administrative rights to the guest system.

Installing the View Agent on the Guest System

The View Agent component assists with session management, single sign-on, and device redirection. You must install View Agent on the guest system in order to allow the View Connection Server to communicate with the desktop.

To install View Manager Agent

1 Run the View Agent executable on the system that will host the agent, where xxx is the build number of the file:

```
VMware-viewagent-xxx.exe
```

The installation wizard opens. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Choose your custom setup options. You must install the **View Manager Composer Agent** if you want to deploy linked clone desktops. Refer to Chapter 6, "View Composer," on page 93 for further information about this feature. You may also select or deselect the following features:

- Install the **View Secure Authentication** component if you want to install the Graphical Identification and Authentication (GINA) dynamic-link library. Installing this component enables single sign on (SSO) so that when a user logs into View Client they are not additionally prompted to re-enter their authentication information in order to log in to their desktop.
- Install the **USB Redirection** component if virtual desktop users need to access locally connected USB devices with their virtual desktops.

  NOTE Windows 2000 does not support USB redirection.

- Install the **Virtual Printing** component if you want to enable users to print to any printer available to their client system without first installing additional drivers on their desktop. Refer to "Virtual Printing" on page 90 for more information about this feature.

4 Accept or change the destination folder and click **Next**.

5 Click **Install** to begin the installation process. On the process is complete click **Finish**.

Using the View Agent on Virtual Machines with Multiple NICs

For guest systems with more than one virtual NIC, you must configure the subnet that the View Agent will use. This determines which network address the View Agent provides to the View Connection Server for client RDP connections.

To configure this subnet, create the following registry string in the virtual machine on which the View Agent is installed, where `n.n.n.n` is the TCP/IP subnet and `m` is the number of bits in the subnet mask:

```
HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Node
Manager\subnet = n.n.n.n/m (REG_SZ)
```

Individual Desktops

Individual desktops are single virtual machines that contain View Agent and can be accessed remotely by View Manager clients. Users entitled to use this type of desktop will always access the same system each time they connect.

Individual desktops are appropriate for users who require a single unique dedicated desktop, or for hosting a costly application with single host license that needs to be accessed by multiple users at different times.

Deploying an Individual Desktop

1. From within the View Administrator interface, click the **Desktops and Pools** button and then click the **Inventory** tab. In the **Desktops** pane, ensure that the **Desktops and Pools** tab is selected and click **Add**.
2. You are presented with the Add Desktop wizard. From here you can configure and deploy a new linked clone desktop pool. Select **Individual Desktop** and click **Next**.
3. Specify the source type of the guest system by selecting **VirtualCenter virtual machine**. Click **Next**.
4. From the list provided, select the VirtualCenter server that will be used by this desktop. Click **Next**.
5. Enter the **Unique ID** and, optionally, the **Display name** and **Description**.

   The unique ID is used by View Manager to identify the desktop pool and is the name that clients see when logging in. The unique ID and display name can be arbitrary but if you do not specify a display name the unique ID is used for both.

   NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters in length and is only visible from within View Administrator.

   Once you have provided the desktop identification details, click **Next**.

6 Configure the desktop properties and click **Next**.

CAUTION If you are using Windows Vista as your Parent VM, you *must* set the power policy to **Ensure VM is always powered on**.

Property	Parameter Description
State	**Enabled**—after being created, the desktop is automatically enabled and ready for immediate use. **Disabled**—after being created, the desktop is disabled and unavailable for use. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
When VM is not in use	**Do nothing (VM remains on)**—Virtual machines that are powered off will be started when required and will remain on, even when not in use, until they are shut down. **Ensure VM is always powered on**—All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart. **Suspend**—All virtual machines in the pool enter a suspended state when not in use. **Power off**—All virtual machines in the pool shut down when not in use.
Automatic logoff after disconnect	**Immediately**—users are logged off as soon as they disconnect. **Never**—users are never logged off. **After**—the time after which users are logged off when they disconnect. Enter the duration in minutes in the field provided.
Allow users to reset their desktop	Select this check box if you want to allow desktop users to be able reset their own desktops without administrative assistance.

7 From the list provided, select the virtual machine you want to use as the individual desktop. Click **Next**.

8 You are presented with a summary of the configuration settings for this deployment.

- If you are unsatisfied with any aspect of the configuration you can use the **Back** button to revisit any previous page.
- If you are satisfied with the configuration click **Finish** to deploy the individual desktop.

Once the deployment has been initiated you can monitor the progress of the individual desktop by selecting either the **Desktops and Pools** or **Desktop Sources** tabs in the Global desktop and pool view pane.

Automated Desktop Pools

Automated desktop pools contain one or more dynamically generated desktops that are automatically created and customized by View Manager from a VirtualCenter virtual machine template. Desktop pools of this type can be either:

- Persistent—Users are allocated a dedicated desktop that retains all of their documents, applications and settings between sessions. The desktop is statically assigned the first time the user connects, and is then used for all subsequent sessions.
- Non-persistent—Users are connected to a different desktop from the pool each time they connect, and there is no persistence of environmental or user data between sessions.

Automated desktop pools can use the link clone feature to rapidly deploy desktops from a single "Parent VM". However, this section describes a deployment that does not use this feature. For more information about link clone, including the deployment procedure, refer to Chapter 6, "View Composer," on page 93.

Virtual Machine Templates

In order to create an automated desktop pool you must first create a virtual machine template in VirtualCenter. The template is created by right-clicking a previously configured guest system VM in VirtualCenter and selecting either of the following entries from the context menu:

- **Clone to Template**—select this option if you want to use the selected guest system as the basis for a new template without altering the VM itself. If you select this option you will be presented with a setup wizard that asks you to provide the name of the template, and environmental information concerning where you want the template to reside and the disk format it should use.
- **Convert to Template**—select this option if you want to change the guest system into a template. This process is instant.

Customization Specifications

Customization specifications are optional, but they can greatly expedite automated desktop pool deployments by providing configuration information for such general properties as licensing, domain attachment, and DHCP settings.

To create a customization specification

1 In VirtualCenter, click **Edit** > **Customization Specifications**.

2 Click **New** to create a new Customization Specification.

3 Ensure that **Windows** is selected in the **Target Virtual Machine OS** drop down menu, and provide a name and an (optional) description for the customization specification in the fields provided. Click **Next**.

4 Enter the **Name** and **Organization** you would like associated with the desktops created in the automated pool in the fields provided. Click **Next** to continue.

5 Select one of the following:

- **Use the virtual machine name** if you want the desktops in the pool to derive their name from the name assigned to each desktop VM during deployment from View Manager. This is the recommended option.
- **Use a specific name** if you want each desktop to derive their name from a predefined label. If you choose this option, it is recommended that you also select the **Append a numeric value to ensure uniqueness** checkbox.

Click **Next**.

6 Enter the license number for the View Manager desktop operating system in the **Product ID** field, and specify if this is a single or multiple seat license. Click **Next**.

7 Enter and confirm the local administrator password in the fields provided. Click **Next**.

8 Select the local time zone from the drop down list. Click **Next**.

9 (Optional) You are presented with the opportunity to provide one or more command prompt instructions that will be executed the first time a user connects. Enter a command in the field provided and click **Add**. Repeat as necessary.

When you have finished, click **Next**.

10 Specify the type of settings you would like to use for your network interface. The recommended selection is **Typical settings**. Click **Next**.

11 Specify how the desktops derived from this template will participate in your network.

If you want to automatically add deployed desktops to a domain, select **Windows Server Domain** and enter the appropriate name in the field provided. In the username, password, and password confirmation fields, enter the credentials for a user who has the requisite level of permission to add a systems to this domain.

12 Ensure that the **Generate New Security ID (SID)** check box is selected and click **Next**.

Deploying an Automated Desktop Pool

1 From within the View Administrator, click the **Desktops and Pools** button and then click the **Inventory** tab. In the Global desktop and pool view pane, ensure that the **Desktops and Pools** tab is selected and click **Add**.

2 You are presented with the Add Desktop wizard. From here you can configure and deploy a new linked clone desktop pool. Select **Automated Desktop Pool** and click **Next**.

3 Select the type of desktop pool you want to create and click **Next**.

Pool Type	Description
Persistent	Desktops in this type of pool are allocated statically in order to ensure that users connect to the same desktop each time they log in.
Non-persistent	Desktops in this type of pool are allocated dynamically when the user logs in, and are returned to the pool when the user disconnects.

4 From the list provided, select the VirtualCenter server that will be used by this desktop. Click **Next**.

5 Enter the **Unique ID** and, optionally, the **Display name** and **Description**.

The unique ID is used by View Manager to identify the desktop pool and is the name that the user sees when logging in. The unique ID and display name can be arbitrary but if you do not specify a display name the unique ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters in length and is only visible from within View Administrator.

Once you have provided the desktop identification details, click **Next**.

6 Configure the desktop properties and click **Next**.

CAUTION If you are using Windows Vista as your Parent VM, you *must* set the power policy to **Ensure VM is always powered on**.

Property	Parameter Description
State	**Enabled**—after being created, the desktop pool is automatically enabled and ready for immediate use. **Disabled**—after being created, the desktop pool is disabled and unavailable for use. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
When VM is not in use	**Do nothing (VM remains on)**—Virtual machines that are powered off will be started when required and will remain on, even when not in use, until they are shut down. **Ensure VM is always powered on**—All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart. **Suspend**—All virtual machines in the pool enter a suspended state when not in use. **Power off**—All virtual machines in the pool shut down when not in use.
Automatic logoff after disconnect	**Immediately**—users are logged off as soon as they disconnect. **Never**—users are never logged off. **After**—the time after which users are logged off when they disconnect. Enter the duration in minutes in the field provided.
Power off and delete virtual machine after first use (non-persistent pools only)	Select this check box if you want the virtual machine to be deleted immediately after the user logs off. If necessary, a new virtual machine is cloned to maintain a specific pool size after virtual machines are deleted.
Allow users to reset their desktop	Select this check box if you want to allow desktop users to be able reset their own desktops without administrative assistance.
Allow multiple sessions per user (non-persistent pools only)	Select this check box if you want to allow individual users to simultaneously connect to multiple desktops in the same pool.

7 Configure the desktop provisioning properties and click **Next**.

Property	Parameter Description
Provisioning	**Enabled**—the desktops in the pool will be immediately created upon completion of the deployment procedure or after a desktop is deleted. **Disabled**—the desktops in the pool will not be immediately created upon completion of the deployment procedure or after a desktop is deleted.
Number of desktops	Specifies the number of desktops to create in this pool. This setting is disabled if you select the **Enable Advanced Pool Settings** check box in the **Advanced Settings** panel.

VM naming pattern	By default, a prefix is used to identify all desktops in a pool as part of the same group. The prefix can be up to 13 characters in length and a numeric suffix is appended to this entry in order to distinguish each desktop from others in the same pool.
	You can override this behavior by entering a name that contains a token representing the pool number; the token can appear anywhere in the name. For example:
	`amber-{n}-desktop`
	After deployment`{n}` is replaced with the pool number of the desktop.
	Fixed length tokens can be entered using the `n:fixed=` construction. For example:
	`amber-{n:fixed=3}`
	After deployment`{n:fixed=3}` is replaced with a fixed-length pool number for each the desktop: `amber-001`, `amber-002`, `amber-003` and so forth.
	A 15 character limit applies to names that contain a token, but only to the "replaced" form where the token length is fixed. For example:
	`my-view-system{n:fixed=1}`
	Where the token length is not fixed, a buffer of 1 is applied to the token, so the maximum "replaced" length is 14 characters. For example:
	`a-view-system{n}`

Property	Parameter Description
Stop provisioning on error	Select this check box if you want View Manager to automatically stop provisioning new virtual machines if an error is detected during desktop creation.
Advanced Settings	Click to display the advanced pool configuration settings. You can enable the advanced parameters by selecting the **Enable Advanced Pool Settings** check box. This will disable the **Pool Size** parameter. **Minimum number of virtual machines**—the minimum number of desktops that must be provisioned for this pool. **Maximum number of virtual machines**—the maximum number of desktops that can be provisioned for this pool. **Number of available virtual machines**—The number of virtual machines that must be unassigned and available for use at any given time. This figure cannot exceed the maximum number of desktops available to the pool overall.

8 Select the template to be used as the base image for the deployment. You are only presented with templates that contain a desktop operating system supported by View Manager. Click **Next**.

9 Select where you want the folder for this desktop pool to reside within VirtualCenter and click **Next**.

10 Select a host or a cluster on which to run the virtual machines used by this desktop and click **Next**.

NOTE Only clusters of 8 hosts or fewer are supported and shown.

11 Select a resource pool in which to run the virtual machines used by this desktop and click **Next**.

12 Select one or more datastores on which to store the desktop pool. If you do not have sufficient space available, you must add free space by selecting an additional datastore.

NOTE For clusters, only shared datastores are supported and shown.

Once you have configured the datastore storage criteria, click **Next**.

13 Select how you would like the desktops created from the guest system to be customized. If a customization specification exists on VirtualCenter you can select it from the **Use this customization specification** list in order to preconfigure such properties as licensing, domain attachment, and DHCP settings.

   If you want to manually configure the desktop or desktops in this pool after they have been provisioned, or if no customization specification is detected, select **None - Customization will be done manually**.

   Click **Next**.

14 You are presented with a summary of the configuration settings for this deployment.

   - If you are unsatisfied with any aspect of the configuration you can use the **Back** button to revisit any previous page.
   - If you are satisfied with the configuration click **Finish** to deploy the automated desktop pool.

Once the deployment has been initiated you can monitor the progress of the automated desktop pool by selecting either the **Desktops** or **Desktop Sources** tabs in the Global desktop and pool view pane.

Manual Desktop Pools

Manual desktop pools are pools of virtual machines that are manually constructed by the View Manager administrator. Desktop pools of this type can be either:

- Persistent—Users are allocated a dedicated desktop that retains all of their documents, applications and settings between sessions. The desktop is statically assigned the first time the user connects, and is then used for all subsequent sessions.
- Non-persistent—Users are connected to a different desktop from the pool each time they connect, and there is no persistence of environmental or user data between sessions.

Deploying a Manual Desktop Pool

1 From within the View Administrator, click the **Desktops and Pools** button and then click the **Inventory** tab. In the Global desktop and pool view pane, ensure that the **Desktops and Pools** tab is selected and click **Add**.

2 You are presented with the Add Desktop wizard. From here you can configure and deploy a new linked clone desktop pool. Select **Manual Desktop Pool** and click **Next**.

3 Select the type of desktop pool you want to create and click **Next**.

Pool Type	Description
Persistent	Desktops in this type of pool are allocated statically in order to ensure that users connect to the same desktop each time they log in.
Non-persistent	Desktops in this type of pool are allocated dynamically when the user logs in, and are returned to the pool when the user disconnects.

4 Specify the source type of the guest system by selecting **VirtualCenter virtual machine**. Click **Next**.

5 From the list provided, select the VirtualCenter server that will be used by this desktop. Click **Next**.

6 Enter the **Unique ID** and, optionally, the **Display name** and **Description**.

The unique ID is used by View Manager to identify the desktop pool and is the name that the user sees when logging in. The unique ID and display name can be arbitrary but if you do not specify a display name the unique ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters in length and is only visible from within View Administrator.

Once you have provided the desktop identification details, click **Next**.

7 Configure the desktop properties and click **Next**.

CAUTION If you are using Windows Vista as your Parent VM, you *must* set the power policy to **Ensure VM is always powered on**.

Property	Parameter Description
State	**Enabled**—after being created, the desktop pool is automatically enabled and ready for immediate use. **Disabled**—after being created, the desktop pool is disabled and unavailable for use. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
When VM is not in use	**Do nothing (VM remains on)**—Virtual machines that are powered off will be started when required and will remain on, even when not in use, until they are shut down. **Ensure VM is always powered on**—All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart. **Suspend**—All virtual machines in the pool enter a suspended state when not in use. **Power off**—All virtual machines in the pool shut down when not in use.
Automatic logoff after disconnect	**Immediately**—users are logged off as soon as they disconnect. **Never**—users are never logged off. **After**—the time after which users are logged off when they disconnect. Enter the duration in minutes in the field provided.
Allow users to reset their desktop	Select this check box if you want to allow desktop users to be able reset their own desktops without administrative assistance.

8 From the list provided, select the virtual machines you want to use add to the pool. Click **Next**.

9 You are presented with a summary of the configuration settings for this deployment.

- If you are unsatisfied with any aspect of the configuration you can use the **Back** button to revisit any previous page.
- If you are satisfied with the configuration click **Finish** to deploy the individual desktop.

Once the deployment has been initiated you can monitor the progress of the manual desktop pool by selecting either the **Desktops and Pools** or **Desktop Sources** tabs in the Global desktop and pool view pane.

Entitling a Desktop or Pool

Once a desktop or desktop pool has been created, you can entitle Active Directory users or groups to access it.

To entitle a desktop to an Active Directory user or group

1 From within View Administrator, click the **Desktops and Pools** button and then click the **Global desktop and pool view** entry under the **Inventory** tab. Choose the desktop or pool you want to entitle from the Global desktop and pool view pane.

2 Click **Entitlements**. You are presented with the Entitlements window which lists the users and groups who can use this desktop or pool. Click **Add**.

3 The user and group entitlement window is displayed. From here you view, search on, and filter all Active Directory users within the domain forest.

4 In **Type**, select **Users** checkbox, **Groups** checkbox, or both.

5 From the **Domain** drop down list, choose the domain that contains the users or groups you want to entitle, or select **Entire Directory** to search across the entire Active Directory domain forest.

6 Using the fields provided, you can search by name or description. Click **Find** to execute the search.

NOTE If you want to view a list of all users in the domain, leave the **Name** and **Description** fields blank.

---

7 From the table, choose the user or groups who you want to be able to use this desktop or pool and click **OK**.

8 You are returned to the first page of the Entitlements window, which now contains the users or groups you selected. Click **OK** to finish.

Searching Desktops and Entitled Users and Groups

Use the Inventory tab to search for information about desktops and entitled users and groups. You can either search by using the columns in the tables that appear on the right side of the page or search by using the categories that appear on the left side of the page.

To search columns in the Desktops Inventory view

1 From within the View Administrator, click the **Desktops and Pools** button.

2 In the **Desktops** field (on the right side of the page), click the **Desktops and Pools, Desktop Sources, or Active Sessions tab**.

3 Click the arrow the left of the search field select the checkboxes for the appropriate columns.

4 Click **Done**.

5 Enter search text and click **Go**.

To search categories in the Desktops Search view

1 From within View Administrator, click the **Desktops and Pools** button and click the **Search** tab on the left side of the page.

2 In the **Search for desktops and pools** field, enter search text.

3 Select or deselect **Display Name**, **Desktop ID**, **Type, User, or Virtual Center name**, **Desktop source**, or **Persistence** to search within that category**.**

4 Click **Search**.

To search columns in the Entitled Users and Groups Inventory view

1 From within View Administrator, click the **Users and Groups** button.

2 In the **Global user and group view** field (on the right side of the page), click the **Entitled Users and Groups, Active Sessions tab**, or (if available) **Offline Sessions**.

3 Click the arrow the left of the search field select the checkboxes for the appropriate columns.

4 Click **Done**.

5 Enter search text and click **Go**.

To search categories in the Entitled Users and Groups Search view:

1 From within View Administrator, click the **Users and Groups** button and click the **Search** tab on the left side of the page.

2 In the **Search for users and groups** field, enter search text.

3 Select or deselect **Name**, **Email**, **Display name**, or **Domain** to search within that category**.**

4 Click **Search**.

Working with Active Sessions

After users connect to a desktop, active sessions are listed in the inventory. You can view active sessions on the Inventory page.

To view, disconnect, or restart active sessions

1 From within View Administrator, click the **Desktops and Pools** button and click the **Inventory** tab on the left side of the page.

2 In Global desktop and pool view, click **Active Sessions**. From this view you can view the user, desktop ID, DNS name, start time, duration, and session state (connected or disconnected) for each active session.

3 Click anywhere in an active session. The **Disconnect Session**, **Logoff Session** and **Reset Virtual Machine** options become available.

Option	Description
Disconnect Session	The user is disconnected, but their session remains active.
Logoff Session	The user is disconnected and their session is logged off.
Reset Virtual Machine	The desktop is shutdown and restarted without a graceful logoff and disconnection.

4 Select the appropriate option, and click **OK** in the confirmation window.

Disabling View Manager and Deleting Objects

If you want to prevent users from accessing their desktops you can disable the View Connection Server to prevent clients from logging in. Currently logged in users are not affected when you disable the View Connection Server.

Disabling the View Connection Server is useful if you need to take it out of service for any reason. When a View Connection Server is disabled, end users who attempt to log in see a message stating that the connection failed and that View Connection Server is currently disabled.

To enable or disable a View Connection Server instance

1 Click the **Configuration** button.

2 Select the View Connection Server from the list of servers and click **Enable or Disable**.

Disabling a View Connection Server does not affect the current active desktop sessions nor will it prevent new desktop sessions from being established.

Deleting View Manager Objects

Delete View Manager objects (VirtualCenter connections, View Connection Server connections, and desktops) by using the administrator user interface.

To remove a VirtualCenter server connection from a View Connection Server

1 From within View Administrator, click the **Configuration** button.

2 In **VirtualCenter Servers,** select the VirtualCenter server you want to remove and click **Remove.**

If desktops are using this VirtualCenter server, an error message tells you that you must first delete the desktops using this VirtualCenter before you can delete the VirtualCenter.

If no desktops are using this VirtualCenter server, a warning message tells you that you can no longer access virtual machines managed by this virtual center.

3 Click **OK**.

The VirtualCenter server entry is deleted.

To delete a desktop pool from a View Connection Server

1 From within View Administrator, click the **Desktops and Pools** button.

2 In the Global desktop and pool, select a desktop or desktop pool from the list on the right click **Delete**.

You are given the option to remove the virtual machines from the connection broker only, which means they are still visible in VirtualCenter, or to delete them from disk, which means they are no longer visible in VirtualCenter.

If the desktop has active sessions, you are given the option to disconnect the users, which means users lose their connected desktops, or to leave the users connected, which means users do not lose their connected desktops.

Client Management 5

The locally installed View Client application and the Web-based View Portal component allow View Manager users to connect to their desktops. These applications can operate within an internal network or externally over the Internet, and their behavior can be modified in a number of ways.

In addition, View Client offers a variety of user authentication models—including secure authentication—all of which must be first configured on View Connection Server.

NOTE Users who want to use the Offline Desktop feature of View Manager must use the View Client with Offline Desktop, which allows both local (offline) and remote desktop access. See Chapter 7, "Offline Desktop," on page 123 for more information about this feature.

This chapter discusses the following topics:

View Client and View Portal

This section describes how to install the components required to use View Client and View Portal. You must be logged in as an administrator on the client system in order to carry out either of these tasks.

The functionality offered by View Client and View Portal is derived from the same set of locally installed base components. Users who have already installed View Client will be invited to install an additional ActiveX control on their browsers when they use View Portal for the first time.

Similarly, View Portal users who do not have View Client installed will be invited to allow the browser to automatically install the required View Client components the first time they connect online.

An expedient way of installing the View Client application is to visit the View Portal page and allow the browser to automatically install the required components on the client system. However, if you choose to do this you must be aware of the following:

- Virtual Printing and USB support is not provided by View Portal is not be available in View Client
- Windows Start Menu entries for View Client are not created after installation

If you install the View Client from the executable, USB support will be offered within the application, and Start Menu entries will be created.

NOTE View Portal does not support USB redirection, regardless of installation path.

To install View Client

1 Run the View Client executable on the system that will host the client, where `xxx` is the build number of the file:

```
VMware-viewclient-xxx.exe
```

The Installation wizard opens. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Choose your custom setup options. You may deselect the **USB Redirection** component if users do not need to access locally connected USB devices through their virtual desktops.

Click **Next** to accept the default destination folder or click **Change** to use a different destination folder and then click **Next**.

4 (Optional) Enter the IP address or FQDN of the server to which the client will connect and click **Next**.

5 Configure shortcuts for the View Client and then click **Next > Install > Finish**.

To start View Client

1 If View Client does not start automatically after installation, click **Start** > **Programs** > **VMware** > **View Manager Client**.

2 In the **Connection Server** drop-down menu, enter the host name or IP address of a View Connection Server and click **Connect**.

3 Enter the credentials for an entitles user, select the domain and click **Login**.

4 Choose a desktop from the list provided and click **Connect**.

View Client will attempt to connect to the specified desktop. Upon connection, the client window is displayed.

To connect to desktops using View Portal

1 Open a browser supported by View Portal, and enter URL of a standard or replica View Connection Server instance.

2 Enter an entitled username and password and select the correct domain from the drop-down menu.

3 Click **Login**.

4 When Access Status is Ready, choose a desktop from the list and click **Connect**.

View Client Policies

Certain View Client features can be controlled through policy. For information about configuring and applying policies to View Client at the global, pool, or user level refer to "Client Policies" on page 139.

Client Connections from the Internet

For a user to access a virtual desktop, their client system must be able to resolve the hostname or IP address of the specified View Connection Server. Initially—and by default—View Connection Server can only be contacted by tunnel clients that reside within the same network and are therefore able to locate the requested server.

Many organizations require that users can connect from an external location by using a globally resolvable domain or subdomain name or IP address, or by reassigning specific ports on an existing address, in order to route client requests to the appropriate location (typically, the security server). For example:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`

However, some additional configuration within View Connection Server is required for addresses like these to work.

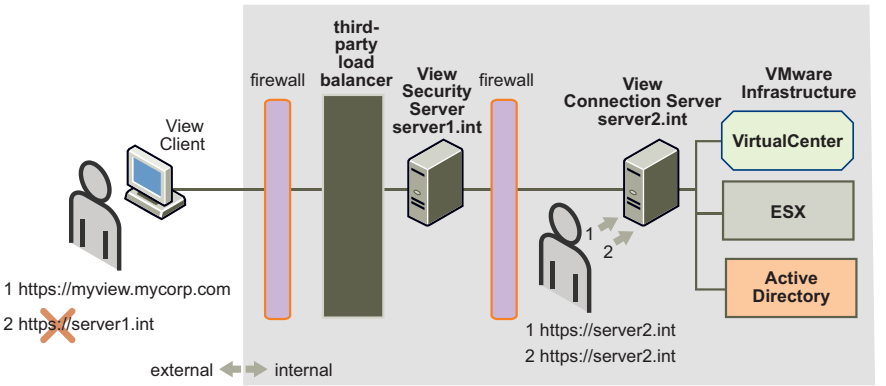
Overview of Client Connections

View Client attempts to create two separate TCP connections between itself and View Connection Server. The first connection handles user operations such as authentication, desktop selection, and so forth. The second connection is instantiated after logon and provides a tunnel for carrying RDP data.

The first connection is made using the URL or IP address entered by the user into the client. Providing the firewall and load-balancing components have been configured correctly in your network environment, this request reaches the server. Upon authentication, the fully qualified domain name (FQDN) of View Connection Server is returned to the client.

The second connection (the tunnel connection, which is SSL encrypted by default) is attempted using the FQDN. However, the connection fails if the FQDN cannot be resolved by the external View Client. An example sequence of external and internal client interactions with the server is shown in Figure 5-1.

Figure 5-1. External Client Connection



This scenario can be addressed by configuring View Connection Server to return an external URL instead of its own FQDN for the second connection channel.

The process of setting the external URL is not the same for all types of server. For standard or replica servers you can set the URL from within View Administrator. For a security server you must create or edit a properties file that contains the inbound connection details and save it in a directory located under the security server installation path.

CAUTION For security servers, you must use the method described in "Generating locked.properties Automatically" on page 74 if you intend to use message security mode in your View Manager environment—the configuration file created by this procedure contains information that is critical to this type of global configuration.

To set the external URL on a standard or replica server

1 From within View Administrator, click the **Configuration** () button.

2 Under View Servers select a View Connection Server entry and click **Edit**.

3 Enter a URL in the **External URL** field. The name must contain the protocol, address and port number. For example:

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

Click **OK.**

To set the external URL on a security server

Create or edit a text file that contains the externally resolvable name of the security server, port number, and protocol, and save it in the following location on the security server:

```
C:\Program Files\VMware\VMware
View\Server\sslgateway\conf\locked.properties
```

For example, if the externally resolvable name of the security server is `viewsecure.example.com`, the port number is `443`, and the client protocol is `HTTPS`, create a properties file called `locked.properties` that contains the following entries:

- `clientHost=viewsecure.example.com`
- `clientPort=443`
- `clientProtocol=https`

NOTE You must restart the View Connection Server service for these changes to take effect.

Generating locked.properties Automatically

If you have already associated a security server with your standard server or replicated group you can generate the `locked.properties` configuration file automatically from View Administrator on any standard or replica server.

To generate a Security Server locked.properties file from the Configuration view

1 From within the View Administrator on a standard or replica server, click the **Configuration** () button.

2 Under Security Servers, click **Add**. The Add Security Server window is displayed.

3 Enter the FQDN of the security server in the **Server Name** field.

4 Enter the external URL in the **External URL** field. The name must contain the protocol, address and port number. For example:

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

Click **OK.** The security server is added to the Security Servers list in the Configuration view.

5 Select the security server entry and click **Download security keys**. Your browser will download the configuration file.

6 Save this file as `locked.properties` in a convenient location and then copy it to the following location on the security server:

```
C:\Program Files\VMware\View Manager\Server\sslgateway\conf
```

NOTE On the security server, you must restart the View Connection Server service for these changes to take effect.

Configuring locked.properties

In addition to determining the information returned to the client in order to establish a tunnel connection, the `locked.properties` file can contain properties relating to the security server communications. These properties are described in Table 5-1.

Table 5-1. locked.properties—Client and Server properties

Property	Description
`clientHost`	The externally resolvable hostname that the client is instructed to use when contacting the security server. If not specified, this is set to the value specified by `serverName` or the system default.
`clientPort`	The port that the client is instructed to use when contacting the security server. If not specified, this is set to the value specified by `serverPort` or the system default.
`clientProtocol`	The protocol that the client is instructed to use when contacting the security server—this can be `http` or `https`. If not specified, this is set to the value specified by `serverProtocol` or the system default.
`serverName`	The unique identity of the security server.
`serverPort`	The port that the security server listens on. Default is `80`.
`serverProtocol`	The protocol that the security server uses—this can be either `http` or `https`. Default is `http`.

By default, the `clientHost`, `clientPort`, and `clientProtocol` properties default to those exhibited by the security server; the server settings themselves can be explicitly configured using the `serverName`, `serverPort`, and `serverProtocol` properties. If these values are explicitly set, the port and protocol values should correlate between client and server.

One scenario where you may need to specify different port and protocol settings is where an intermediary SSL accelerator exists between the client and security server. In an arrangement such as this, the `clientPort` and `clientProtocol` could be set to `443` and `https`, but the back-end communications between the accelerator and the server could take place over `http` using port `80`.

Creating SSL Server Certificates

A Secure Sockets Layer (SSL) certificate is a cryptographically sealed data object that contains the identity of a server, public and private encryption keys, and the digital signature of the certificate issuer. Certificates serve two major purposes:

- They can provide authenticated proof to a client that the web site they visit is owned by the company or individual who has installed the certificate.
- They contain the public key that the client uses to establish an encrypted connection to a server.

By default, in View Connection Server when a client visits a secure page such as View Administrator they are presented with the self-signed certificate provided with the application. By reading the server certificate the user can decide if the server is a trusted source, and then accept (or reject) the connection.

The certificate can be signed by a Certificate Authority (CA)—a trusted third party who guarantees the identity of the certificate and its creator.

To create your own certificate for View Connection Server do one of the following:

- Create a self-signed certificate for your system using the `keytool` utility provided with the Java Runtime Environment (JRE) instance that accompanies View Connection Server. Self-signed certificates are user generated certificates that have not been officially registered with any trusted CA, and are therefore not guaranteed to be authentic.
- Create a certificate and then send a certificate signing request (CSR) that contains your certificate details to a CA. After conducting some checks on the company or individual making the application, the CA signs the request and encrypts it with their private key. The valid certificate is returned and is then inserted into a keystore on View Connection Server.

Clients connecting to View Connection Server are presented with your certificate. If the certificate is self-signed but accepted by the user, or signed by a CA that is trusted by the client browser, the client uses the public key contained within the certificate to encrypt the data it sends to View Connection Server. Typically, the certificate for the CA itself is embedded in the browser or is located in a trusted database that is accessible by the client.

NOTE Certificates are only required for standard, replica, or security servers that receive direct connections from their clients. If you are using a security server as your client-facing system, only this server will require a certificate.

Once a certificate has been accepted, the client responds by sending its own public key so that View Connection Server can encrypt the data it transmits to the client. In this way, a secure connection between the client and server is established.

By default, View Connection Server includes a self-signed SSL certificate that clients can use to create secure sessions when they connect. This certificate is not trusted by clients and does not have the correct name for the service, but it does allow connectivity.

You can replace the default certificate provided with View Manager with a properly defined certificate for the service. If the certificate is signed by a trusted CA, users will not be presented with messages asking them to verify the certificate, and thin client devices will be able to connect without requiring additional configuration.

To create and install your own certificate you must first add the Java `keytool` utility to your command path so that you can execute it from any location using the command prompt. Once this is done you can create a self-signed SSL certificate using the `keytool` utility.

To obtain a validated certificate that has been signed by a trusted certificate authority you must first submit a certificate signing request (CSR) to a the CA in order to receive a trusted certificate. Once you have received a trusted certificate from the CA you can import it into the keystore for the View Connection Server, and then configure View Connection Server to use it.

NOTE You may already have an SSL certificate that you want to use with View Connection Server. Refer to "Using Existing SSL Certificates" on page 81 for more information on how to do this.

To add the Java keytool to the system path

1 Press the Windows key+Break to display the Windows System Properties dialog box.

2 Under the **Advanced** tab, click on **Environment Variables**.

3 In the System variables group, select **PATH** and then click **Edit**.

4 In the **Variable value** field add the path to the JRE installation directory:

```
C:\Program Files\VMware\View Manager\Server\jre\bin
```

Ensure that this entry is delimited with a semicolon (`;`) from any other entries present in the field.

5 Click **OK** > **OK** > **OK** to close the Windows System Properties dialog box.

Creating an SSL Certificate

Deciding what name to bind to a certificate is an important consideration. A certificate binds the name of the service to a cryptographic key pair and, in doing so, assumes ownership of the service and keys. Once the certificate is signed the client can trust the server (and its cryptographic key) because the CA independently determined that the organization that is claiming ownership requested the key.

The most important part of the certificate is the common name (CN) attribute. Use the fully qualified domain name that the client computer uses to connect to the View Connection Server. In a single-server environment, the name is typically the name of the server. If load balancing is being used, use the load-balanced name.

To create a self-signed SSL certificate

1 From a command prompt, enter the following:

```
keytool –genkey –keyalg "RSA" –keystore keys.p12 –storetype pkcs12
–validity 360
```

2 You are prompted to enter a password for the keystore and then to provide information about yourself and your organization. When you are asked to enter your first and last name, enter the FQDN of the View Connection Server instance you want to secure.

3 Enter your department, organization, location, state, and country. The latter must be in the form of a two-letter country code.

4 You are shown a summary of the data you have entered and are asked if you want to proceed. Enter yes if you are satisfied that the details are correct.

5 You are prompted for a key password, which is the password specifically for this certificate (as opposed to any other certificates stored in the same keystore file). The `keys.p12` file is created in the current directory.

It is advisable to back up the `keys.p12` file after the certificate is imported into it in case you need to rebuild the configuration for the server at some point.

Validating the SSL Certificate

Self-signed certificates, while adequate for data encryption between server and client, do not provide any reliable information about the location of View Connection Server or the corporate entity responsible for its administration.

Where it is important for your clients to be able to determine the origin and integrity of the data they receive, it is recommended that you obtain a CA-authenticated certificate for your site.

To create a certificate signing request (CSR)

From a command prompt, enter the following where `<secret>` is the keystore password:

```
keytool –certreq –keyalg "RSA" –file certificate.csr –keystore
keys.p12 –storetype pkcs12 –storepass <secret>
```

The `certificate.csr` file is created in the same location. The contents of the file should resemble a slightly longer version of the following example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----

MIIBuDCCASECAQAweDELMAkGA1UEBhMCR0IxEDAOBgNV

BAgTB1Vua25vd24xEDAOBgNVBAcTB1Vua25vd24xFDAS

BgNVBAoTC1ZNd2FyZSBJbmMuMRMwEQYDVQQLEwp2bXdh

XU8/2jEUL5DocLDLnygsUD2g7cUMYdz/HeECAwEAAaAA

AeHnsPs7a1Q0JH6OZvdU

-----END NEW CERTIFICATE REQUEST-----
```

To submit the CSR and import the certificate

1 Send the CSR file to a certificate authority in accordance with their enrollment process and request a certificate in PKCS7 format. As part of this process, you may need to provide proof of identity, proof of domain ownership, and so forth.

NOTE If the certificate authority does not offer PKCS#7 as a format, use the default settings provided—you will be able to export the certificate data in the appropriate format at a later stage.

For testing purposes, many certificate authorities also provide a free temporary SSL certificate based on an untrusted root:

Thawte—https://www.thawte.com/cgi/server/try.exe

VeriSign—http://verisign.com/ssl/buy-ssl-certificates/free-ssl-certificate-trial

GlobalSign—http://globalsign.com/free-ssl-certificate/free-ssl.htm

---

NOTE A temporary certificate is preferable to the default self-signed certificate supplied with View Manager because it uses the correct domain name. However, clients still issue warnings that the service is not trusted.

---

2 If you have received either a temporary or full PKCS#7 certificate from the CA, copy the contents of the file into a text editor and save it as `certificate.p7`. The contents of the file should resemble a slightly longer version of the following example:

```
-----BEGIN PKCS7-----

MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgkqhkiG9w0BBwGgggXNMIID

LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgkqhkiG9w0BAQUFADCBhzEL
```

```
i7coVx71/lCBOlFmx66NyKlZK5mObgvd2dlnsAP+nnStyhVHFIpKy3nsDO4JqrIg

EhCsdpikSpbtdo18jUubV6z1kQ71CrRQtbi/WtdqxQEEtgZCJO2lPoIWMQA=

-----END PKCS7-----
```

3 From a command prompt, enter the following where <secret> is the keystore password:

```
keytool –import –keystore keys.p12 –storetype pkcs12 –storepass
<secret> –keyalg "RSA" –trustcacerts –file certificate.p7
```

If you are using a temporary certificate you may be presented with the following message:

```
... is not trusted. Install reply anyway?
```

This message is generated because the root certificate given to you is not trusted by Java because it is a test certificate and not for production use.

To configure the View Connection Server to use the new certificate

1 Place a new certificate file in the following location on a standard, replica, or security server instance of View Connection Server:

```
C:\Program Files\VMware\View Manager\Server\sslgateway\conf
```

2 Create or edit the following file on each server:

```
C:\ProgramFiles\VMware\View
Manager\Server\sslgateway\conf\locked.properties
```

3 Add the following properties:

- `keyfile=keys.p12`
- `keypass=secret`

This changes the values as needed to match what you created in the previous step.

4 Restart the View Connection Server service.

Assuming your environment is configured to use SSL, a log message like the following appears:

```
13:57:40,676 INFO  <Thread-1> [NetHandler] Using SSL certificate
store: keys.p12 with password of 6 characters
```

This message indicates that the configuration is in use.

Using Existing SSL Certificates

You organization may already have a valid (CA signed) SSL certificates that you want to use with View Connection Server. In order to use an SSL certificate you will require both the certificate and the private key that accompanies it.

Exporting from Microsoft IIS Server

In order to use an existing Microsoft IIS SSL server certificate, you must first export it from the IIS application server that hosts the Web site, or sites, that use it. Windows provides visual tools to assist you with this.

To export an SSL server certificate from the IIS application

1 On the IIS application server host system, click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**. The Internet Information Services Manager is displayed.

2 From the tree widget in the left pane, expand the local computer entry and then click Web Sites to view the list of sites hosted by the server.

3 In the right-hand pane, right-click the Web site entry that contains the SSL certificate you want to export, and select **Properties** from the context menu. The Web site properties window is displayed.

4 Select the **Directory Security** tab. Under Secure communications click **Server Certificate**. You are presented with the Web Server Certificate wizard. Click **Next**.

5 Select **Export the current certificate to a .pfx file**. Click **Next**.

6 Specify a filename for the file you want to export. Click **Next**.

7 Enter and confirm a password that will be used to encrypt the information you want to export. Click **Next**.

8 You are shown a summary of the certificate you are about to export. Ensure that the information is correct (and that you have selected the correct certificate) and click **Next** > **Finish**.

The certificate is exported to the specified location. You must now carry out the procedure described in "To configure the View Connection Server to use the new certificate" on page 80. Ensure that the `keypass` entry in the `locked.properties` file corresponds to the password you used when exporting the certificate.

Smart Card Authentication

Some organizations require personnel to pass multiple stages of authentication before allowing them to connect to their systems. View Manager provides support for high-security environments by offering smart card authentication of client sessions.

Smart card authentication works by presenting a trusted set of client credentials—a user certificate—to View Connection Server. A user certificate is an encrypted set of authentication credentials that includes the digital signature of the trusted root Certificate Authority (CA) that issued the certificate.

The user certificate is stored on the smart card and can only be retrieved and passed to the server after the user has verified their ownership by entering a personal identification number (PIN). Certificates are then authenticated by using a public key to verify the included digital signature; the expected digital signature is contained in a trusted CA certificate that is stored on View Connection Server.

This following sections describe how to configure and enable this feature on View Connection Server.

NOTE Smart card authentication is only supported by View Client; it is not supported by View Administrator, View Portal, or by offline desktop instances accessed through View Client with Offline Desktop.

Smart Card Hardware

Each client system using smart card authentication will require View Client and a Windows-compatible smart card reader to be installed.

In order to recognize and use the smart card hardware, product-specific application drivers must be installed on both the client systems and remote desktops. Smart card profiles can vary between vendors; refer to the documentation that accompanies the smart card reader for more information about how to do this.

Obtaining a Root Certificate

You must obtain the root certificate from the CA that signed the certificates on the smart cards presented by your users. The root certificate is obtained from one of the following sources:

- Microsoft IIS server running Microsoft Certificate Services. The procedure for installing Microsoft IIS, issuing certificates, and distributing them in your organization exceeds the scope of this guide. Refer to the following Web resources to learn more about these tasks:
  - How to Install IIS on Windows Server 2003: http://technet.microsoft.com/library/aa998483.aspx
  - Managing Microsoft Certificate Services: http://technet.microsoft.com/library/bb727098.aspx
- The public root certificate of a trusted third-party CA. This is the more likely source in environments with a pre-existing smart card infrastructure and a standardized approach to smart card distribution and authentication (for example, governmental or military establishments).

Once you have determined the correct certificate to be used, looking at the signing chain will list a series of signing authorities. Usually the best certificate to select is the intermediate authority immediately above the user certificate. Check that this is not used to sign other certificates on the card.

Exporting a Root Certificate from a User Certificate

If you do not have the root certificate of the CA but have been provided with a CA signed user certificate, or a smart card that contains one, you can export the root certificate from this information if the root certificate is trusted by your system.

NOTE If you have been provided with a smart card that contains a user certificate, insert the smart card into the reader. In many cases this will automatically add the user certificate to your personal store. If this does not happen you must use the software that accompanies the reader to export the user certificate to a file which you can then import into Internet Explorer during the following procedure.

To export a root certificate from a user certificate

1 Start **Internet Explorer** and click **Tools** > **Internet Options**.

2 Under the **Content** tab, click **Certificates**.

3 Under the **Personal** tab, select the certificate you wish to use and click **View**.

NOTE If the user certificate is not present in the list you must first click the **Import** button to manually import the user certificate. Once the certificate has been imported, select it from the list and click **View**.

4 Under the **Certification Path** tab, select the certificate at the top of the tree and click **View Certificate**.

5 Under the **Details** tab click **Copy to File**. You are presented with the Certificate Export Wizard.

6 Click **Next** > **Next**, and enter a name and location for the file you want to export.

7 Click **Next**. The file is saved as a root certificate in the location specified.

Trust Hierarchies

A user certificate may be signed as part of a trust hierarchy—the signing certificate may itself be signed by another, higher level, certificate.

While it is permitted to use any signing certificate from anywhere within the hierarchy, it is best practice to use the parent certificate (the one that actually signed the user certificate) as your root certificate.

Adding a Root Certificate to Trusted Roots on Active Directory

This section describes how to import the third-party root CA certificates into both Active Directory and the Enterprise NTAuth store. The procedures described below are only required if you are using a third-party CA to issue smart card logon or domain controller certificates—they are not required in environments where the Windows Domain Controller acts as the Root CA.

To add the third-party root CA to the trusted roots in an Active Directory Group Policy object

1 Click **Start** > **All Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

2 In the left pane, locate the domain in which the policy you want to edit is applied.

3 Right-click the domain, and then click **Properties**.

4 Under the Group Policy tab, click the **Default Domain Policy Group Policy** object, and then click **Edit**. A new window is displayed.

5 In the left pane, expand **Computer Configuration > Windows Settings** > **Security Settings** > **Public Key Policy**

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

7 Follow the instructions in the wizard to import the certificate. Click **OK**.

8 Close the Group Policy window.

By adding the certificate to the list of trusted roots, you are ensuring that all systems in the domain have a copy of the certificate in their trusted root store.

To add the third-party root CA to the NTAuth store in Active Directory

To import a CA certificate into the Enterprise NTAuth store enter the following from the command prompt on the Active Directory server, where `<certificate>` is the path to the third-party root CA certificate:

```
certutil –dspublish –f <certificate> NTAuthCA
```

By publishing the certificate to the Enterprise NTAuth store, you are confirming that the CA is trusted to issue certificates of this type.

Creating a Truststore

A truststore is a keystore that is used by View Manager when making decisions about which clients to trust. In order for View Connection Server to authenticate smart card users and connect them to their desktops, the root certificate for all trusted users must first be added to the server truststore.

A truststore can be created by using the `keytool` utility provided with the Java Runtime Environment (JRE) instance that accompanies View Connection Server.

To add the JRE utilities to your command path

1 Press the Windows key+Break to display the Windows System Properties dialog box.

2 Under the **Advanced** tab, click on **Environment Variables**.

3 In the System variables group, select **PATH** and then click **Edit**.

4 In the **Variable value** field add the path to the JRE installation directory:

```
C:\Program Files\VMware\View Manager\Server\jre\bin
```

Ensure that this entry is delimited with a semicolon (`;`) from any other entries present in the field.

5 Click **OK** > **OK** > **OK** to close the Windows System Properties dialog box.

Using keytool to Create a Truststore

From a command prompt, enter the following where <alias> is a unique (case-insensitive) name for a new entity entry in the truststore (in this case, the certificate you are about to import), <certificate> is the name of the root CA certificate you previously obtained or exported, and <truststore filename> is the name of the truststore output file:

```
keytool –import –alias <alias> –file <certificate> –keystore
<truststore_filename>
```

NOTE You may be asked to create a password for the keystore—this is not required for future procedures, but you should remember it if you want to add additional certificates to the truststore at a later date.

Enabling Smart Card Authentication on the Server

All types of View Connection Server support smart card authentication but it is recommended that only security servers are configured to allow smart card access. If you add smart card support to standard or replica servers you will be prompted to select a certificate every time you connect to View Administrator on those systems.

NOTE In environments where not all users will authenticate using a smart card it is also recommended that you configure a new (or an additional) security server specifically for the purpose of client smart card authentication.

To add smart card authentication to View Connection Server

1 Copy the truststore file you previously created (<truststore_filename>) to the following location on View Connection Server:

   `C:\Program Files\VMware\View Manager\Server\sslgateway\conf`

2 Create a text file called `locked.properties` that contains the following entries:

   - `trustKeyfile=<truststore filename>`
   - `trustStoretype=JKS`
   - `useCertAuth=true`

   The value for `trustKeyfile` must correspond to that of <truststore filename>.

You must restart the View Connection Server service for these changes to take effect.

NOTE Once a standard or replica View Connection Server has been configured, you will be prompted to choose a certificate when logging in to View Portal or to View Administrator on that server.

Configuring a Standard or Replica Server

A security server that has been configured to use smart card authentication will automatically require the user to authenticate using their card and PIN during login. Standard and replica servers can be configured to accommodate several different smart card authentication scenarios.

To set the smart card authentication setting on a standard or replica server

1 From within the View Administrator, click the **Configuration** ( ) button.

2 Under View Servers select a View Connection Server entry and click **Edit**.

3 From the **Smart card authentication** drop-down menu, select one of the following:

- **Not allowed**—Smart card authentication is disabled.
- **Optional**—Users may use smart cards authentication to connect, but password authentication is also permitted. Failure to authenticate using a smart card authentication will require that password authentication is used instead.
- **Required**—Users may only connect using smart card authentication.

4 Click OK.

NOTE Smart card authentication only replaces Windows password authentication. If SecurID is enabled, users will still be required to authenticate using this mechanism as well.

Configuring User Profiles

A user principal name (UPN) is an account name and a domain name identifying the domain in which the user account is located. For a user to connect using smart card authentication, their user account in the Active Directory must have a valid UPN associated with their `userPrincipalName` property.

The UPN for each user who requires smart card authentication must be set to the subject alternative name (SAN) contained within the root certificate of the trusted CA. You can locate this information by viewing the certificate properties, as described in "Exporting a Root Certificate from a User Certificate" on page 83.

To set the UPN to the SAN on ADAM

1 On any standard or replica connection server, click **Start** > **All Programs** > **ADAM** > **ADAM ADSI Edit**.

2 In the left pane, expand the domain in which the user you want to edit is located and expand **CN=Users**.

3 Right-click the user, and then click **Properties**. An attribute editing window for the user is displayed.

4 Double-click the user `userPrincipalName` entry from the list. In the field provided, enter the SAN value of the trusted CA certificate.

5 **Click OK** > **OK**, and close ADAM ADSI Edit.

RSA SecurID Authentication

View Manager supports RSA SecurID as an additional method for user authentication. RSA SecurID provides strong, two-factor authentication when users access virtual desktops, in addition to the authentication provided when using Active Directory credentials.

If you are using RSA SecurID, you must first enable it by editing your View Connection Server settings. After you install the RSA SecurID software on your server or servers, you can edit RSA settings in the View Administrator user interface.

To enable or edit RSA SecurID

1 From within the View Administrator, click the **Configuration** () button.

2 Under View Servers select a View Connection Server entry and click **Edit**.

3 Under the RSA SecurID 2-Factor Authentication heading, configure the desired RSA settings:

- **Enable**—Enables RSA SecurID authentication for end users accessing virtual desktops.
- **Enforce SecurID and Windows user name matching**—SecurID checks user names against the Active Directory user names and denies access to entries that do not match.
- **Clear node secret**—refers to the node secret on the View Agent.

For more information about this setting, see the RSA Authentication Manager user documentation.

4 In the **Upload RSA authentication agent configuration file (sdconf.rec)** field, enter the location of the `sdconf.rec` file or click **Browse** to search for the file. For more information about the `sdconf.rec` file, refer to the RSA Authentication Manager user documentation. Click **OK**.

View Client Command Line Options

View Client has a number of startup options that can be invoked when launching the application from a command prompt. Options are preceded by a hyphen (–) or a forward slash (/), are case-insensitive, and can be abbreviated down to their shortest unique form. For example, to display the full list of commands enter the following:

```
"C:\Program Files\VMware\View Manager\Client\bin\wswc" /?
```

To launch View Client in fully scripted mode—that is, with all connection, user, and desktop criteria provided—enter the following:

```
"C:\Program Files\VMware\View Manager\Client\bin\wswc" –serverURL
<server> –userName <username> –password <password> –domainName
<domain> –desktopName <desktop>
```

Table 5-2 describes the command line options you can use when you launch View Client.

Table 5-2. View Client Command Line Options

Property	Description
`file <xxx>`	Text file with additional command line parameter. To simplify repetitive tests, type `wswc /f test1`.
`nonInteractive`	Used to suppress error message boxes in fully scripted startup.
`languageId <xxx>`	Provides localization support for different languages in View Client. If a resource library is available you can specify the Windows language ID to use. For US English, enter `0x409`
`desktopName <xxx>`	Desktop name for the select desktop dialog box. **Note:** This is the name as you see it in the select desktop dialog box.
`serverURL <xxx>`	The URL for View Connection Server.
`userName <xxx>`	The username of the client user.
`password <xxx>`	The password of the client user.
`domainName <xxx>`	The domain name of the client user.
`screenFull`	Start the session in full-screen mode. This property requires the `desktopName` property to be supplied.
`screenWindow`	Start the session in a window. This property requires the `desktopName` property to be supplied.
`screenMulti`	Start the session in full-screen multi-monitor mode. This property requires the `desktopName` property to be supplied.

Table 5-2. View Client Command Line Options (Continued)

Property	Description
`rollback`	(Offline Desktop only) Unlocks the online version of a checked out desktop and discards the offline session. This property requires the `desktopName` property to be supplied.
`checkout`	(Offline Desktop only) Checks out the specified desktop, and locks the online equivalent. This property requires the `desktopName` property to be supplied.
`checkin`	(Offline Desktop only) Checks in the specified desktop and unlocks the online equivalent. This property requires the `desktopName` property to be supplied.
`staycheckedout`	(Offline Desktop only) Backs up the data on a checked out desktop to the server, but keeps the offline desktop checked out. This property requires the `desktopName` property to be supplied.
`offlineDirectory <xxx>`	(Offline Desktop only) Specifies the local directory path into which a new offline desktop is downloaded. This property requires the `desktopName` property to be supplied.

All parameters except `file`, `langaugeId`, `rollback`, `checkout`, `checkin`, `staycheckedout`, and `offlineDirectory` can also be specified by Active Directory group policies. Refer to Chapter 8, "Component Policies," on page 135 for more information about this.

NOTE Command line properties override system policies, which in turn override user policies.

Virtual Printing

The Virtual Printing (ThinPrint) feature of View Manager allows View Client and View Client with Offline Desktop users to transparently use local or network printers from within their remote systems, yet removes the requirement for installing proprietary printer drivers on each View Manager desktop.

NOTE View Portal does not support Virtual Printing.

Virtual Printing is a plug-and-play solution; once a printer is installed on the local system it is automatically added to the list of available printers on the View Manager desktop. No further configuration is required.

Virtual Printing consists of a guest component (.print Client) which resides within the View Client or View Client with Offline Desktop application, and a host component (.print Engine) which is part of the View Agent service on the View Manager desktop. Jobs are sent by .print Engine to .print Client over an RDP connection.

NOTE On an offline desktop, .print Engine uses a named pipe (`Com1:`) to pass print data to .print Client.

Where a user has administrative privileges, printer drivers can still be installed on the View Manager desktop; this action does not interfere with the virtual printing component.

To configure a virtual printer instance on the View Manager desktop

1 Click **Start** > **Settings** > **Printers and Faxes**. The Printers and Faxes window is displayed.

2 Right-click any of the locally available printers and select **Properties** from the context menu. You are presented with the print properties window associated with the selected printer.

3 Select the **ThinPrint Device Setup** tab.

4 Using the slider, select an option for print data compression:

- **No images**—Only text is printed.
- **Extreme**—Images are compressed with maximum possible compression rate without regard to image quality.
- **Maximum**—Images are compressed with good quality.
- **Optimal**—Images are compressed with optimal quality.
- **Normal**

Enable or disable the **duplex** and **Show tray selection** check boxes as required.

5 Select the **General** tab and click **Printing Preferences**.

6 Edit the page and color settings; the default values are acquired from the host printer.

7 Click the **Advanced** tab. If the printer installed on the host supports these options, edit the following settings for double-sided printing: Long edge for portrait or Short edge for landscape printing.

   To preview each printout on the host, enable **Preview on client before printing**. From this preview, you can use any printer with all its available properties.

8 Click the **Adjustment** tab to view the automatic print adjustment options. VMware recommends that you retain the default settings.

9 Click **Apply** or **OK**. Click **OK** to close the print properties window.

6 View Composer

The View Composer feature provides a versatile and highly storage-efficient alternative to creating and managing many standalone virtual machines. This chapter provides an overview of View Composer functionality of View Manager.

In addition to offering a conceptual overview of how linked clone desktops are created within VirtualCenter by View Composer and managed by View Manager, the following sections describe how to prepare VirtualCenter and a base virtual machine image for use in a View Composer deployment.

This chapter discusses the following topics:

Overview of View Composer

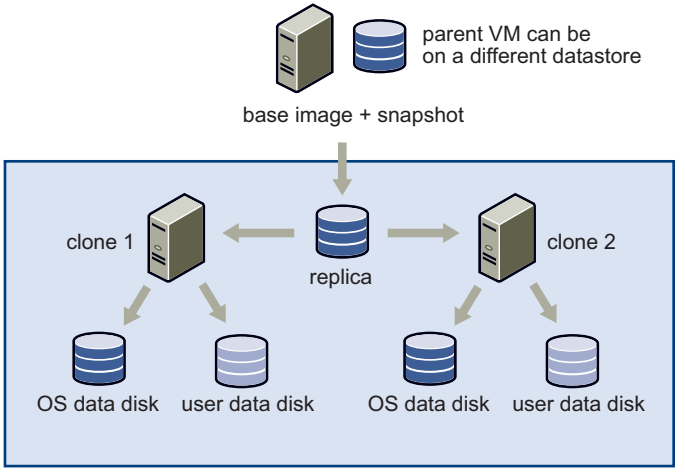
The View Composer feature enables View Manager administrators to rapidly clone and deploy multiple desktops from a single centralized base image, called a Parent VM. Once the desktops have been created they remain indirectly linked to a snapshot residing on the Parent VM.

The link is indirect because the first time one or more desktop clones are created, a uniquely identified copy of the Parent VM—called a replica—is also created. All the desktop clones are anchored directly to the replica and not to the Parent VM. Desktops of this type are called linked clone desktops.

The Parent VM can be updated or replaced without directly affecting the linked clone desktops and can therefore can be viewed as a standalone virtual machine. This set of relationships is illustrated in Figure 6-1.

NOTE If a replica is deleted the desktops anchored to them will cease to work, so replicas are treated as protected entities within VirtualCenter.

Figure 6-1. Parent VM, Linked Replica, and Desktop Clones



Because all the linked clone desktops in this environment are connected to a common source, View Composer permits the centralized management of desktops while maintaining a seamless user experience. Tasks such as resetting each system to its default configuration, balancing storage, installing software, and applying service packs are greatly accelerated by this type of deployment.

View Manager administrators can simultaneously update (or change) the operating systems of all linked clone desktops, install or update client applications, or modify the desktop hardware settings by carrying out these activities on the Parent VM and then anchoring the linked clones to a new snapshot of this configuration. This action is called desktop recomposition.

Administrators can also return the operating system data of each linked clone desktop—which may have expanded through ongoing usage—to its original state (that of the Parent VM) by carrying out an action called desktop refresh.

NOTE Linked clones can also be anchored to a new snapshot of a completely different Parent VM.

View Administrator delivers a high-level overview of what actions are being carried out. Policies can control what actions are executed and at what time in order to minimize disruption to the user base. Connected users can be notified with custom messages if an update that will affect their session is about to take place.

Linked Clone Desktop Disk Usage

The initial disk usage of a linked clone virtual machine is far lower than that of a full clone because the operating system and client applications are derived from a Parent VM. The greatly reduced storage overhead for operating system and user data is accomplished through the use of delta disks and thin provisioning.

Every new desktop created in a standard (non-linked clone) automated pool is a duplicate of a base template. Consequently, each standard clone uses the same amount of disk space as the base template because the operating system data and user data of the base template is replicated by every clone created in the pool.

View Composer greatly reduces the physical storage overhead of linked clone desktop pools through use of delta disks: abstract storage mechanisms whose logical size can be greater than their physical size. Thin disk growth depends on factors such as workload, power-off policy, pool type and so forth.

In a linked clone deployment, delta disks are used by the desktop to store the data difference between its own operating system and the operating system of the Parent VM from which it is derived. Immediately after deployment, the difference between the Parent VM and each of its linked clones is extremely small; thus, the delta disk is also extremely small.

Because the delta disks for each desktop will inevitably grow over time, during linked clone deployment you can define the maximum allowable size of each virtual machine, up to the original size of the Parent VM. The amount of disk space required to store the difference between the linked clone operating system data and Parent VM operating system data will typically remain far smaller than that required by a standard clone. If the size of the delta disk gets too large it can be returned to its baseline state by carrying out a desktop refresh.

Thin provisioned disks (thin disks) are used by the linked clones to store user data, and are not linked to the Parent VM. This type of disk occupies no more space than that required by the data it contains but does not reduce in size if data is removed. These disks are not affected by recomposition or refresh events.

Storage Overcommit

When the datastore for a new linked clone desktop pool is being assigned, administrators can control how aggressively the system assigns new virtual machines to the free space available on the datastore by modifying the storage overcommit property.

When the storage overcommit level is low, the majority of free space is used as buffer in which the delta disks for each clone can expand. As the overcommit level increases, less space is reserved for individual delta disk growth but more virtual machines will fit on the datastore.

A very aggressive level of storage overcommit results in a relatively small amount of space being reserved for delta disk expansion; however, administrators can add a lot of extra virtual machines to the datastore if they predict that the delta disks of each virtual machine will never grow to their maximum possible size.

While a high overcommit level may be optimal for creating a large number of virtual machines, a desktop pool of this type also demands more attention from the administrator in order to ensure that the remaining disk space is not completely consumed by virtual machine expansion. This condition can be prevented by periodically refreshing or rebalancing the desktop pool and reducing the size of the operating system data to its baseline level.

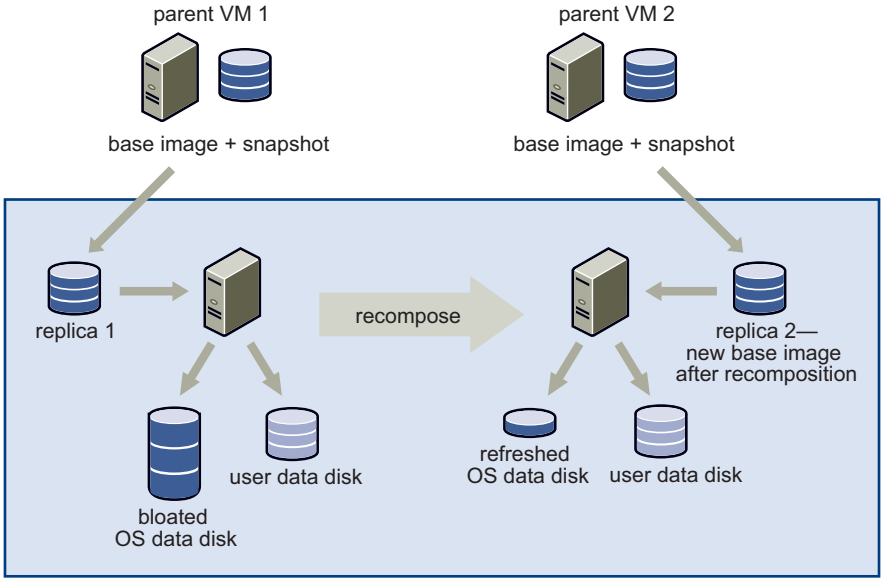
Storage overcommit levels can be varied between different types of datatstores in order to address the different levels of throughput on each datastore (for example, NAS versus SAN). Where throughput is relatively slow, the overcommit level can be set to a lower level to ensure that a smaller number of clones are created on the datastore. Conversely, a higher level of overcommit could be applied to datastores that exhibit a greater rate of data transfer.

Storage overcommit only applies to delta disks. It does not apply to user disks or standard (non linked) clones where thin disks are used.

Desktop Recomposition

In Figure 6-2 an assigned desktop clone is linked to replica 1, which itself is a copy of Parent VM 1. A recomposition action is initiated when the administrator selects a different snapshot in the same Parent VM or different Parent VM (as in this example). In either case a new replica is provisioned.

Figure 6-2. Desktop Recomposition



Replica 2 is an exact copy of Parent VM 2. When the recomposition action is complete the desktop will be anchored to replica 2 and the operating system data modified accordingly. The operating system data of a recomposed desktop is reduced in size after recomposition, however the user data is unaffected by this event.

Source Virtual Machine

Recomposition is expedited through the use of an additional protected linked clone desktop in VirtualCenter— called a source virtual machine—that is created alongside the replica when a linked clone desktop pool is first deployed.

NOTE The source virtual machine is located with the replica inside a folder called `VMwareViewComposerReplicaFolder` in VirtualCenter.

When a recomposition event takes place, the source virtual machine is the first desktop to be recomposed against a new snapshot. View Composer removes the existing linked clone desktop pool from VirtualCenter and then copies the source virtual machine as many times as necessary in order to replace it.

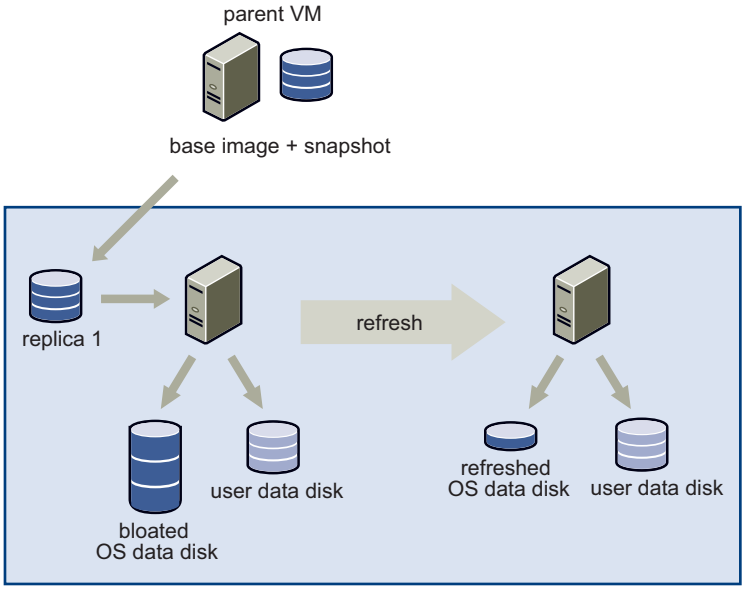
This method of pool generation optimizes the recomposition process and is typically much faster than individually recomposing each linked clone desktop in the pool.

Desktop Refresh

A desktop refresh is similar to a desktop recomposition but without any change to the base image. This action is carried out in order to restore the system data for a desktop pool to a baseline state and thereby reduce the size of the operating system data of each attached clone.

A desktop refresh can be carried out either on demand, as a timed event, or when the operating system data reaches a specified size. Figure 6-3 illustrates the effect of this action—note that the user data disk remains unaffected by this event.

Figure 6-3. Desktops Refresh



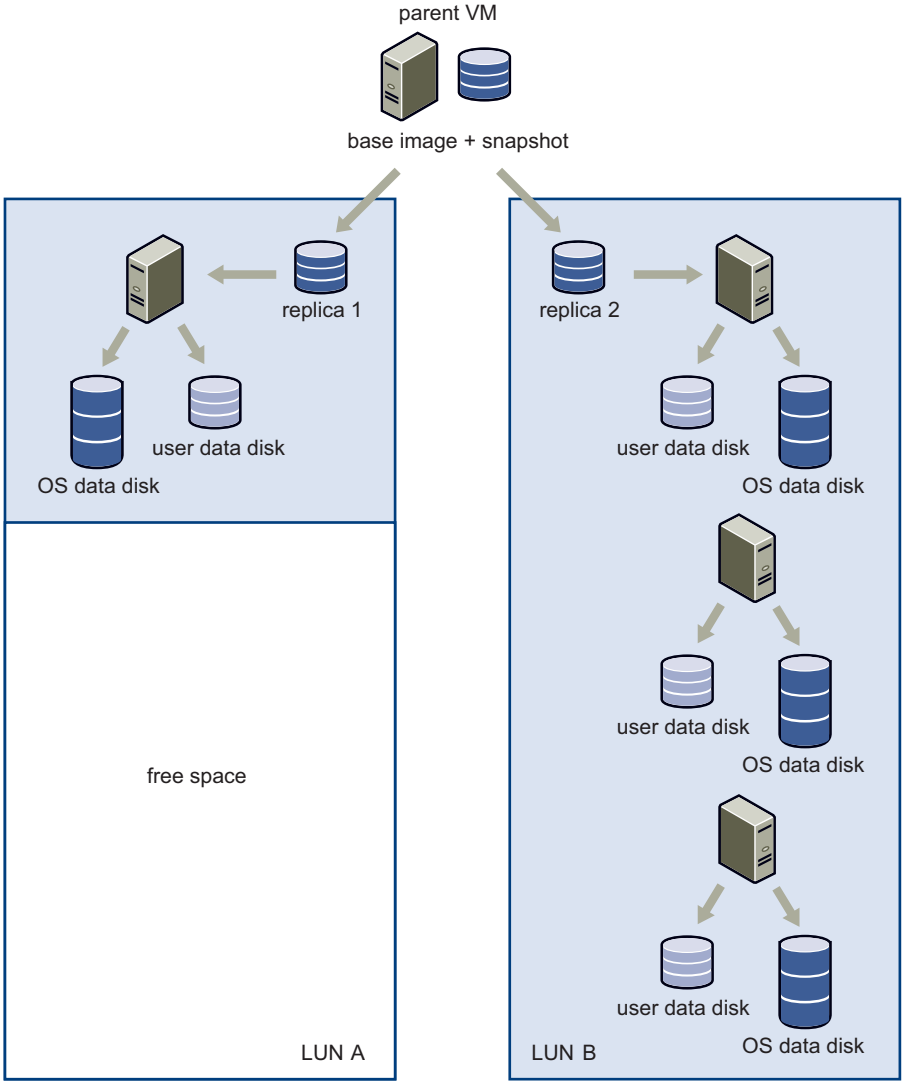
It is important to occasionally refresh the attached systems in order to prevent the desktop clones growing to the size of a full virtual machine. If all the anchored virtual machines are left to grow unchecked then all free space remaining on the datastore could be rapidly consumed—particularly if the storage overcommit level is particularly aggressive.

Desktop Rebalance

A logical drive is a structure created on a subsystem for data storage that is defined over a set of drives called an array. Logical drives—often referred to as LUNs, which stands for Logical Unit Number and represents the identifier a host uses to access the logical drive—are the logical segmentation of arrays.

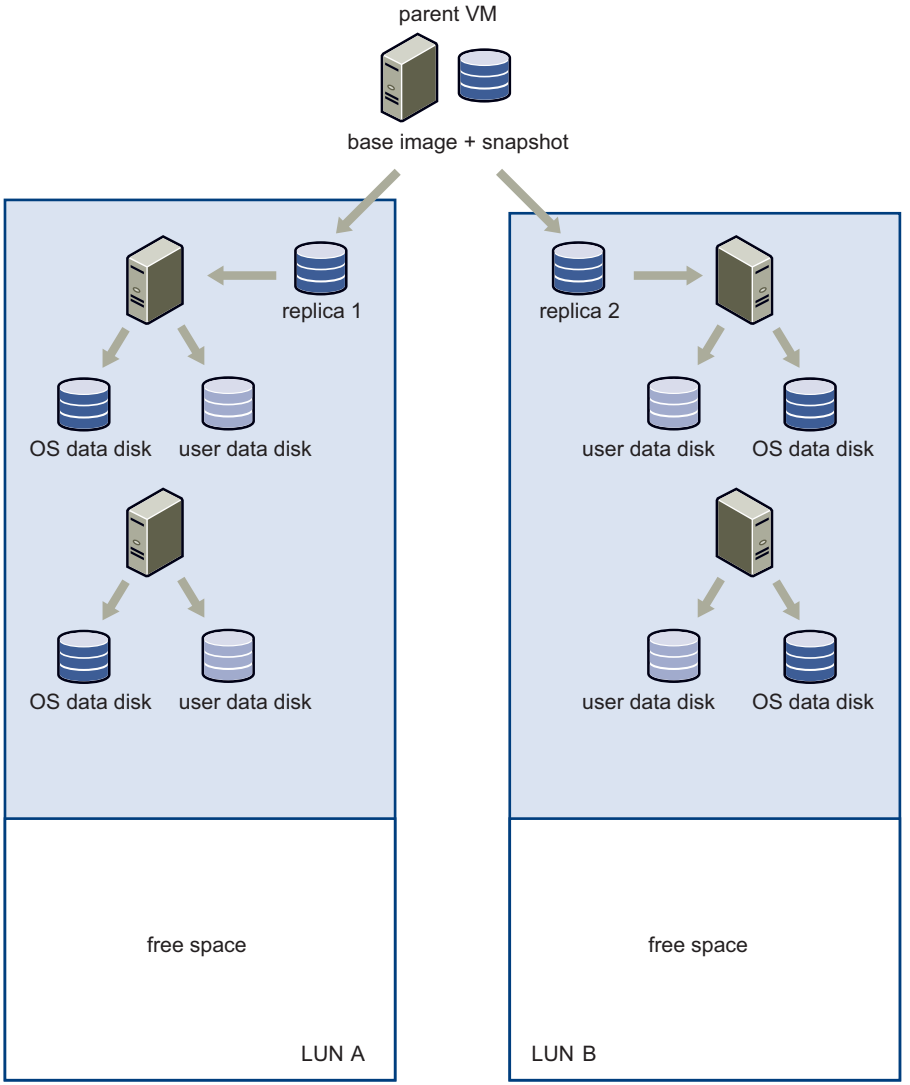
If administrators are creating large pools of desktops and are using multiple LUNs, there is a possibility that the space is not being used efficiently if the initial sizing was inaccurate. Figure 6-4 shows a number of virtual desktops, distributed unevenly over two LUNs.

Figure 6-4. Desktop Rebalance – Before



Rebalancing the LUNs evenly distributes any selected (or all) virtual machines between the available logical drives. This result of this action is illustrated in Figure 6-5.

Figure 6-5. Desktop Rebalance – After



A high level of storage overcommit introduces the possibility of virtual machines growing to such a level that all free space within the datastore is consumed. When the volume of space being used by the virtual machines on the datastore reaches:

- 95%—A log entry is generated that states the datastore is short on free space.
- 99%—Every virtual machine resident within the datastore is suspended.

The rebalance feature offers administrators a graceful mechanism for introducing additional storage to a datastore in order to prevent the latter outcome. In addition, prior to executing the rebalance action you may also retire old storage and make resource pool alterations, and host changes.

Only desktops in the Ready, Error, or Customizing state with no schedules or pending cancellations can be rebalanced. In addition, you cannot rebalance the load between the local storage systems on multiple standalone ESX servers.

It is recommended to keep linked clone desktop virtual machines on a datastore with no other type of virtual machine so that the rebalance action is applied to all the virtual machines.

NOTE In order to rebalance the desktops it is necessary for View Manager to automatically refresh their operating systems against their current base image and return the system data to its baseline state—user data is unaffected if it resides on a separate user data disk.

Persistent and Non-Persistent Desktops

Both persistent and non-persistent desktop configurations are supported by View Composer. In persistent configurations, dedicated disks—a system disk for operating system data and a user disk for user data—can be used to keep the operating system and user data separate. This ensures that even if the operating system is recomposed or refreshed the user data remains unaffected.

In non-persistent configurations the user data is transient so both the operating system data and the user data is stored on the system disk. In this configuration user data is not protected if the system is recomposed or refreshed.

NOTE Persistent desktops can be set to refresh automatically when the user logs off. This can help minimize the space requirements of the pool. Similarly, non-persistent pools can be set to delete after first use, which reduces the number of inactive desktops in the pool overall.

QuickPrep

QuickPrep is a system tool executed by View Composer during a linked clone desktop deployment that is responsible for personalizing each desktop created from the Parent VM. During the initial startup of each new desktop, QuickPrep ensures that the system is given a new name (specified during the deployment process) and joined to the appropriate domain, and for mounting the new volume that will contain the user profile information. In addition, a new computer account corresponding to each desktop is created by QuickPrep on the Active Directory domain controller. These events also take place after a desktop refresh.

After a desktop is created or after a refresh, a user-defined customization script can be optionally applied to each resynchronized desktop in order to carry out additional operations. A script can also be applied to desktops immediately prior to them being powered off. QuickPrep is responsible for ensuring that these scripts are read and executed during either scenario.

You are presented with the opportunity to provide the path to each type of script (which must reside on the Parent VM) during the final stage of the initial linked clone desktop deployment.

Preparing VirtualCenter for View Composer

Before carrying out a linked clone desktop deployment you must configure the VirtualCenter host system in order to prepare it for creating replicas and linked clone desktops from a Parent VM using the View Composer service.

- The view composer service must be installed locally on the VirtualCenter server.
- Your Active Directory administrator must create a user with the requisite level of authority to be used by the View Composer service to create linked clone desktops and add them to your domain.
- If the VirtualCenter user used by View Manager is not an administrator, you must extend their role to incorporate VirtualCenter privileges required by the View Composer Service.
- If an available resource pool does not already exist within VirtualCenter, you must create one on the ESX host or cluster in which you want to store the linked clone desktops. Refer to the VirtualCenter documentation on how to do this.
- If one does not already exist within your network environment, a database and data source name (DSN) must be created in order to store linked clone desktops.

Adding the View Composer Service to VirtualCenter

View Composer is used by View Manager to create and deploy linked clone desktops from VirtualCenter. During the installation of the service you are offered the opportunity to specify which port the service should use to communicate with View Connection Server. If Windows firewall is running on the VirtualCenter system you must add this port to the exception list or deactivate the local firewall service.

The following procedure describes how to install the View Composer service on the VirtualCenter server, and configure it to use a datasource that is dedicated to the storage of linked clones.

Install the View Composer Service

1 Run the View Composer service installation program, where `xxx` is the build number of the executable file:

`VMware-viewcomposer-xxx.exe`

2 Accept the VMware license terms and click **Next**.

3 Accept or change the destination folder path and click **Next**.

4 In the Datasource Name field enter the name you provided in the Microsoft ODBC Data Source Administrator wizard for your database (in the previous example, `VMware Linked Clone`).

5 Enter a domain administrator username and password in the fields provided and click **Next**.

6 Select the **Create a new RSA key container** radio button. An RSA key pair is created in order to encrypt and decrypt the Active Directory authentication information that will be stored inside the linked clone desktop database. Click **Next**.

7 Enter a port value or use the default and select the **Create default SSL certificate** radio button. Click **Next**.

8 Click **Install** to begin the installation process. On the process is complete click **Finish**.

Domain User for View Composer

View Composer requires the credentials of domain user account with the requisite level of domain administration authority to add systems to a domain. While you may use an existing domain administrator account for this role, it is strongly recommended that your Active Directory administrator creates a user account specifically for this purpose.

VirtualCenter User Permissions

If the View Manager user is not an administrator in VirtualCenter you must assign a role to the VirtualCenter user entry in order to confer upon it the appropriate level of authority over the objects it creates and manages.

In addition to the standard privileges described in "VirtualCenter Permissions for View Manager Users" on page 36, the View Composer service requires that you enable some additional privileges, described in Table 6-1.

Table 6-1. Create View Composer Role: Required Privileges

Privilege Group	Privilege(s) to Enable
Folder	Create Folder
Datastore	Browse Datastore File Management
Virtual Machine	Inventory Configuration State Provisioning > Clone Provisioning > Allow Disk Access
Resource	Assign Virtual Machine To Resource Pool
Global	Enable Methods Disable Methods

NOTE Administrative users in VirtualCenter have all the requisite permissions enabled by default.

Local System Administrator

View Composer requires that the VirtualCenter user is also a system administrator on the machine hosting the service (the VirtualCenter server). To address this requirement, any VirtualCenter user used by View Manager to deploy linked clone desktops must be a member of the local system `Administrators` group on the VirtualCenter server.

Creating a Database and DSN for Linked Clone Desktops

The following instructions describe how to add a new linked clone desktop database to an existing SQL server instance and make this datasource visible to all other components running on the host system. If a linked clone desktop database already exists in your environment, refer to "Using an Existing Linked Clone Desktop Database" on page 120 for supplementary information on how to use this datasource.

NOTE If a SQL server does not reside on the VirtualCenter host system or elsewhere within your environment you must install one as the View Composer service installer does not include a database.

These instructions assume that Microsoft SQL Server 2005 is installed locally on the VirtualCenter host, and that SQL Server Management Studio Express will be used to create and administer the datasource. If the database resides on the same system as VirtualCenter you can use the Integrated Windows Authentication security model; you cannot use this method of authentication if the database resides on a remote system.

SQL Server Management Studio Express is available from:

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

Add a linked clone desktop database instance to SQL Server 2005

1 On the VirtualCenter server host system select **Start** > **All Programs** > **Microsoft SQL Server 2005** > **SQL Server Management Studio Express** and connect to the existing SQL Server instance for Virtual Infrastructure Management.

2 In the Object Explorer pane, right-click the **Databases** entry and select **New Database...** You are presented with the **New Database** dialog.

3 Enter a name (for example `linkedClone`) in the **Database name** field and click **OK**. Your database is added under the **Databases** entry in the Object Explorer.

4 Exit Microsoft SQL Server Management Studio Express.

Add an ODBC datasource

1 Select **Start** > **Administrative Tools** > **Data Source (ODBC)**. The Microsoft ODBC Data Source Administrator wizard is displayed.

2 Select the **System DSN** tab.

3 Click **Add** and select **SQL Native Client** from the list. The Create a New Data Source to SQL setup wizard is displayed.

4 In the appropriate fields, enter a name (for example, `VMware Linked Clone`) and a brief description of the linked clone desktop database.

5 In the **Server** field, enter the server details in the form **<hostname>\<database name>**, where **<hostname>** is the name of the host system and **<database>** is the SQL Server instance. For example:

```
VCHOST1\SQLEXP_VIM
```

Click **Next**.

6 Ensure that the **Connect to SQL Server to obtain default settings for the additional configuration options** checkbox is selected and select one of the following options:

- If you are using local SQL Server, select **Windows NT authentication**. It is also known as "trusted authentication" and is supported only if the SQL Server is running on the same system as the VirtualCenter Server.
- If you are using remote SQL Server, select **SQL Server authentication**. Windows NT authentication is not supported on remote SQL servers.

Click **Next**

7 Enable the **Change the default database to** checkbox and select the name of the database you have created for the linked clone desktops from the associated list (in this example, `linkedClone`). Click **Next**.

8 Click **Finish** > **OK**.

9 Click **OK** to close the Microsoft ODBC Data Source Administrator dialog.

Preparing a Parent VM

The Parent VM is used by linked clone desktops as the base image for each linked desktop clone. For a Parent VM to be used by View Manager in a linked clone desktop deployment, you must first install the View Agent on its operating system.

Make sure that you have administrative rights to the Parent VM and that the following prerequisites are in place. Ensure that the Parent VM:

- Is joined to the Active Directory domain in which you want linked clone desktops to reside.
- Networking settings (proxies, and so forth) are properly configured.
- Uses DHCP in order to acquire its IP address.
- System disk is be attached to the SCSI (0:0) Virtual Device Node. This property can be configured from within VirtualCenter.
- Operating system power settings are set to remain on at all times.

- System disk contains a single volume (multiple virtual disks are supported).

CAUTION Do not attempt to deploy clones from a Parent VM that contains more than one volume as the result of disk partitioning. Multiple partitions are not supported by the View Composer service.

- The View Agent service is installed and is running.

  NOTE For automated updating of View Agent in large environments, VMware recommends using standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software.

If you have not already done so, install the latest operating system and application service packs and patches on the Parent VM.

DHCP Lease Removal

It is recommended that you release any DHCP information that may exist on the Parent VM so that a leased IP address is not replicated amongst the linked clones in the pool. You can release a DHCP lease by opening a command prompt on the Parent VM and entering the following:

```
ipconfig /release
```

Installing the View Agent on the Parent VM

If it is not already present, you must install the View Agent on the Parent VM in order to allow the View Connection Server to communicate with the desktop clones created from the base image.

To install View Agent

1 Run the View Agent installation program, where `xxx` is the build number of the executable file:

  ```
  VMware-viewagent-xxx.exe
  ```

  The installation wizard opens. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Choose your custom setup options. You must install the **View Manager Composer Agent**, however you may also select or deselect the following features:

- Install the **View Secure Authentication** component if you want to install the Graphical Identification and Authentication (GINA) dynamic-link library. Installing this component enables single sign on (SSO) so that when a user logs into View Client they are not additionally prompted to re-enter their authentication information in order to log in to their desktop.
- Install the **USB Redirection** component if virtual desktop users need to access locally connected USB devices with their virtual desktops.

  NOTE Windows 2000 does not support USB redirection.

- Install the **Virtual Printing** component if you want to enable users to print to any printer available to their client system without first installing additional drivers on their desktop. Refer to "Virtual Printing" on page 90 for more information about this feature.

4 Accept or change the destination folder and click **Next**.

5 Click **Install** to begin the installation process. On the process is complete click **Finish**.

Creating a Parent VM Snapshot

Once View Agent has been installed on the base image you must use VirtualCenter to take a snapshot of the system in its powered-down state. This snapshot will be used as the baseline configuration for the first set of linked clone desktops anchored to the Parent VM.

NOTE The Parent VM must be completely shut down before you take the snapshot.

Deploying Linked Clone Desktops from View Manager

View Manager can only deploy linked clone desktops if it is able to communicate with a properly configured VirtualCenter host that is running the View Composer service. In addition, your Active Directory forest must have a fully qualified domain name, for example, `example.com`—you cannot use View Composer in environments where the domain controller has an unqualified name.

Before you attempt to create a new linked clone desktop pool you must first ensure that View Manager is able to contact VirtualCenter and that the View Composer service has started. Once a connection has been established you will be able to deploy a new linked clone desktop pool.

CAUTION Do not modify the Parent VM (for example, convert it to a template) from within VirtualCenter before or during the deployment process—the View Composer service has a requirement that the Parent VM remains in a static and unaltered state during this operation.

To add or edit a VirtualCenter server entry in View Manager

1 From within the View Administrator, click **Configuration** to display the configuration view.

2 Under VirtualCenter Servers, if you have not already done so click **Add** and complete the details for the VirtualCenter to use with View Manager:

a Enter the FQDN or IP address of the VMware VirtualCenter server you want View Manager to communicate with in the **Server address** text box.

CAUTION If you enter a server using a DNS name or URL, no DNS lookup is performed to verify whether or not the server has previously been entered using its IP address. A conflict will arise if a VirtualCenter server is added with both its DNS name and its IP address.

b Enter the username of a VirtualCenter user in the **User name** text box.

c Enter the password that corresponds to the user entered above in the **Password** text box.

d (Optional) Enter a description for this VirtualCenter server in the **Description** text box.

e If you will be connecting to the VirtualCenter through a secure channel (SSL) then make sure the Connect using SSL checkbox is checked. This is the default setting.

f Enter the TCP port number in the Port text box. The default is 443.

If the required VirtualCenter server is already present, select the entry and click **Edit**. The VirtualCenter settings list is displayed.

3 Ensure that the **Enable View Composer** check box is selected and that the port number corresponds to the port specified during the installation of the View Composer service on the VirtualCenter host.

4 Click **Add** and enter the required details into the **Add Domain Administrators** window.

NOTE This is where you enter the credentials of the user—created by your Active Directory administrator—who can add systems to the domain, as described in "Preparing VirtualCenter for View Composer" on page 102.

Enter the VirtualCenter user information in the form `domain\username`, where `domain` is the fully qualified domain name of the Active Directory domain. For example: `example.com\admin`

5 Click **Add** > **OK**.

6 The View Composer user is added to the **Domain administrator accounts** list. Click **OK** to close the VirtualCenter settings window.

To configure and deploy a new linked clone desktop pool

1 From within the View Administrator, click the **Desktops** button and then click the **Inventory** tab. In the **Desktops** pane, ensure that the **Desktops** tab is selected and click **Add**.

2 You are presented with the Add Desktop wizard. From here you can configure and deploy a new linked clone desktop pool. Select **Automated Desktop Pool** and click **Next**.

3 Select the type of desktop pool you want to create and click **Next**.

Pool Type	Description
Persistent	Desktops in this type of pool are allocated statically in order to ensure that users connect to the same desktop each time they log in.
Non-persistent	Desktops in this type of pool are allocated dynamically when the user logs in, and are returned to the pool when the user disconnects.

4 Select the VirtualCenter server that will be used by this desktop, and ensure that the **Use linked clone technology to create desktops in this pool** checkbox is selected. Click **Next**.

5 Enter the **Desktop ID** and, optionally, the **Desktop Display Name** and **Description**.

The desktop ID is used by View Manager to identify the desktop pool and is the name that the user sees when logging in. The desktop ID and display name can be arbitrary but if you do not specify a display name the desktop ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters and is only visible from within View Administrator.

Once you have provided the desktop identification details, click **Next**.

6 Configure the desktop properties and click **Next**.

CAUTION If you are using Windows Vista as your Parent VM, you *must* set the power policy to **Ensure VM is always powered on**.

Property	Parameter Description
Desktop state	**Enabled**—after being created, the desktop pool is automatically enabled and ready for immediate use. **Disabled**—after being created, the desktop pool is disabled and unavailable for use. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
Virtual machine power policy	**Do nothing (VM remains on)**—Virtual machines that are powered off will be started when required and will remain on, even when not in use, until they are shut down. **Ensure VM is always powered on**—All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart. **Suspend**—All virtual machines in the pool enter a suspended state when not in use. **Power off**—All virtual machines in the pool shut down when not in use.
Automatic logoff after disconnect	**Immediately**—users are logged off as soon as they disconnect. **Never**—users are never logged off. **After**—the time after which users are logged off when they disconnect. Enter the duration in minutes in the field provided.

Property	Parameter Description
Refresh OS disk on logoff (persistent pools only)	**Never**—the base operating system image is never refreshed. **Always**—the base operating system image is refreshed every time the user logs off. **Every**—the base operating system image is refreshed on a recurring basis at a specified time. Enter a positive number of days in the field provided. **At**—the base operating system image is refreshed when the size of the operating system data reaches a certain level on the datastore. Enter a percentage value in the field provided.
Power off and delete virtual machine after first use (non-persistent pools only)	Select this check box if you want the virtual machine to be deleted immediately after the user logs off. If necessary, a new virtual machine is cloned to maintain a specific pool size after virtual machines are deleted.
Allow users to reset their desktop	Select this check box if you want to allow desktop users to be able reset their own desktops without administrative assistance.
Allow multiple sessions per user (non-persistent pools only)	Select this check box if you want to allow individual users to simultaneously connect to multiple desktops in the same pool.

7 Configure the desktop provisioning properties and click **Next**. The parameters for each property are described are described in Table 6-2.

Table 6-2. Add Desktop: Desktop Provisioning Settings

Property	Parameter Description
Provisioning	**Enabled**—the desktops in the pool will be immediately created upon completion of the deployment procedure or after a desktop is deleted. **Disabled**—the desktops in the pool will not be immediately created upon completion of the deployment procedure or after a desktop is deleted.
Number of desktops	Specifies the number of desktops to create in this pool. This setting is disabled if you select the **Enable Advanced Pool Settings** check box in the **Advanced Settings** panel.

Table 6-2. Add Desktop: Desktop Provisioning Settings (Continued)

Property	Parameter Description

VM naming pattern	By default, a prefix is used to identify all desktops in a pool as part of the same group. The prefix can be up to 13 characters in length and a numeric suffix is appended to this entry in order to distinguish each desktop from others in the same pool.
	You can override this behavior by entering a name that contains a token representing the pool number; the token can appear anywhere in the name. For example:
	`amber-{n}-desktop`
	After deployment`{n}` is replaced with the pool number of the desktop.
	Fixed length tokens can be entered using the `n:fixed=` construction. For example:
	`amber-{n:fixed=3}`
	After deployment`{n:fixed=3}` is replaced with a fixed-length pool number for each the desktop: `amber-001`, `amber-002`, `amber-003` and so forth.
	A 15 character limit applies to names that contain a token, but only to the "replaced" form where the token length is fixed. For example:
	`my-view-system{n:fixed=1}`
	Where the token length is not fixed, a buffer of 1 is applied to the token, so the maximum "replaced" length is 14 characters. For example:
	`a-view-system{n}`

Stop provisioning on error	Select this check box if you want View Manager to automatically stop provisioning new virtual machines if an error is detected during desktop creation.
Advanced Settings	Click to display the advanced pool configuration settings. You can enable the advanced parameters by selecting the **Enable Advanced Pool Settings** check box. This will disable the **Pool Size** parameter. **Minimum number of virtual machines**—the minimum number of desktops that must be provisioned for this pool. **Maximum number of virtual machines**—the maximum number of desktops that can be provisioned for this pool. **Number of available virtual machines**—The number of virtual machines that must be unassigned and available for use at any given time. This figure cannot exceed the maximum number of desktops available to the pool overall.

8 Select the Parent VM to be used as the base image for the deployment. You are only be presented with virtual machines that contain one or more snapshots that were taken when the virtual machine was powered down. Click **Next**.

9 Select the snapshot you previously created on the Parent VM while in its inactive state and click **Next**.

10 Select where you want the folder for this desktop pool to reside within VirtualCenter and click **Next**.

11 Select a host or a cluster on which to run the virtual machines used by this desktop and click **Next**.

NOTE Only clusters of 8 hosts or fewer are supported and shown.

12 Select a resource pool in which to run the virtual machines used by this desktop and click **Next**.

13 (Optional) This step applies to persistent pools only and determines how user data should be stored by desktops within this pool.

- If you want user data to be preserved after a refresh or recomposition event select **Redirect user profile to a separate disk**, and specify the maximum size of the user data disk and associated drive letter.

CAUTION Do not select a letter that corresponds to a drive that is already present on the Parent VM.

- If you do not want user data to be preserved after a refresh, recomposition, or rebalance event select **Store user profile on the same disk as the OS**. User data will be retained until either of these events are performed by the administrator or executed automatically by policy.

Once you have configured the user data storage criteria, click **Next**.

14 Select one or more datastores on which to store the desktop pool. If you do not have sufficient space available, you must add free space by selecting an additional datastore.

NOTE For clusters, only shared datastores are supported; every host in the cluster must be connected to the datastore to be shown.

If you are creating a persistent pool where more than one datastore is available you can click the fields in the **Use For** column and specify how the storage space for the corresponding datastore should be used. By default, both **OS Data** and **User Data** are selected for each datastore.

NOTE You must allocate sufficient space for both the operating system and user data in order to proceed.

The **Storage Overcommit** column entry determines how aggressively the system assigns new virtual machines to the free space available on a datastore. As the level increases, less space will be reserved for individual virtual machine growth but more virtual machines will fit on the datastore. Click the entry to modify the aggression level for each datastore.

NOTE The "Min Recommended", "Storage at 50% provision", and "Storage at 100% provision" values are only provided as guidelines. The actual requirements for the pool will vary based on client usage patterns, application workload, pool type, and so forth.

Once you have configured the datastore storage criteria, click **Next**.

15 In order to join linked clone desktops to a domain, View Manager requires domain administrator credentials for the target domain. Select the desired domain\administrator entry from the **Domain Administrator Account** drop down menu.

Click **Next**.

16 You are presented with a summary of the configuration settings for this deployment.

- If you are unsatisfied with any aspect of the configuration you can use the **Back** button to revisit any previous page.
- If you are satisfied with the configuration click **Finish** to deploy the linked clone desktop pool.

Once the deployment has been initiated you can monitor the progress of the provisioned desktop pool or the individual desktops by selecting either the **Desktops** or **Desktop Sources** tabs in the Desktops pane.

Once the process is complete you can entitle users or groups to use the desktop pool by carrying out the procedure described in "Entitling a Desktop or Pool" on page 65.

Refreshing, Recomposing, and Rebalancing Linked Clone Desktops

You can only recompose, refresh, or rebalance linked clone desktops that are part of a persistent pool. If you want to change the Parent VM of a non-persistent linked clone desktop pool you must modify the pool directly by using the pool deployment wizard. The deployment wizard can be invoked by clicking **Edit** on the summary page for the non-persistent pool.

If you want to make changes to the datastore profile (add or remove a storage, or modify the pool configuration) before rebalancing, you must first use the Edit Desktop wizard to reconfigure the pool.

NOTE Rebalancing will automatically initiate a refresh of the target desktop or desktops. In addition, only desktops in the Ready, Error, or Customizing state with no schedules or pending cancellations can be rebalanced.

CAUTION Do not modify the Parent VM (for example, convert it to a template) from within VirtualCenter before or during any of the procedures described in this section.

To refresh a linked clone desktop pool

1 From within the View Administrator, click **Desktops and Pools** to display the desktop page.

2 Ensure that the **Inventory** tab is selected in the left-hand pane and select the persistent desktop pool you want to refresh.

3 Select one of the following options:

- To refresh the entire desktop pool, ensure that the **Summary** tab is selected in the right-hand pane.
- To refresh the desktops assigned to specific users in the desktop pool, ensure that the **Users and Groups** tab is selected in the right-hand pane.

  If you want to refresh the desktop of one or more assigned users, select the corresponding check boxes. You do not need to do this if you want to refresh the desktops of all assigned users.
- To refresh specific desktop sources in the pool, ensure that the **Desktop Sources** tab is selected in the right-hand pane, select.

  If you want to refresh multiple desktops, select the corresponding check boxes. You do not need to do this if you want to refresh all the desktops in the pool.

4 Click **Edit Image**. You are presented with the Edit Image wizard. Select the **Refresh** option and click **Next**.

5 If you selected the **Users and Groups** tab you can now filter your user selection. Select **All users** if you want to execute a global refresh against all assigned users in the desktop pool. If you selected one or more users you can select **The following users** if you want the refresh to apply only to specific users within the selected group.

If you selected the **Summary** or **Desktop Sources** tab you can now filter your desktop source selection. Select **All virtual machines** if you want to execute a global refresh against all desktops in the pool. If you specified one or more individual assigned desktops you can select **The following virtual machines** if you want the refresh to apply only to specific systems within the selected group.

Click **Next**.

6 Schedule when you want the refresh event to take place (the default is set to the current time, and therefore immediately).

- If you want any currently connected users to be logged off as soon as the refresh event starts, select **Force Users to log off**.

NOTE If you select this option, connected users will be notified prior to disconnection and given the opportunity to close their applications and log out. The notification message can be accessed from within the **Global Settings** section of the configuration page.

- If you want the system to wait until a user has disconnected before initiating a refresh of their desktop, select **Wait for users to log off**.

7 Click **Finish** to start the refresh.

To recompose a linked clone desktop pool

1 From within the View Administrator, click **Desktops and Pools** to display the desktop page.

2 Ensure that the **Inventory** tab is selected in the left-hand pane and select the desktop pool you want to recompose.

3 Select one of the following options:

- To recompose the entire desktop pool, ensure that the **Summary** tab is selected in the right-hand pane.
- To recompose the desktops assigned to specific users in the desktop pool, ensure that the **Users and Groups** tab is selected in the right-hand pane.

  If you want to recompose the desktop of one or more assigned users, select the corresponding check boxes. You do not need to do this if you want to recompose the desktops of all assigned users.
- To recompose specific desktop sources in the pool, ensure that the **Desktop Sources** tab is selected in the right-hand pane, select.

  If you want to recompose multiple desktops, select the corresponding check boxes. You do not need to do this if you want to recompose all the desktops in the pool.

4 If you want to recompose the desktop of one or more assigned users, select the corresponding check box. You do not need to do this if you want to recompose the desktops of all assigned users.

5 Click **Edit Image**. You are presented with the Edit Image wizard. Select the **Recompose** option and click **Next**.

6 If you selected the **Users and Groups** tab you can now filter your user selection. Select **All users** if you want to execute a global recomposition against all assigned users in the desktop pool. If you selected one or more users you can select **The following users** if you want the recomposition to apply only to specific users within the selected group.

If you selected the **Summary** or **Desktop Sources** tab you can now filter your desktop source selection. Select **All virtual machines** if you want to execute a global recomposition against all desktops in the pool. If you specified one or more individual assigned desktops you can select **The following virtual machines** if you want the recomposition to apply only to specific systems within the selected group.

7 Click **Next**.

8 Edit the base image used by the selected desktop pool.

- If you want to anchor the clones in the desktop pool to a different snapshot within the same base image, select a new snapshot from the list provided.
- If you want to change the current base image to that of a new Parent VM, click **Change** and select a new virtual machine to be the Master VM for the pool from those highlighted in the list. Click **OK**.

Click **Next**.

9 Schedule when you want the recomposition event to take place (the default is set to the current time, and therefore immediately).

- If you want any currently connected users to be logged off as soon as the recompose event starts, select **Force Users to log off**.

NOTE If you select this option, connected users will be notified prior to disconnection and given the opportunity to close their applications and log out. The notification message can be accessed from within the **Global Settings** section of the configuration page.

- If you want the system to wait until a user has disconnected before initiating a recomposition of their desktop, select **Wait for users to log off**.

10 Click **Finish** to start the recomposition.

To rebalance a linked clone desktop pool

1 From within View Administrator, click **Desktops and Pools** to display the desktop page.

2 Ensure that the **Inventory** tab is selected in the left-hand pane and select the desktop pool you want to rebalance.

3 In the right-hand pane, select the **Desktop Sources** tab.

4 Select one or more desktops from the desktop source list provided. You do not have to select any desktops if you intend to rebalance the entire pool.

5 Click **Rebalance**. You are presented with the Rebalance wizard, which provides you with important information about what will happen when you rebalance one ore more desktops in the pool. Once you have read this information and are satisfied that you want to proceed click **Next**.

6 If you previously selected one or more virtual machines from the desktop source list you can choose to rebalance only these systems by selecting the corresponding radio button. If you did not select any virtual machines, or want to rebalance the entire pool, select **All virtual machines**. Click **Next**.

7 Schedule when you want the rebalance event to take place (the default is set to the current time, and therefore immediately):

- If you want any currently connected users to be logged off as soon as the rebalance event starts, select **Force Users to log off**.

  NOTE If you select this option, connected users will be notified prior to disconnection and given the opportunity to close their applications and log out. The notification message can be accessed from within the **Global Settings** section of the configuration view in View Administrator.

- If you want the system to wait until a user has disconnected before initiating a rebalancing of their desktop, select **Wait for users to log off**.

8 Click **Finish** to start the recomposition.

Using an Existing Linked Clone Desktop Database

When selecting the ODBC datasource during the installation of the View Composer service you can use an existing database that already contains linked clone desktop data. However, in order to make this datasource compatible with a new instance of the View Composer service you must first transfer the RSA key container created by the original View Composer service to the new host system.

NOTE RSA key pairs are created by the View Composer service in order to encrypt and decrypt the sensitive authentication information that is stored inside the View Composer database.

The ASP.NET IIS registration tool provided with the Microsoft .NET Framework allows you to conduct multiple configuration operations, including migrating key container content between different systems.

To carry out the following procedure you must have the .NET Framework installed on the system that contains (or previously contained) the instance of View Composer that was associated with the database you want to use. You must also install the .NET framework on the system on which you want to install the new instance.

You can download the .NET Framework and view additional information about the ASP.NET IIS registration tool from the following locations:

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

The following procedure must be carried out before installing the View Composer service on the new system.

To migrate an RSA key container between systems

1 Export the RSA keys associated with the earlier instance of the View Composer from their local key container by entering the following from a command prompt on the source system:

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

The RSA public-private key pair is exported from the `SviKeyContainer` container to a file called `keys.xml` that is saved locally to the ASP.NET IIS registration tool.

2 Copy the `keys.xml` file to the system on which you want to install a new instance of the View Composer service.

3 Import the key pair data into the local key container by entering the following from the command prompt on the target system, where `<path>` is the path to the exported file:

```
aspnet_regiis –pi "SviKeyContainer" "<path>\keys.xml"
```

4 Install the View Composer service using the procedure described in "Adding the View Composer Service to VirtualCenter" on page 103 and provide the required information about the existing datasource, but select **Use the existing RSA key container** when prompted.

7 Offline Desktop

Offline Desktop offers mobile users the ability to check out a cloned instance of certain types of View Manager desktop onto a local system such as a laptop. Once checked out, the local copy behaves like a standalone desktop system and can be used with or without a network connection; the desktop is now considered to be "offline."

The following sections provide an overview of Offline Desktop, its purpose and implementation.

NOTE Offline Desktop is an experimental feature. Please refer to "System Requirements" on page 14 for more information about experimental features.

This chapter discusses the following topics:

NOTE For information about usage policies that relate specifically to offline client sessions, refer to "Client Policies" on page 139.

Overview of Offline Desktop

Offline Desktop addresses the challenge of continuous access that is implicit in any online desktop solution: through circumstance or choice, users occasionally find themselves in environments where network availability is extremely limited or completely absent.

In anticipation of this, an Offline Desktop user can use the View Client with Offline Desktop application to download a copy of their desktop virtual machine from the View Connection Server for use on a local computer—an event that also "locks" the online desktop virtual machine, preventing it from being accessed from any other location.

NOTE While a lock is in place, VirtualCenter operations such as powering on the online desktop, taking snapshots, editing the virtual machine settings and so forth are disabled.

Once downloaded, Offline desktops behave in the same way as their online equivalents yet can take advantage of local resources; latency is minimized and performance is enhanced. The presence of a downloaded virtual machine has no effect on the existing operating system of the client system, which users can continue to utilize if they wish.

A consistent user experience is ensured through use of View Client with Offline Desktop for both online and offline sessions. In addition, users can disconnect from their offline desktop and then log in again without connecting to the View Connection Server. Once network access is restored (or when the user is ready) the checked out virtual machine can be:

- Backed up—the online system is updated with all new data and configurations, but the offline desktop remains checked out on the local system and the online lock remains in place.

- Rolled back—the offline desktop is discarded and the online lock is released. Future client connections will be directed to the online system until the desktop is checked out again

- Checked in—the offline desktop is uploaded to the online host and the online lock released. Future client connections will be directed to the online system until the desktop is checked out again.

NOTE Users cannot access their offline desktop while the above actions are taking place.

The ability of users to download an online desktop for use on their local system is conferred through entitlement and Offline Desktop access policy. While a desktop is checked out, View Manager administrators are still able to access the online system while monitoring the offline equivalent.

The flow of a typical online and offline usage scenario is illustrated in Figure 7-1, with each stage summarized in Table 7-1.

Figure 7-1. Offline Desktop – Usage Flow

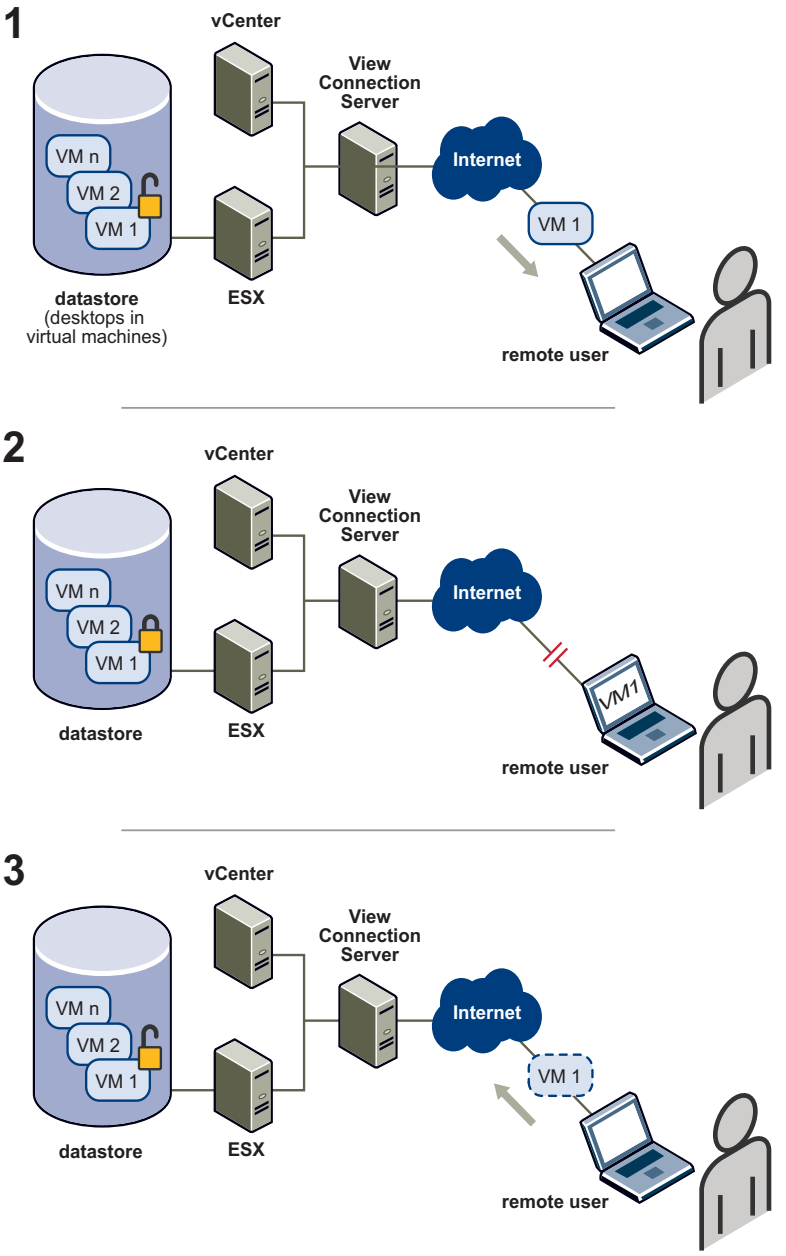


Table 7-1. Offline Desktop – Stage Description

Stage	Description
1	The remote user starts View Client with Offline Desktop and is presented with a list of their entitled desktops. The user selects an Offline Desktop compatible desktop and initiates a download that copies the desktop virtual machine onto their local system.
2	Once the virtual machine is downloaded, the user can log into Windows and use their desktop locally, even in the absence of a network connection. The online equivalent is shut down and locked in order to prevent access or modification. While working offline, users can backup their data to the server at any time.
3	When the user checks the virtual machine back in to the server, the online data is updated and the server lock is released. Subsequent View Client with Offline Desktop connections will be directed to the online desktop until the virtual machine is checked out once more.

Offline Desktop Licensing and VirtualCenter Access

The availability of the Offline Desktop feature is determined by your View Connection Server license type. In order to use the administrative and client components associated with Offline Desktop, your license must include this feature as part of its coverage.

NOTE You can examine your Offline Desktop license status by referring to the License section in the **Configuration** view of View Administrator.

Desktops can only be checked out from VirtualCenter if the VirtualCenter user specified in View Manager is an administrator. Ensure that the VirtualCenter user that has administrative rights before attempting to use Offline Desktop.

NOTE You can examine the VirtualCenter user (or users) currently assigned to View Manager by referring to the VirtualCenter Servers box in the **Configuration** view of View Administrator.

Storage, Communications, and Security

The time taken for an initial desktop check out will be longer than subsequent check in and check out actions as an entire virtual machine clone must first be downloaded onto the client system. Thereafter, incremental changes are communicated between the server and the client as differences between the two systems, and this involves the transfer of a much smaller volume of data.

Once checked out, Offline Desktop uses thin provisioned virtual disks to store information on the host system. This type of disk occupies no more space than that required by the data it contains, and physical disk space is only allocated as data is written; this minimizes the storage footprint of the downloaded system.

If a network connection is present on the client system, the desktop that has been checked out will continue to communicate with View Connection Server in order to obtain usage data, provide policy updates, and ensure that locally cached authentication criteria is current. Contact is attempted every 5 minutes. In the absence of a network connection, the desktop will fall back on locally cached information in order to authenticate the user during login.

The data on each offline system is encrypted and has a lifetime controlled through policy—if the client loses contact with the View Connection Server, the maximum time without server contact is the period in which the user can continue to use the desktop before they are refused access; this countdown is reset once the connection is re-established. Prior to disconnection, the user is notified that the offline desktop lifetime is about to expire.

Similarly, if user access is removed—that is, if entitlement is withdrawn or the account is suspended—the client system becomes inaccessible when the cache expires or after the client is made aware of this change by the View Connection Server (whichever comes first). In this scenario, the user is not notified prior to disconnection.

Tunneled Communications and SSL

Offline Desktop supports tunneled or non-tunneled communications for LAN-based data transfers.

- When tunneling is enabled, all traffic is routed through the View Connection Server.
- When tunneling is not enabled, data transfers take place directly between the online desktop host system and the offline client.

You can disable tunneling by selecting the **Direct connection for Offline Desktop operations** check box in the **Configuration** page of the administrative interface.

In addition to specifying the route for communications, you can encrypt the communications and data transfers that take place between the Offline Desktop client and the View Connection Server by selecting the **Require SSL for Offline Desktop operations** check box in the **Configuration** page of the administrative interface.

NOTE Bypassing the tunnel and using an unencrypted connection increases data transfer speed at the expense of secure data communication. The encryption setting has no effect on the offline data itself, which is always encrypted on the client system.

Offline Desktop Policies

Certain Offline Desktop features can be controlled through policy. For information about configuring and applying policies to offline desktops at the global, pool, or user level refer to "Client Policies" on page 139.

Supported Desktop Types

Not all types of View Manager desktop configuration support Offline Desktop. Table 7-2 provides a matrix that describes the availability of this feature to the different desktop types.

Table 7-2. Offline Desktop – Supported Desktops

Type	Persistence	Desktop Configuration	Offline Desktop
Individual Desktop	Non-Persistent	Virtual machines managed by VirtualCenter	Yes
		Virtual machines not managed by VirtualCenter	No
		Physical systems	
Automated Desktop Pool	Persistent	Non-linked clone	Yes
		Linked clone	No
	Non-Persistent	All	
Manual Desktop Pool	Persistent	Virtual machines managed by VirtualCenter	Yes
		Virtual machines not managed by VirtualCenter	No
		Physical systems	
	Non-Persistent	All	
Microsoft Terminal Services Desktop Pool	N/A	N/A	

Additional Considerations

When using Offline Desktop you must be aware of the following considerations:

- View Client with Offline Desktop cannot be run on a virtual machine.
- View Client with Offline Desktop does not support the use of smart cards.

- You cannot download a desktop to a system where the guest exceeds the capabilities of the host; the host system must be at least as capable as the guest in order to run the View Manager desktop.
- You cannot download a desktop if another user is currently logged in to that desktop.
- ESX supports two simultaneous desktop checkouts. ESXi supports five simultaneous desktop checkouts.
- Host CD-ROM redirection is not supported.
- When a desktop is checked out, NAT is used for network communications. The MAC address of the offline system remains the same as its online equivalent.
- As with RDP, you can copy and paste text between host and guest systems. However, you cannot copy and paste system objects such as folders and files between systems.
- Local drives are automatically mounted on the guest system.
- Once a desktop is checked out on a client system, any changes made within View Administrator to the desktop or desktop pool settings will only be applied after the desktop has been checked in again.

View Client with Offline Desktop

In order to access an offline desktop, users must first download a copy of the online virtual machine to their local system using the View Client with Offline Desktop application. You cannot install View Client with Offline Desktop on any system that has the following applications installed:

- VMware Workstation
- VMware ACE
- VMware Player
- VMware Server

The above applications must be uninstalled prior to installing View Client with Offline Desktop.

NOTE The View Client application provides a subset of the functionality offered by View Client for Offline Desktop; however, many of the administrative tasks and connection considerations are common to both applications, including a number of startup options that can be invoked when launching the application from a command prompt. Refer to Chapter 5, “Client Management,” on page 69 for more information about this.

Before downloading an automated pool desktop for the first time, users must connect to this desktop using any View Manager client. This will ensure that a local profile is created on that desktop that can be used to authenticate offline sessions in environments that have no network availability. It will also ensure that the desktop is correctly associated with the user in View Manager. This step is optional (although recommended) for individual desktops.

NOTE In environments where a network connection is available, the user session will always be authenticated by View Connection Server.

To install View Client with Offline Desktop

1 Run the View Client with Offline Desktop executable on the system that will host the client, where `xxx` is the build number of the file:

```
VMware-viewclientwithoffline-xxx.exe
```

The Installation wizard is displayed. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Choose your custom setup options. You must install the **View Client with Offline Desktop** component, however you may deselect the **USB Redirection** component if virtual desktop users do not need to access locally connected USB devices with their virtual desktops.

Click **Next** to accept the default destination folder or click **Change** to use a different destination folder and then click **Next**.

4 (Optional) Enter the default IP address or FQDN of the server to which the client will connect and click **Next**.

5 Configure shortcuts for the View Client with Offline Desktop and then click **Next > Install > Finish**.

To start View Client with Offline Desktop

1 If View Client does not start automatically after installation, click **Start** > **Programs** > **VMware** > **View Manager Client**.

2 In the **Connection Server** drop-down menu, enter the host name or IP address of a View Connection Server and click **Connect**.

3 Enter the credentials for an entitles user, select the domain and click **Login**.

4 Choose a desktop from the list provided and click **Connect**.

5 View Client with Offline Desktop will attempt to connect to the specified desktop. Upon connection, the client window is displayed.

Users can determine if a desktop is eligible for checkout by right-clicking it in the list provided by View Client with Offline Desktop to display its context menu. If the desktop can be used offline, the **Check out** option is displayed.

NOTE Only the user who checks out the desktop can access it, even if the desktop is entitled to a group.

Checking Out a Desktop

When users check out a desktop for the first time, they are given the opportunity to specify where the downloaded virtual machine should reside on their local system. After the check out begins, the download progress is provided by an on-screen indicator.

NOTE Users can pause or cancel the check in or check out process whenever data is being moved between the online and offline context by right-clicking the entry to display its context menu.

Once the data has been downloaded, user access is directed to the offline desktop until it is checked back in.

NOTE Users cannot use their offline desktop if they manually move the virtual machine data on their system to an alternate location or onto a different system.

Offline Desktop Status

You can examine all current offline sessions at the global or desktop pool level by clicking the **Desktops and Pools** button and then selecting the **Offline Sessions** tab—either for all desktops or for a specific pool—in View Administrator.

This view presents you with a pane that contains a status table for all the offline sessions currently known to the server. The column entries in this table are described in Table 7-3.

Table 7-3. Offline Sessions

Field	Description
User	The Active Directory ID of the user who checked out the desktop—this is in the form **`domain\username`**.
Desktop	The persistent desktop or desktop pool display name (if one was provided when the desktop or pool was created in View Manager).
Status	The current checkout status, which can be one of the following: ■ Checking out—data is being downloaded to the client system, or has been paused during transfer ■ Checked out—an offline desktop exists on the client system and the online equivalent is locked ■ Checking in—data is being uploaded from the client system (either in the form of a backup or as a full check in) or has been paused during transfer
Check-out Time	The time at which the last check out was initiated by the client.
Offline Duration	The overall time of offline usage known to the View Connection Server since the desktop was checked out.
Last Server Contact	The last time View Client with Offline Desktop made contact with View Connection Server. When a connection can be established, the server is contacted every 5 minutes.
Last Backup	The last time the offline desktop was backed up to the View Connection Server. If no backup has yet taken place, the time indicated is the same as **Check-out Time**.

In addition to the above information, you can view the hostname and IP address of a client system and the name of the checked out desktop and its DNS entry or IP address by selecting a desktop from the list and clicking **Details**.

Client Connection

Multiple users may be entitled to use a system, but only the user who initially checks out a desktop can access it locally using the View Client with Offline Desktop application.

If a user connects to the offline desktop in the absence of a network connection, the locally cached user information is used to authenticate the user. Once logged in, if the connection is restored the user must reauthenticate in order to continue to use their desktop; if RSA authentication is enabled, this information will also be required.

Removing Access

In addition to the standard methods of account suspension or removal offered by Active Directory, Offline Desktop sessions can be terminated from within the administrative interface by removing user entitlement from an individual desktop or desktop pool, or by discarding the offline session.

If you remove entitlement from an individual desktop or desktop pool that contains an active checked out session where the View Connection Server is able to communicate with the client, the desktop is suspended as soon as the client detects that entitlement has been withdrawn. Upon suspension, the user is presented with an error that informs them that the desktop is no longer allowed to run offline.

If no communication can be established with the offline client, the user is notified that their access has been removed the next time they attempt to access their desktop in the presence of a network connection.

Rolling Back a Desktop

You can also remove client access to their offline desktop by rolling back their offline session. Once a rollback event has been initiated, the offline client—if it can be contacted— is notified that the user is no longer allowed to log in to their checked out desktop.

- If a checked out desktop is rolled back while the user is logged in, the current session is terminated as soon as View Client with Offline Desktop receives notification.
- If the user is not logged in, subsequent attempts to connect will be redirected to the online desktop.

In order to continue working offline, the user must now check out the desktop from the server.

To roll back an offline desktop session, select the desktop from the list provided in the table under the **Offline Sessions** tab, and click **Rollback**.

If the client policy allows it, users can also roll back a desktop from within View Client or View Portal desktop by right-clicking on the offline desktop entry and clicking **Rollback** from the context menu. Only the user who checked out the desktop is allowed to do this.

NOTE A Roll back cannot be executed during any type of active transfer.

---

8 Component Policies

A policy is a rule or set of rules defined by a system administrator that governs the behavior of an application. Within View Manager, policies can be used to establish the configuration of constituent components by controlling the logging of information, managing client access, restricting device usage, establishing security parameters for client usage, and so forth.

Some component policies can be assigned through View Administrator, whereas others are contained within Group Policy Objects inside Active Directory and are applied to users or desktops at the Windows registry level. The following sections describe the purpose of each type of policy, and where they are configured and applied.

This chapter discusses the following topics:

Power Policy

During the deployment process, many types of desktop or desktop pool present you with the opportunity to configure the power policy of their desktop sources. Power policy controls how desktops behave when they are not in use and is therefore an important mechanism for the management of resources within your VI environment.

NOTE A View Manager desktop is not in use before the user has logged in, or after the user has disconnected or logged off.

Table 8-1 describes the different virtual machine power policy states that can be assigned to a desktop or desktop pool during deployment.

Table 8-1. Power Policy Definitions

Property	Description
Do nothing (VM remains on)	Virtual machines that are powered off will be started when required and will remain on, even when not in use, until they are shut down.
Ensure VM is always powered on	All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they will immediately restart.
Suspend	All virtual machines in the pool enter a suspended state when not in use.
Power off	All virtual machines in the pool shut down when not in use.

Table 8-2 describes the circumstances under which the power policy is applied

Table 8-2. Power Policy Notes

Desktop Type	Power Policy is Applied...
Individual Desktop (VirtualCenter Managed VM)	After user disconnection or logoff.
Persistent Automated Pool	When not in use or after user disconnection or logoff. This policy only applies to unassigned desktops.
Non-Persistent Automated Pool	When not in use or after user disconnection or logoff. **Note:** If the **Power Off** policy is applied after a disconnection, the session is discarded. If the **Suspend** policy is applied after a disconnection, an orphaned session could be created (the desktop is non-persistent so there is no guarantee that the user will ever be able to return to it). Ensure that **Automatic logoff after disconnect** is set to **Immediately** in order to prevent either scenario.
Persistent Manual Pool (VirtualCenter Managed VMs)	After user disconnection or logoff. This policy only applies to unassigned desktops.

Table 8-2. Power Policy Notes (Continued)

Desktop Type	Power Policy is Applied...
Non-Persistent manual Pool	After user disconnection or logoff. **Note:** If the **Power Off** policy is applied after a disconnection, the session is discarded. If the **Suspend** policy is applied after a disconnection, an orphaned session could be created (the desktop is non-persistent so there is no guarantee that the user will ever be able to return to it). Ensure that **Automatic logoff after disconnect** is set to **Immediately** in order to prevent either scenario.
Physical Systems / Terminal Services Desktop Pool	N/A

Power Policy in Automated Pools

In an automated pool, power policy is acquiescent to the rules regarding desktop availability. An available desktop is one that is active, does not contain a user session, is not assigned to a user, and has an active View Agent service that confirms its availability to View Connection Server based upon the preceding criteria.

Power Policy Example 1

If a particular number of desktops are required to be available at any given time, the power policy for those desktops ensures that they are always powered on. This behavior is illustrated in the following pooling example, the parameters for which are provided in Table 8-3.

Table 8-3. Pooling Example 1

Type	Minimum	Maximum	Available	Power Policy
Non-Persistent Automated Pool	10	20	2	Suspend

After the deployment process is completed, 10 desktops are created: 2 are powered on and immediately available, and 8 are in a suspended state. For each new user that connects, a desktop is powered on so as to maintain the availability level.

When the number of connected users exceeds 8, additional desktops—up to a limit of 20—are created so that the availability level can be maintained. Once the maximum number is reached, the desktops of the first 2 users to disconnect remain powered on in order to maintain the availability threshold. The desktop of each subsequent user to disconnect is suspended, as per policy.

Power Policy Example 2

In the following pooling example—the parameters for which are provided in Table 8-4—the maximum and minimum number of desktops are equal.

Table 8-4. Pooling Example 2

Type	Minimum	Maximum	Available	Power Policy
Non-Persistent Automated Pool	5	5	2	Suspend

Initially, 5 desktops are created: 3 suspended and 2 powered on and available. If a fourth system in this pool is suspended, no additional desktop is created as the maximum number has already been reached. Instead, one of the existing system is resumed.

Power Policy Example 3

Persistent automated pools behave slightly differently. Although a desktop may be powered on, it may also be assigned to a user and is therefore not considered to be available. Table 8-5 contains example parameters for a pool of this type.

Table 8-5. Pooling Example 3

Type	Minimum	Maximum	Available	Power Policy
Persistent Automated Pool	3	5	2	Ensure VM is always powered on

In this example, 3 desktops are created and powered on. If the desktops are then manually powered off in VirtualCenter they will all immediately power on again, as per policy.

Once a user connects to a desktop, it becomes permanently assigned to them; after they disconnect, it is no longer available to any other user. If the assigned desktop is shut down from within VirtualCenter, it remains powered down—the power policy no longer applies—although the reconnection of its assigned View Manager user will automatically power on the desktop once more.

At this time, there are still a sufficient number of unassigned desktops remaining in the pool for the availability criteria to be met. However, when another user connects a second desktop becomes assigned. Now, the number of available desktops has fallen below the threshold level so a new desktop is created and powered on.

In the above scenario, the creation of additional desktops takes place every time a new user is assigned until the maximum desktop threshold is reached.

Client Policies

The properties provided under the policies tab in View Administrator are used to assert behavioral control over client components at the global, desktop pool, or desktop user level. By default, each user-level policy inherits its setting from a pool-level policy that, in turn, inherits its setting from a global policy.

A number of general component behaviors relating to desktop sessions can be configured directly from within View Administrator. These policies can apply to both View Client and View Client with Offline Desktop and are described in Table 8-6.

Table 8-6. Client Policies

Property	Description
USB Access	Specifies if desktops can use USB devices connected to the client system. Administrators can prevent use of external devices as a security measure. Available options are **Allow** and **Deny**. Pool- and user-level policies may also **Inherit** the default setting from their parent. The default is `Allow`.
MMR	Specifies if multimedia redirection (MMR) is enabled on the client. MMR is a Microsoft DirectShow filter that forwards multimedia data from specific codecs on the remote system directly through a TCP socket to the client. The data is then decoded directly on the client, where it is played. Administrators can disable MMR if the client has insufficient resources to handle local multimedia decoding. Available options are **Allow** and **Deny**. Pool- and user-level policies may also **Inherit** their default settings from their parent. **Note:** MMR will not work correctly if the client video display hardware does not have overlay support. MMR policy does not apply to Offline Desktop sessions. The default is `Allow`.

The View Manager policies that relate specifically to Offline Desktop sessions are described in Table 8-7.

Table 8-7. Client Policies for Offline Desktop

Property	Description
Offline Desktop	Specifies if desktops can be checked out for local use. Available options are **Allow** and **Deny**. Pool- and user-level policies may also **Inherit** the default setting from their parent. The default is `Allow`.
User-initiated Rollback	Specifies if users are allowed to discard their offline desktop in order to revert to using the online version. When this action is carried out, the lock on the online desktop is released and the offline desktop is abandoned—the local folder that contains the offline desktop data can then be manually removed and deleted if necessary. Available options are **Allow** and **Deny**. Pool- and user-level policies may also **Inherit** their default settings from their parent. The default is `Allow`.
Max time without server contact	Specifies the amount of time an Offline Desktop desktop can run without successfully contacting the View Connection Server for policy updates. When this time is reached, a warning is displayed to the user and the offline desktop is suspended. The available options for pool- and user-level policies are **Inherit**, where the default setting is inherited from the parent, and **Set**. When **Set** is selected you can then enter the lifetime of the cache in **Days**, **Hours**, or **Minutes** in the field provided. This policy can be modified at the global level in the same way and starts with a default of **7** days.

Configuring and Applying Client Policies

Where the new pool-level policy is more restrictive, a pool-level policy can be configured to override the equivalent global policy.

For example, if the global policy for desktop check out is **Allow**, you can set the equivalent pool-level policy to **Deny**. The reverse is not true. If the global policy for desktop check out is **Deny**, you cannot apply the equivalent pool-level policy to **Allow**.

Similarly, if the global policy that specifies the amount of time a checked out desktop can run without successfully contacting the server is set to **10** minutes, you cannot apply a server contact policy of **30** minutes to any desktop pool.

NOTE View Administrator warns you if you attempt to apply a less restrictive policy to a pool.

User-level policies override global- or pool-level policies—that is, they can be more or less restrictive than either. For example, if the global server contact policy for all checked out desktops is **10** minutes, and the pool-level equivalent is **5** minutes, you can assign a server contact policy of **30** minutes to any user in that pool.

To configure and assign global policy settings

1 From View Administrator, click the **Desktops and Pools** button () to display the Global desktop and pool view and then click the **Inventory** tab. In the **Inventory** pane, ensure that the top-level **Desktops** entry () is selected.

2 In the Desktops pane, click the **Global Policies** tab. You are presented with the global policies page.

3 In the View Policies box or Offline Desktop Policies box, click **Edit**. The appropriate policies window is displayed.

4 Specify the policy settings and click **OK**. The global policy settings are now applied.

To configure and assign pool-level policy settings

1 From View Administrator, click the **Desktops and Pools** button () to display the Global desktop and pool view and then click the **Inventory** tab.

2 In the **Inventory** pane, select the desktop pool entry () that corresponds to the pool you want to apply the policy to.

3 In the Desktops pane, click the **Policies** tab. You are presented with the policies page for this desktop pool.

4 In the View Policies box, click **Edit Pool Policies.** If you have selected an offline desktop and want to configure offline policies, click **Offline Desktop Policies**. The appropriate policies window is displayed.

5 Specify the **Offline Desktop**, **User-initiated rollback**, and **Max time without server contact** policy settings and click **OK**. The pool-level policy settings are now applied.

To configure and assign user-level policy settings

1 From View Administrator, click the **Desktops and Pools** button ( ) to display the Global desktop and pool view and then click the **Inventory** tab.

2 In the **Inventory** pane, select the desktop pool entry ( ) that corresponds to the pool you want to apply the policy to.

3 In the Desktops pane, click the **Policies** tab. You are presented with the policies page for this desktop pool.

4 In the Policy Overrides box, click **Add User**. The Policy Override window is displayed.

5 Click **Add** and enter the name or description of the user or users you want to assign the policy to, and click **Find Now**.

NOTE If you want to view a list of all users in the domain, leave the **Name** and **Description** fields blank.

---

6 Select one or more users from the list and click **OK** to return to the Policy Override window.

7 Select the user, or users, you want to assign a new policy to and click **Next**.

8 Specify the policy settings and click **OK**. The user-level policy settings are now applied.

Group Policy Objects

Group Policy is a feature of the Microsoft Windows NT family of operating systems that provides centralized management and configuration of computers and remote users in an Active Directory environment. Policy properties are contained within entities called Group Policy Objects (GPOs) and can be configured by using the Group Policy editor features provided by Active Directory.

GPOs can be applied to View Manager components at a domain-wide level in order to provide granular control over various areas of the View Manager environment. Once applied, GPO properties are stored in the local Windows registry of the specified component.

In order to minimize the administrative overhead of creating bespoke polices, a number of component-specific GPO templates are provided with View Connection Server that can be imported into Active Directory. The template files that accompany View Manager are described below:

- `vdm_agent.adm` contains properties relating to the authentication and environmental components of a client desktop controlled by View Agent
- `vdm_client.adm` contains properties relating to the configuration parameters of View Client

  NOTE Clients connecting from outside the View Connection Server domain are unaffected by any GPOs applied to the View Client component.

- `vdm_server.adm` contains properties relating to View Connection Server
- `vdm_common.adm` contains properties relating to all components of View Manager

The GPO template files are stored in the following location:

```
C:\Program Files\VMware\View Manager\Server\Extras\GroupPolicyFiles
```

Microsoft TechNet provides detailed guidance on how to load GPO templates directly into Active Directory:

http://technet.microsoft.com/en-us/library/cc728217.aspx

Application of Group Policies

Once the GPO templates have been loaded into Active Directory they are read and applied: at startup for desktops, and during logon for users. By default, client systems refresh most Group Policy settings approximately every 90 minutes.

NOTE The policy update interval is controlled by a general Windows policy, and can itself be modified.

Computer Configuration GPO

With the Computer Configuration GPO you can set policies that are applied to all systems, regardless of who connects to the desktop. Where equivalent policies exist in the User Configuration GPO, the policies contained in this group are overridden.

View Agent Configuration

Use the GPOs described in Table 8-8 and Table 8-9 to configure View Agent behavior.

Table 8-8. View Agent Configuration Properties

Property	Description
`Recursive enumeration of trusted domains`	Determines if every domain trusted by the domain in which the agent resides is enumerated. In order to establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to View Connection Server in order to ensure that all trusted domains are available to the client on login. This property is `enabled` by default. When disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place. **Note:** In environments with complex domain relationships—such as those that use multiple forest structures with trust between domains in their forests—this process can take a few minutes to complete.

Table 8-9. View Agent Configuration Properties - Agent Configuration

Property	Description
`AllowDirectRDP`	Determines if non-View clients can connect directly to desktops using RDP. When disabled, the agent will only permit View Manager-managed connections via View Client or View Portal. This property is enabled by default.
`AllowSingleSignon`	Determines if single sign-on (SSO) is used to connect users to View Manager desktops. When enabled, users are only required to enter their credentials when connecting to View Client or View Portal. When disabled, users must reauthenticate when the remote connection is made. This property requires that the Secure Authentication component of View Agent is installed on the desktop, and is enabled by default.
`ConnectionTicketTimeout`	Specifies the time in seconds for which the View connection ticket is valid. The connection ticket is used by View clients when connecting to View Agent and is used for verification and single sign-on purposes. For security reasons, these tickets are only valid within the specified time period. If this property is not explicitly set, a default of `900` seconds applies.

Table 8-9. View Agent Configuration Properties - Agent Configuration (Continued)

Property	Description
`Connect Using DNS Name`	Determines if the View Connection Server uses the DNS name of the machine to connect to, rather than its IP address. This is often used in a NAT/Firewall situation when the View Client or View Connection Server cannot use the virtual desktop IP address directly. This property is disabled by default.
`Disable Time Zone Synchronization`	Determines if the time zone of the View Manager desktop is synchronized with that of the connected client. When enabled, this property will only apply if the `Disable time zone forwarding` property of the View Client Configuration policy is not set to `disabled`. This property is disabled by default.
`CommandsToRunOnConnect`	A list of one or more commands that are executed when a client logs on to a desktop.
`CommandsToRunOnReconnect`	A list of one or more commands that are executed when a client reconnects to a desktop that contains an active session.

View Client Configuration

Use the GPO described in Table 8-10, Table 8-11 and Table 8-12 to configure View Client and View Client with Offline Desktop behavior.

Table 8-10. View Client Configuration Properties

Property	Description
`Disable time zone forwarding`	Determines if the time zone of the View Manager desktop is synchronized with that of the connected client. When enabled, this property will only apply if the `Disable Time Zone Synchronization` property of the View Agent Configuration policy is not set to `disabled`. This property is disabled by default.
`Pre-login message precedes smart card PIN request`	When enabled the pre-login message is sent before a smart card PIN request. When disabled the pre-login message is presented after a smart card PIN request. This property is enabled by default.

Table 8-11. View Client Configuration Properties: Scripting Definitions

Property	Description
`Server URL`	Determines the URL used by View Client during login. For example: `http://view1.example.com`
`Logon UserName`	Determines the username used by View Client during login.
`Logon DomainName`	Determines the NETBIOS domain name used by View Client during login.
`Logon Password`	Determines the password used by View Client during login. Warning: this password is stored in plain text by Active Directory
`DesktopName to select`	Determines the default desktop used by View Client during login.
`DesktopLayout (requires DesktopName)`	Determines the display state of the View Client window when the desktop is launched. When this property is enabled, the available settings are: ■ `FullScreen` ■ `MultiMonitor` ■ `Window` **Note:** This property is only available when the `DesktopName to select` property has been set.
`Suppress error messages (when fully scripted only)`	Determines if error messages are displayed during login. **Note:** This property is only applied when the login process is fully scripted, that is, when all the requisite login information has been pre-populated beforehand through policy. **Note:** If the login fails on account of incorrect login information being entered, the user is not notified and the View Client `wswc.exe` process will continue to run in the background.

Table 8-12. View Client Configuration Properties - Security Settings

Property	Description
`Ignore incorrect SSL certificate common name (host name field)`	Determines if errors associated with incorrect server certificate common names are disabled. When the common name on the certificate does not correlate with the hostname of the server that sends it, an error results. When this property is enabled, this error is ignored. This property is disabled by default.
`Ignore bad SSL certificate date received from the server`	Determines if errors associated with invalid server certificate dates are disabled. This error occurs when the date on certificate sent by the server has passed.
`Ignore unknown certificate authority problems`	Determines if errors associated with an unknown certification authority on the server certificate are ignored. This error occurs when the certificate sent by the server is signed by an untrusted third-party authority.
`Ignore certificate revocation problems`	Determines if errors associated with a revoked server certificate are ignored. This error occurs when the certificate sent by the server has been revoked.
`Ignore incorrect usage problems`	Determines if errors associated with incorrect usage of a server certificate are ignored. This error occurs when the certificate sent by the server intended for some purpose other than verifying the identity of the sender and encrypting server communications.
`Always show certificate select dialog`	This policy applies to smart card authenticated sessions on View Client, and ensures that the user is presented with a certificate selection dialog box during login.

View Common Configuration

Use the GPOs described in Table 8-13, Table 8-14, and Table 8-15 to configure properties that apply to all View Manager components:

Table 8-13. View Manager Common Configuration Properties

Property	Description
`Enable extended logging`	Determines if `trace` and `debug` events are included in the log files
`Disk threshold for log and events in MegaBytes`	Specifies the minimum remaining disk space threshold for logs and events. If no value is specified, a default of `200` applies. When this value is reached, event logging will stop.

Table 8-14. View Manager Common Configuration - Log Configuration

Property	Description
`Number of days to keep logs`	Specifies the number of days for which log files are retained on the system. If no value is set, the default applies and log files will only be kept for `7` days.

View Server Configuration

Use the following GPOs to configure settings that can apply to all View Connection Server:

Table 8-15. View Manager Server Configuration Properties

Property	Description
`Recursive enumeration of trusted domains`	Determines if every domain trusted by the domain in which the server resides is enumerated. In order to establish a complete chain of trust, the domains trusted by each trusted domain are also enumerated and the process continues recursively until all trusted domains are discovered. This information is passed to View Connection Server in order to ensure that all trusted domains are available to the client on login. This property is `enabled` by default. When disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place. **Note:** In environments with complex domain relationships—such as those that use multiple forest structures with trust between domains in their forests—this process can take a few minutes to complete.

User Configuration GPO

With the User Configuration GPO you can set policies that apply to users, regardless of which desktop they connect to. These policies override any equivalent Computer Configuration Policies that may have been applied to the target desktop.

View Agent Configuration

Use the GPO described in Table 8-16 to configure View Agent behavior.

Table 8-16. View Agent Configuration Properties - Agent Configuration

Property	Description
`Disable Time Zone Synchronization`	Determines if the time zone of the View desktop is synchronized with that of the View client. When enabled, this property will only apply if the `Disable time zone forwarding` property of the View Client Configuration policy is not disabled. This property is disabled by default.

View Client Configuration

Use the GPOs described in Table 8-17, Table 8-18 and Table 8-19 to configure View Client and View Client with Offline Desktop behavior.

Table 8-17. View Client Configuration Properties

Property	Description
`Disable time zone forwarding`	Determines if the time zone of the View desktop is synchronized with that of the connected client. When enabled, this property will only apply if the `Disable Time Zone Synchronization` property of the View Agent Configuration policy is not disabled. This property is disabled by default.
`Enable the shade`	Determines if the shade [menu bar] at the top of the View Client window is enabled. This property is enabled by default.
`Pin the Shade`	Determines if the pin on the shade at the top of the View Client window is enabled, in order to prevent auto-hiding of the menu bar. **Note:** this property has no effect if the shade is disabled. This property is enabled by default.

Table 8-17. View Client Configuration Properties (Continued)

Property	Description
`Don't check monitor alignment on spanning`	By default, the client desktop will not span multiple monitors if the screens do not form an exact rectangle when in combination (that is, identical heights if positioned left and right monitors, or identical widths if positioned top and bottom). This property overrides this rule and is disabled by default.
`Enable multi-media acceleration`	Specifies if multimedia redirection (MMR) is enabled on the client. MMR is a Microsoft DirectShow filter that forwards multimedia data from specific codecs on the remote system directly through a TCP socket to the client. The data is then decoded directly on the client, where it is played. Administrators can disable MMR if the client has insufficient resources to handle local multimedia decoding. **Note:** MMR will not work correctly if the View client video display hardware does not have overlay support. MMR policy does not apply to Offline Desktop sessions.

Table 8-18. View Client Configuration Properties – Scripting Definitions

Property	Description
`Server URL`	Determines the URL used by View Client during login. For example: `http://view1.example.com`
`Logon UserName`	Determines the username used by View Client during login.
`Logon DomainName`	Determines the NETBIOS domain name used by View Client during login.
`Logon Password`	Determines the password used by View Client during login. Warning: this password is stored in plain text by Active Directory
`DesktopName to select`	Determines the default desktop used by View Client during login.

Table 8-18. View Client Configuration Properties – Scripting Definitions (Continued)

Property	Description
`DesktopLayout (when fully scripted only)`	Determines the display state of the View Client window when the desktop is launched. When this property is enabled, the available settings are: ■ `FullScreen` ■ `MultiMonitor` ■ `Window` **Note:** This property is only available when the login process is fully scripted, that is, when all login criteria have been pre-populated beforehand through policy.
`Suppress error messages (when fully scripted only)`	Determines if error messages are displayed during login. **Note:** This property is only applied when the login process is fully scripted, that is, when all the requisite login information has been pre-populated beforehand through policy. If the login fails on account of incorrect login information being entered, the user is not notified and the View Client `wswc.exe` process will continue to run in the background.

Table 8-19. View Client Configuration Properties – RDP Settings

Property	Description
`Color Depth`	Determines the color depth of the remote desktop. When this property is enabled, the available settings are: ■ `8` ■ `15` ■ `16` ■ `24` ■ `32` **Note:** For 24 bit Windows XP systems, ensure that the following Computer Configuration GPO property is set to `Enabled` and `24 bit`: `Computer Configuration` > `Administrative Templates` > `Windows Components` > `Terminal Services` > `Limit Maximum Color Depth`
`Desktop Background`	Determines if the desktop background is displayed when clients connect to the remote desktop.
`Show contents of window while dragging`	Determines if folder contents are displayed when users drag a folder to a new location.
`Menu and animation`	Determines how menus and windows behave when clients connect to the remote computer.

Table 8-19. View Client Configuration Properties – RDP Settings (Continued)

Property	Description
`Themes`	Determines if themes are displayed when clients connect to the remote desktop.
`Cursor shadow`	Determines if a shadow is displayed under the cursor on the remote desktop.
`Font smoothing`	(Windows Vista or later) Determines if anti-aliasing is applied to the fonts on the remote desktop.
`Desktop composition`	(Windows Vista or later) Determines if desktop composition is enabled on the remote desktop. When desktop composition is enabled, individual windows no longer draw directly to the screen or primary display device as they did in previous versions of Microsoft Windows. Instead, their drawing is redirected to off-screen surfaces in video memory, which are then rendered into a desktop image and presented on the display.
`Audio redirection`	Determines how audio information is channelled when played on the remote desktop. When this property is enabled, the available settings are: ■ `Disable Audio`—no audio ■ `Play in VM (needed for VoIP USB support)`—audio plays within the remote desktop (requires a shared USB audio device to provide sound on the client) ■ `Redirect to client`—audio is redirected to the client. This is the default mode. This property only applies to RDP audio—audio that is redirected via MMR will play in the client.
`Redirect drives`	Determines if local disk drives are automatically redirected when clients connect to the remote computer.
`Redirect printers`	Determines if local printers are automatically redirected when clients connect to the remote desktop.
`Redirect serial ports`	Determines if local COM ports are automatically redirected when clients connect to the remote desktop.
`Redirect smart cards`	Determines if local smart cards are automatically redirected when clients connect to the remote desktop.
`Redirect clipboard`	This setting determines if local clipboard information will be automatically redirected when clients connect to the remote desktop.

Table 8-19. View Client Configuration Properties – RDP Settings (Continued)

Property	Description
`Redirect supported plug and play devices`	Determines if local plug and play and point of sale devices are automatically redirected when clients connect to the remote desktop. This is not the same as the redirection managed by the USB Redirection component of View Agent.
`Bitmap caching`	Determines if remote bitmaps are cached on the local computer.
`Shadow bitmaps`	Determines if shadow bitmaps should be used. Shadow bitmaps are always disabled in full-screen mode, therefore this property has no effect when in full-screen mode.
`Cache persistence active`	Determines if persistent bitmap caching should be used. Persistent caching can improve performance but requires additional disk space.
`Enable compression`	Determines if the compression of RDP data is used, and is enabled by default.
`Windows key combinations`	Determines where Windows key combinations are applied. When this property is enabled, the available settings are: ■ `Apply key combinations locally` ■ `Send key combinations to VM`
`Bitmap cache file size in Kb for 8bpp bitmaps`	Specifies the size, in KB, of the persistent bitmap cache file to use for the 8 bits per pixel high-color setting. When this property is enabled, enter a file size in KB.
`Bitmap cache file size in Mb for 8bpp bitmaps`	Specifies the size, in MB, of the persistent bitmap cache file to use for the 8 bits per pixel high-color setting. When this property is enabled, enter a file size in MB.
`Bitmap cache file size in Mb for 16bpp bitmaps`	Specifies the size, in MB, of the persistent bitmap cache file to use for the 16 bits per pixel high-color setting. When this property is enabled, enter a file size in MB.
`Bitmap cache file size in Mb for 24bpp bitmaps`	Specifies the size, in MB, of the persistent bitmap cache file to use for the 24 bits per pixel high-color setting. When this property is enabled, enter a file size in MB.
`Bitmap cache file size in Mb for 32bpp bitmaps`	Specifies the size, in MB, of the persistent bitmap cache file to use for the 32 bits per pixel high-color setting. When this property is enabled, enter a file size in MB.

Unified Access

9

Large enterprises use a mix of physical PCs, server-based desktops, or applications that are published using terminal services, virtual desktops, and blade PCs. Users requiring access to more than one platform must use several different interfaces. Unified Access enables View Manager to provide a unified interface through which users can access their desktops being delivered by multiple back ends.

The term "desktop source" is used in this chapter to refer to terminal servers, physical computers, or unmanaged virtual machines.

This chapter describes the following topics:

Prepare Multiple Back-End Machines to Access Remote Desktops

A desktop source must be prepared to deliver desktop access. If desktop sources do not meet the following conditions, remote desktop delivery fails.

- Install View agent on the back-end machine. For more information about installing View agents, see "Install View Agent on an Unmanaged Desktop Source" on page 158.
- Ensure that the back-end machine meets the following requirements:
  - It is on the same domain as the View server or is on a trusted domain to enable single signon.
  - It allows the required domain users and groups to remotely connect to the machine to enable single signon.
- Ensure that a back-end machine that is not managed by VirtualCenter is powered on and is reachable by View Broker.
- Enable RDP connectivity on the back-end machine.

When these conditions are met, the machine is available to deliver remote desktops.

Desktop Parameters

You must set desktop parameters when you are configuring managed and unmanaged individual desktops, desktop pools, and terminal servers. The desktop parameters differ for managed and unmanaged resources. This section explains the significance of the desktop parameters and also discusses the mapping between desktop resources and their specific parameters. See Table 9-1, "Desktop Parameters," on page 157.

Table 9-1. Desktop Parameters

Property	Parameter Description
Desktop pool state	**Enabled** – After being created, the desktop pool is enabled and ready for immediate use. **Disabled** – After being created, the desktop pool is disabled and unavailable for use. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
Virtual machine power policy	**Do nothing (VM remains on) –** Virtual machines that are powered off are started when required and remain on, even when not in use, until they are shut down. **Ensure VM is always powered on –** All virtual machines in the pool remain powered on, even when they are not in use. If they are shut down, they immediately restart. **Suspend –** All virtual machines in the pool enter a suspended state when not in use. **Power off –** All virtual machines in the pool shut down when not in use.
Automatic logoff after disconnect	**Immediately** – Users are logged off as soon as they disconnect. **Never** – Users are never logged off. **After** – The time after which users are logged off when they disconnect. Enter the duration in minutes.
Power off and delete virtual machine after first use	Delete the virtual machine immediately after the user logs off. If necessary, a new virtual machine is cloned to maintain a specific pool size after virtual machines are deleted.
Allow users to reset their desktop	Allow desktop users to reset their own desktops without administrative assistance.
Allow multiple sessions per user	Allow individual users to simultaneously connect to multiple desktops in the same pool.

Table 9-2 shows which parameters are applicable to each desktop type.

Table 9-2. Mapping Desktop Parameters to Desktop Types ###

Parameters	Individual Managed Desktop	Individual Unmanaged Desktop	Manual Managed Pool		Manual Unmanaged Pool		Terminal Server Pool
			Persistent	Non-Persistent	Persistent	Non-Persistent	
Desktop State	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual machine power policy	Yes		Yes	Yes			
Automatic logoff after disconnect	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Allow users to reset their desktop	Yes		Yes	Yes			
Allow multiple sessions per user				Yes		Yes	

Install View Agent on an Unmanaged Desktop Source

During installation, the installer detects when the agent is being installed on an unmanaged desktop source. An unmanaged desktop source is a virtual machine that is not running on an ESX server. At the same time, the desktop source is also registered with a View connection server. After it is registered, the specified View connection server and its replica instances can communicate with the desktop source.

This section discusses installing the View agent on an unmanaged desktop source. For information about installing View agents on managed desktop sources, see "Preparing the Guest System" on page 52.

To install VMware View Agent on an unmanaged desktop source

1 Run the View Agent executable file on the system that will host the agent, where xxx is the build number of the file:

```
VMware-viewagent-e.x.p-xxx.exe
```

The installation wizard opens. Click **Next**.

2 Accept the VMware license terms and click **Next**.

3 Select your custom setup options.

Accept or change the destination folder and click **Next**.

4 In the **Register with View Connection Server** window, specify a server name or IP address.

The IP address can be a standard or replica View connection server instance.

5 Provide your administrator log in credentials to register this machine with the View connection server and click **Next**.

You can log in as the current user. If you select this option, the **Username** and **Password** fields are disabled.

You can specify administrator credentials. Specify the user name and password of the View connection server's administrator.

6 Your installation choices appear.

Click **Next** to confirm and continue with the installation.

7 Click **Install** to begin the installation process.

After the process is complete click **Finish**.

The unmanaged desktop source is now ready for use.

Add and Change Desktop Sources

Perform an end-to-end configuration on desktop sources to ensure that installation and configuration issues can be easily resolved. This section refers to both individual desktops and desktop pools.

To add an unmanaged individual desktop

1 Ensure that you have the appropriate login credentials and log in to View Administrator.

2 On the **Desktops** tab, click **Add**

3 In the **Desktop Type** window, select **Individual Desktop** and click **Next**.

4 In the **Desktop Source** window, select **Physical computers or virtual machines not managed by a VirtualCenter server** and click **Next**.

5 Enter the **Unique ID** and the **Display name** and **Description**.

The unique ID is the name that View Manager uses to identify the desktop. The desktop display name is what the user sees when logging in. The unique ID and display name can be arbitrary, but if you do not specify a display name, the unique ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters long and is only visible from the View administrator interface.

After you provide the desktop identification details, click **Next**.

6 Specify the desktop parameters and click **Next**.

For more information on the parameters that are applicable to unmanaged individual desktops, see Table 9-2, "Mapping Desktop Parameters to Desktop Types ###," on page 158.

7 In the table on the **Desktop Source** page, select the desktop source to be added as an individual desktop and click **Next**.

You can only select one desktop source. All registered desktop sources that are running a supported guest operating system and that another desktop or desktop pool is not using appear in the table. For more information about registering desktop sources, see "Install View Agent on an Unmanaged Desktop Source" on page 158.

8 Review the information in **Ready to Complete** and click **Finish** to accept it or **Back** to make corrections.

9 Click **Finish**.

The desktop is added and appears in the main **Desktops** page.

To add an unmanaged manual pool

1 Ensure that you have the appropriate login credentials and log in to View Administrator.

2 On the **Desktops** tab, click **Add**.

3 In the **Desktop Type** window, select **Manual Desktop Pool** and click **Next**.

4 In the **Desktop Persistence** window, specify the persistence settings for the desktops in this pool.

Persistent – This desktop pool allows users to log in to the same desktop every time. Users can save documents and files on persistent desktops because they return to the same desktop.

Non-persistent – Desktops are available to users when they log in but are returned to the pool when users log off. Users log in to a different desktop each time and cannot save documents or files on the desktop.

5 In the **Desktop Pool Source** window, choose **Physical computers or virtual machines not managed by a VirtualCenter server** and click **Next**.

6 Enter the **Unique ID**, the **Display name**, and **Description**.

The unique ID is the name that View Manager uses to identify the desktop. The desktop display name is what the user sees when logging in. The unique ID and display name can be arbitrary but if you do not specify a display name, the unique ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters in length and is only visible from within the View administrator interface.

After you provide the desktop identification details, click **Next**.

7 Specify the desktop parameters and click **Next**.

For more information on the parameters that are applicable to unmanaged persistent and non-persistent pools, see Table 9-2, “Mapping Desktop Parameters to Desktop Types ###,” on page 158.

8 In the table on the **Desktop Sources** page, select the desktop sources to include in the pool and click **Next**.

All registered desktop sources that are running a supported guest operating system and that another desktop or desktop pool is not using appear in the table. For more information about registering desktop sources, see “Install View Agent on an Unmanaged Desktop Source” on page 158.

9 Review the information in **Ready to Complete** and click **Finish** to accept it or **Back** to make corrections.

10 Click **Finish**.

The desktop is added successfully and appears in the main **Desktops** page.

To add a terminal server pool

1 Ensure that you have the appropriate login credentials and log in to View Administrator.

2 In the **Desktops** tab, click **Add**.

3 In the **Desktop Type** window, select **Microsoft Terminal Services Desktop Pool** and click **Next**.

4 Enter the **Unique ID**, the **Display name**, and the **Description**.

The unique ID is the name that View Manager uses to identify the desktop. The desktop display name is what the user sees when logging in. The unique ID and display name can be arbitrary but if you do not specify a display name, the unique ID is used for both.

NOTE You can use any alphanumeric character, including spaces, to provide an optional description. The description can be up to 1024 characters and is only visible from the View administrator interface.

After you provide the desktop identification details, click **Next**.

5 Specify the desktop parameters and click **Next**.

For more information on the parameters that are applicable to terminal server pools, see Table 9-2, "Mapping Desktop Parameters to Desktop Types ###," on page 158.

6 Click **Next**.

7 In the table on the **Desktop Sources** page, select the terminal services sources to include in the desktop pool and click **Next**.

All registered desktop sources that are running a supported guest operating system and that another terminal server pool is not using appear in the table. For more information about registering desktop sources, see "Install View Agent on an Unmanaged Desktop Source" on page 158.

8 Review the information in **Ready to Complete** and click **Finish** to accept it or **Back** to make corrections.

9 Click **Finish**.

The desktop is added and appears in the main **Desktops** page.

Enable or Disable a Desktop

You can only access desktops that are enabled.

To enable or disable a desktop

1 On the Desktops tab, select a desktop and click **Enable/Disable**.

If the desktop is currently enabled, you can disable it, and if it is currently disabled, you can enable it.

2 Select **Enable Desktop** or **Disable Desktop** as applicable, and click **OK**.

Entitle Users and Groups to a Desktop

After desktops or desktop pools are added, you must entitle them so that they are accessible to users and groups. A desktop can be assigned to multiple users, or multiple user groups.

To entitle users and groups

1 On the **Desktops** tab, select a desktop or desktop pool and click **Entitle**.

2 In the **Entitlement** window, click **Add** to add users or groups.

3 Specify the search criteria to retrieve a list of users or groups and click **Find Now**.

A list of users or groups or both are displayed.

4 Select the users or groups to entitle to use this desktop source and click **OK**.

The users or groups appear in the **Entitlement** window.

5 Select the users or groups and click **Remove** to stop them from accessing the desktop.

6 Click **OK** to return to the **Desktops** tab.

Add or Remove a Desktop Source

You can add or remove desktop sources from desktop pools.

To add a desktop source to a desktop pool

1 In the desktop pane, select a desktop pool and click on the **Desktop Sources** tab.

2 Click **Add** to add a desktop source to the pool.

3 Select the desktop sources to include in the pool and click **OK**.

You return to the main page, which lists all of the desktop sources in the pool.

To remove a desktop source from a desktop pool

1 In the desktop pane, select a desktop pool and click the **Desktop Sources** tab.

2 Select desktop sources and click **Remove**.

A confirmation message appears.

3 Click **OK** to remove the selected desktop source from the pool.

4 If any of the desktop sources have active sessions, indicate the action to be taken:

- Leave active – Active sessions will remain until the user logs off. The View connection server does not track these sessions.
- Terminate – Terminates all active sessions immediately.

5 You return to the main page and the desktop sources that you removed are no longer listed.

Change an Individual Desktop Source

You cannot add or remove desktop sources in the case of an individual desktop. But you can change or reset the desktop source. This section is applicable only to Individual Desktops and not to desktop pools.

To change an individual desktop source

1 In the desktop pane, select an individual desktop and click on the **Desktop Sources** tab.

2 Select the desktop source and click **Change**.

3 Select the virtual machine for the desktop to use and click **OK**.

All available virtual machines that are running a supported guest operating system and that another virtual desktop is not using appear in the table, including virtual machines that are suspended or not powered on.

A confirmation page appears.

4 Click **OK** to change the original desktop source to the selected one.

5 You return to the main page and you can see the desktop source that you changed.

Delete a Desktop

You can delete an individual desktop or a desktop pool.

To remove unmanaged desktops, you must unregister them. See "Unregister a Desktop Source."

To delete an unmanaged desktop pool

1 On the **Desktops** tab, select an unmanaged desktop pool or desktop and click **Delete**.

A warning message appears that you are trying to permanently delete this desktop pool.

Only the desktop pool is deleted. The registration information of the unmanaged desktops that belong to the pool is not deleted.

2 If any of the desktop sources have active sessions, select the action to be taken:

- **Leave active** – Active sessions remain until the user logs off. The View Connection Server does not track these connections.
- **Terminate** – Terminates all active sessions immediately.

3 Click **OK** to delete the desktop pool and return to the main page.

Unregister a Desktop Source

All desktop sources that the VirtualCenter Server manages are registered when you install the View Agent. For more information about installing View Agents, see "Install View Agent on an Unmanaged Desktop Source" on page 158. You can unregister only unmanaged desktop sources.

To unregister an unmanaged desktop source

1 Click on the **Configuration** tab.

The **Registered Desktop Sources** section displays the number of registered terminal sources and other unmanaged virtual machines.

2 Select the type of desktop source and click **View**.

3 Select the desktop source to unregister and click **Unregister**.

You can select only desktop sources that are not assigned to a desktop.

A message appears to check if you want to unregister the desktop source. If you unregister a desktop source, it becomes unavailable. To make these sources available again, reinstall the View Agent should in each desktop source.

4 Click **OK** if you want to unregister the selected desktop source.

The desktop sources are unregistered and are no longer available.

Troubleshooting 10

Occasionally when using the View Manager product, administrators or users may encounter unexpected behavior. In these situations, you can obtain assistance from VMware.

This chapter provides a summary of some of the high-level steps you can take to gather application data, request assistance, and search for support information in our knowledge base.

This chapter discusses these topics:

Collecting View Manager Diagnostic Information

Diagnostic information helps VMware Technical Support diagnose and resolve issues. View Manager includes a script called `vdm-support` that collects information for use by VMware Technical Support. Send the file generated by the script with your support request.

On the View Connection Server you can run the script manually or by using the support tool in the **Start** menu. For View Client or on View Manager desktops running View Agent, you must run the script manually.

Using the View Manager Support Tool to Collect Diagnostic Information

The View Manager Support tool lets you generate log files and set log levels that determine if you want to generate normal, debug, or full log files for the View Connection Server.

To set log levels using the View Manager Support Tool

1 On View Connection Server, click **Start**, click **All Programs**, and click **VMware**.

2 Select **Set View Connection Server Log Levels**.

3 In the **Choice** field, enter `1` for normal, `2` for debug, or `3` for full and press **Enter**.

To generate log files using the View Manager Support Tool

1 On View Connection Server, click **Start**, click **All Programs** and click **VMware**.

2 Select **Generate View Connection Server Log Bundle**.

The support tool creates a folder called `vdm-sdct` containing the generated log files, and places it on the desktop of View Connection Server.

Using the View Manager Support Script to Collect Diagnostic Information

Use View Manager Support Script to generate log files for View Connection Server, View Client and View Portal, and View Manager desktops running View Agent.

To collect diagnostic information using the script

1 Open a command prompt and change to the View Manager program directory. The location for each View Manager component is shown below:

- View Connection Server—`C:\Program Files\VMware\View Manager\Server\DCT`
- View Client or Web Access—`C:\Program Files\VMware\View Manager\Client\DCT`
- View Manager desktops running View Agent—`C:\Program Files\VMware\View Manager\Agent\DCT`

NOTE If you did not install the program in the default directory, substitute the appropriate drive letter and path.

2 Run the support script:

```
cscript vdm-support.vbs
```

When the script finishes, it informs you of the output filename and location.

3 File a support request on the Support page of the VMware Web site:

https://www.vmware.com/support/login.do

View Composer Support

The `svi-support` script provided with View Manager offers component-specific support for View Composer by collecting configuration and logging data. This information is gathered in order to help VMware customer support diagnose any issues that may arise while using this feature.

The svi-support script must be run with `cscript.exe`, a command-line version of the Windows Script Host that provides command-line options for setting script properties. Microsoft TechNet provides detailed guidance on how to use `cscript.exe`:

http://technet.microsoft.com/library/bb490887.aspx

The `svi-support` script is located on the VirtualCenter server in the same directory as the View Composer service:

```
C:\Program Files\VMware\View Composer
```

The `svi-support` script instructions are submitted from a Windows command prompt in the following form:

```
cscript.wsf svi-support.wsf [/?] [/novclogs] [/dmpdir:<value>]
[/dmpformat:<value>] [/nolog] [/fullbundle] [/filescount:<value>]
[/destdir:<value>] [/logdir:<value>] [/logformat:<value>]
[/zip:<value>]
```

All the parameters associated with the tool are optional, must be preceded by a forward-slash (/), and are described in Table 10-1.

Table 10-1. svi-support – Parameters

Parameter	Description
?	Displays the parameters used with the support script.
`novclogs`	VirtualCenter contains diagnostic scripts that collect server and database-related information from the VirtualCenter application logs. Specify this option if you want to disable the collection of information from the VirtualCenter logs.

Table 10-1. svi-support – Parameters (Continued)

Parameter	Description
`dmpdir`	The absolute path of the directory from which to gather the View Composer logs. Default is: `%ALLUSERSPROFILE%\Application Data\VMware\View Composer\Logs`
`dmpformat`	The prefix that will be used to filter the dmp files. Default is `vmware-svi-`
`nolog`	Disables the logging of events logged buy the system eventlog.
`fullbundle`	Generate full bundle containing extended data. This procedure can take up to 10 minutes and is omitted by default.
`filescount`	Maximum number of files to gather from each folder location. Default is `50`.
`destdir`	The absolute path of directory under which the log data will be saved. The default is the Windows desktop directory of the current user. If specified, ensure the directory permissions secure the log data.
`logdir`	The path of directory from which to gather logs. Default is: `%ALLUSERSPROFILE%\Application Data\VMware\View Composer\Logs`
`logformat`	The prefix that will be used to filter the log files. Default is `vmware-desktopcomposer`
`zip`	Specifies the utility used to archive the support information. If no value is specified, the default (built-in) tool is used.

Updating Support Requests

After you file a support request, you may receive an email request from VMware Technical Support asking for the output of the `vdm-support` or `svi-support` scripts. Reply to the email message and attach your script output file to the reply.

If the output is too large to include as an attachment (10MB or more), contact VMware Technical Support with your support request number and request FTP upload instructions. You can also update your support request and attach the file at the support Web site.

To update your support request

1 Visit the Support page at the VMware Web site and log in.

2 Click **Support Request History** and find the applicable support request number.

3 Update the support request and attach your `vdm-support` or `svi-support` script output.

Further Troubleshooting Information

The following URLs for VMware Knowledge Base (KB) articles contain troubleshooting information for View Manager. The KB articles are continually updated with new troubleshooting information.

- Top-level Knowledge Base search page:

  http://kb.vmware.com/selfservice/microsites/microsite.do

- Troubleshooting end user connection issues:

  http://www.vmware.com/info?id=342

- Troubleshooting pooling issues:

  http://www.vmware.com/info?id=343

- Troubleshooting USB issues:

  http://www.vmware.com/info?id=346

Glossary

A

Active Directory
A Microsoft directory service that stores information about the network operating system and provides services. Active Directory configures and manages users and groups and enables administrators to set security policies, control resources, and deploy programs across an enterprise.

ADAM (Active Directory Application Mode)
An LDAP implementation based on Active Directory.

active session
A live connection from a client or Web Access user to a virtual desktop. An established connection to a virtual desktop that has not timed out.

administrator user interface
The Web-based administrator user interface used to perform configuration and management tasks in View Manager. Also known as the View Administrator.

B

broker
Also known as a connection broker. The View Connection Server is a type of connection broker.

C

connection broker
A server that allows connections between remote users and virtual desktops and provides authentication and session management. The View Connection Server is a type of connection broker.

D

datastore
Virtual representations of combinations of underlying physical storage resources in the datacenter. A datastore is the storage location (for example, a physical disk, a RAID, or a SAN) for virtual machine files.

desktop
See "virtual desktop."

desktop virtual machine
See "virtual desktop."

desktop pool
A pool of virtual machines that an administrator designates for users or groups of users. *See also* "persistent desktop pool," "non-persistent desktop pool."

DMZ (demilitarized zone)
A logical or physical subnetwork that connects internal servers to a larger, untrusted network (usually the Internet) and provides an additional layer of security and gives administrators more control over who can access network resources.

DNS (Domain Name System)
An Internet data query service that translates host names into IP addresses. Also called "Domain Name Server" or "Domain Name Service."

F

FQDN (fully qualified domain name)
The name of a host, including both the host name and the domain name. For example, the FQDN of a host named `esx1` in the domain `vmware.com` is `esx1.vmware.com`.

G

guest
See "guest operating system."

guest operating system
An operating system that runs inside a virtual machine.

H

high availability
A system design approach that ensures a degree of operational continuity.

L

load balancing
A technique used for distributing processes across servers so that the traffic load is spread more evenly and servers do not become overloaded.

N

non-persistent desktop pool
A desktop pool in which users are not assigned to a specific desktop. When users log off or are timed out of a desktop, their desktops are returned to the pool and made available to other users. Users cannot save data or files to their desktops when using a non-persistent pool.

P

persistent desktop pool
A desktop pool in which users are assigned to a specific desktop. Users log on to the same desktop every time and their data is preserved when they log off. Users can save data and files to their desktops when using a persistent pool.

R

RDP (remote desktop protocol)
A multichannel protocol that allows a user to connect to a computer remotely.

RSA SecurID
A product from RSA that provides strong, two-factor authentication using a password and an authenticator.

S

security server
A View Connection Server deployment that adds a layer of security between the Internet and the internal network.

T

thin client
A device that allows a user to access virtual desktops but requires little memory or disk drive space. Application software, data, and CPU power resides on a network computer and not on the client device.

V

virtual desktop
A desktop operating system that runs on a virtual machine. A virtual desktop is indistinguishable from any other computer running the same operating system.

Index

E

F

G

I

Q

R

S

T

U

V

W