VMware View Administration

View 5.0
View Manager 5.0
View Composer 2.7

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

EN-000502-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

VMware View Administration

VMware View Administration describes how to configure and administer VMware View™, including how to configure View Connection Server, create administrators, provision and deploy View desktops, set up user authentication, configure policies, and manage VMware ThinApp™ applications in View Administrator. This information also describes how to maintain and troubleshoot VMware View components.

Intended Audience

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

1 Configuring View Connection Server

After you install and perform initial configuration of View Connection Server, you can add vCenter Server instances and View Composer services to View Manager, set up roles to delegate administrator responsibilities, and schedule backups of your configuration data.

This chapter includes the following topics:

Using View Administrator

View Administrator is the Web interface through which you configure View Connection Server and manage your View desktops.

For a comparison of the operations that you can perform with View Administrator, View cmdlets, and `vdmadmin`, see the *VMware View Integration* document.

View Administrator and View Connection Server

View Administrator provides a management interface for View Manager.

Depending on your View deployment, you use one or more View Administrator interfaces.

- Use one View Administrator interface to manage the View components that are associated with a single, standalone View Connection Server instance or a group of replicated View Connection Server instances.

  You can use the IP address of any replicated instance to log in to View Administrator.

- You must use a separate View Administrator interface to manage the View components for each single, standalone View Connection Server instance and each group of replicated View Connection Server instances.

You also use View Administrator to manage security servers and View Transfer Server instances associated with View Connection Server.

- Each security server is associated with one View Connection Server instance.
- Each View Transfer Server instance can communicate with any View Connection Server instance in a group of replicated instances.

Log In to View Administrator

To perform initial configuration tasks, you must log in to View Administrator.

Prerequisites

- Verify that View Connection Server is installed on a dedicated computer.
- Verify that you are using a Web browser supported by View Administrator. For View Administrator requirements, see the *VMware View Installation* document.

Procedure

1 Open your Web browser and enter the following URL, where *server* is the host name or IP address of the View Connection Server instance.

```
https://server/admin
```

You access View Administrator by using a secure (SSL) connection. When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. This response is expected behavior because the default certificate supplied with View Connection Server is self-signed.

2 Click **Ignore** to continue using the current SSL certificate.

3 Log in using administrator credentials on the View Connection Server computer.

Initially, all users who are members of the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer are allowed to log in to View Administrator.

After you log in to View Administrator, you can use **View Configuration > Administrators** to change the list of users and groups that have the View Administrators role.

Tips for Using the View Administrator Interface

You can use View Administrator user-interface features to navigate View Pages and to find, filter, and sort View objects.

View Administrator includes many common user interface features. For example, the navigation pane on the left side of each page directs you to other View Administrator pages. The search filters let you select filtering criteria that are related to the objects you are searching for.

Table 1-1 describes a few additional features that can help you to use View Administrator.

Table 1-1. View Administrator Navigation and Display Features

View Administrator Feature	Description
Navigating backward and forward in View Administrator pages.	Click the **Back** button in the upper left corner of a View Administrator page to go to the previously displayed View Administrator page. Click the **Forward** button to return to the current page. Do not use your browser's **Back** button. This button displays the View Administrator log-in page.
Multicolumn sorting	You can sort View objects in a variety of ways by using multicolumn sorting. Click a heading in the top row of a View Administrator table to sort the View objects in alphabetical order based on that heading. For example, in the **Inventory > Desktops** page, you can click **Pool** to sort desktops by the pools that contain them. The number **1** appears next to the heading to indicate that it is the primary sorting column. You can click the heading again to reverse the sorting order, indicated by an up or down arrow. To sort the View objects by a secondary item, Ctrl+click another heading. For example, in the **Desktops** table, you can click **Users** to perform a secondary sort by users to whom the desktops are dedicated. A number **2** appears next to the secondary heading. In this example, desktops are sorted by pool and by users within each pool. You can continue to Ctrl+click to sort all the columns in a table in descending order of importance. Press Ctrl+Shift and click to deselect a sort item. For example, you might want to display the desktops in a pool that are in a particular state and are stored on a particular datastore. You can click **Inventory > Pools**, click the pool ID, click the **Datastore** heading, and Ctrl+click the **Status** heading.
Selecting View objects and displaying View object details	In View Administrator tables that list View objects, you can select an object or display object details. ■ To select an object, click anywhere in the object's row in the table. At the top of the page, menus and commands that manage the object become active. ■ To display object details, double-click the left cell in the object's row. A new page displays the object's details. For example, on the **Inventory > Pools** page, click anywhere in an individual pool's row to activate commands that affect the pool. Double-click the **Pool ID** cell in the left column to display a new page that contains details about the pool.
Expanding dialog boxes to view details	You can expand View Administrator dialog boxes to view details such as desktop names and user names in table columns. To expand a dialog box, place your mouse over the dots in the lower right corner of the dialog box and drag the corner.

Troubleshooting Access to View Administrator Without a Secure SSL Connection

You cannot log in to View Administrator through a Web browser when the SSL setting for your View clients is not consistent with the URL you use to connect to View Administrator. If you deselect the SSL setting, you cannot use `https` in the URL.

Problem

The URL that you use to log in to View Administrator no longer works. A connection failure occurs.

Cause

By default, View Manager uses SSL to create secure connections between View clients and View Connection Server. This setting also applies to computers that connect to View Administrator through a Web browser.

This problem occurs when you change this setting in View Administrator by navigating to **View Configuration > Global Settings** and deselecting the **Require SSL for client connections and View Administrator** check box.

Solution

Use the following URL to connect to View Administrator, where *server* is the host name or IP address of the View Connection Server instance.

`http://server/admin`

Troubleshooting the Text Display in View Administrator

If your Web browser runs on a non-Windows operating system such as Linux, UNIX, or Mac OS, the text in View Administrator does not display properly.

Problem

The text in the View Administrator interface is garbled. For example, spaces occur in the middle of words.

Cause

View Administrator requires Microsoft-specific fonts.

Solution

Install Microsoft-specific fonts on your computer.

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

Configuring vCenter Server and View Composer

To use virtual machines as desktop sources, you must configure View Manager to communicate with vCenter Server. To create and manage linked-clone desktops, you must configure View Composer settings in View Manager.

Add vCenter Server Instances to View Manager

You must configure View Manager to connect to the vCenter Server instances in your View deployment. vCenter Server creates and manages the virtual machines that View Manager uses as desktop sources.

If you run vCenter Server instances in a Linked Mode group, you must add each vCenter Server instance to View Manager separately.

Prerequisites

- Install the View Connection Server product license key.
- Prepare a vCenter Server user with permission to perform the operations in vCenter Server that are necessary to support View Manager. To use View Composer, you must give the user additional privileges. To manage desktops that are used in local mode, you must give the user privileges in addition to those that are required for View Manager and View Composer.

  For details about configuring a vCenter Server user for View Manager, see the *VMware View Installation* document.
- If you plan to have View Connection Server connect to the vCenter Server instance using a secure channel (SSL), install a server SSL certificate on the vCenter Server host.

Procedure

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

2 In the vCenter Servers panel, click **Add**.

3 In the server address text box, type the fully qualified domain name (FQDN) or IP address of the vCenter Server instance.

The FQDN includes the host name and domain name. For example, in the FQDN ***myserverhost.companydomain.com***, ***myserverhost*** is the host name and ***companydomain.com*** is the domain.

NOTE If you enter a server by using a DNS name or URL, View Manager does not perform a DNS lookup to verify whether an administrator previously added this server to View Manager by using its IP address. A conflict arises if you add a vCenter Server with both its DNS name and its IP address.

4 Type the name of the vCenter Server user.

5 Type the vCenter Server user password.

6 (Optional) Type a description for this vCenter Server instance.

7 To connect to the vCenter Server instance using a secure channel (SSL), make sure that **Connect using SSL** is selected. SSL connection is the default setting.

8 Type the TCP port number.

The default port is 443.

9 (Optional) Click **Advanced** to configure the maximum concurrent pool operations in vCenter Server.

a Set the maximum number of concurrent provisioning operations.

This setting determines the largest number of concurrent requests that View Manager can make to provision full virtual machines in this vCenter Server instance. The default value is eight. This setting does not control linked-clone provisioning.

b Set the maximum number of concurrent power operations.

This setting determines the largest number of power operations (startup, shutdown, suspend, and so on) that can take place simultaneously on virtual machines managed by View Manager in this vCenter Server instance. The default value is five. This setting controls power operations for full virtual machines and linked clones.

10 Choose whether to configure View Composer.

Option	Action
You are not using View Composer	Click **OK**.
You are using View Composer	Configure the View Composer settings.

What to do next

If this View Connection Server instance or group of replicated View Connection Server instances uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Remove a vCenter Server Instance from View Manager

You can remove the connection between View Manager and a vCenter Server instance. When you do so, View Manager no longer manages the View desktops created in that vCenter Server instance.

Prerequisites

Delete all the View desktops that are associated with the vCenter Server instance. See "Delete a Desktop Pool from View Manager," on page 209.

Procedure

1 Click **View Configuration > Servers**.

2 In the vCenter Servers panel, select the vCenter Server instance.

3 Click **Remove**.

A dialog warns you that View Manager will no longer have access to the virtual machines that are managed by this vCenter Server instance.

4 Click **OK**.

View Manager can no longer access the virtual machines created in the vCenter Server instance.

Create a User Account for View Composer

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

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

Procedure

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

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

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

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

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

What to do next

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

Configure View Composer Settings for vCenter Server

To use View Composer, you must configure View Manager with initial settings that match the settings for the View Composer service that is installed in vCenter Server. View Composer is a feature of View Manager, but its service operates directly on virtual machines in vCenter Server.

NOTE If you are not using View Composer, you can skip this task.

Prerequisites

- Verify that you created a user in Active Directory with permission to add and remove virtual machines from the Active Directory domain that contains your linked clones. See "Create a User Account for View Composer," on page 14.
- Verify that you configured View Manager to connect to vCenter Server. See "Add vCenter Server Instances to View Manager," on page 12.

Procedure

1 In View Administrator, open the Edit vCenter Server dialog box.

   a Click **View Configuration > Servers**.

   b In the vCenter Servers panel, select the vCenter Server entry.

   c Click **Edit**.

2 Select **Enable View Composer** and make sure that the port number is the same as the port that you specified when you installed the View Composer service on vCenter Server.

   View Manager verifies that the View Composer service is running on vCenter Server.

3 Click **Add** to add the domain user for View Composer account information.

   a Type the domain name of the Active Directory domain.

   For example: `domain.com`

   b Type the domain user name, including the domain name.

   For example: `domain.com\admin`

   c Type the account password.

   d Click **OK**.

   e To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.

4 Click **OK** to close the Edit vCenter Server dialog box.

What to do next

Repeat this procedure for each vCenter Server instance in which View Composer services are installed.

Remove View Composer from View Manager

You can remove the connection between View Manager and the View Composer service installed in a vCenter Server instance. When you do so, View Manager no longer manages the linked-clone desktops created by View Composer in the vCenter Server instance.

Before you disable the connection to View Composer, you must remove from View Manager all the linked-clone desktops that were created by View Composer. After the connection to View Composer is disabled, View Manager cannot provision, manage, or delete the linked clones. View Manager does not force you to delete the linked clones. You must take this action on your own.

Procedure

1 Remove the linked-clone pools that were created by View Composer.

   a In View Administrator, click **Inventory > Pools**.

   b Select a linked-clone pool and click **Delete**.

      A dialog box warns that you will permanently delete the linked-clone pool from View Manager. The virtual machines are deleted from vCenter Server. In addition, the associated View Composer database entries and the replicas that were created by View Composer are removed.

   c Click **OK**.

   d Repeat these steps for each linked-clone pool that was created by View Composer.

2 Click **View Configuration > Servers**.

3 In the vCenter Servers panel, select the vCenter Server instance in which View Composer is installed.

4 Click **Edit**.

5 In the View Composer Settings panel, deselect **Enable View Composer** and click **OK**.

You can no longer create linked-clone desktops in this vCenter Server instance, but you can continue to create and manage full virtual-machine desktop pools in the vCenter Server instance.

If linked-clone desktops were not deleted before you disabled the connection to View Composer, you can try enabling the connection to View Composer, deleting the linked clones, and disabling the connection to View Composer again. For details about enabling View Composer, see "Configure View Composer Settings for vCenter Server," on page 15.

Conflicting vCenter Server Unique IDs

If you have multiple vCenter Server instances configured in your environment, an attempt to add a new instance might fail because of conflicting unique IDs.

Problem

You try to add a vCenter Server instance to View Manager, but the unique ID of the new vCenter Server instance conflicts with an existing instance.

Cause

Two vCenter Server instances cannot use the same unique ID. By default, a vCenter Server unique ID is randomly generated, but you can edit it.

Solution

1 In vSphere Client, click **Administration > vCenter Server Settings > Runtime Settings**.

2 Type a new unique ID and click **OK**.

For details about editing vCenter Server unique ID values, see the vSphere documentation.

Backing Up View Connection Server

After you complete the initial configuration of View Connection Server, you should schedule regular backups of your View Manager and View Composer configuration data.

For information about backing up and restoring your View configuration, see "Backing Up and Restoring View Configuration Data," on page 287.

Configuring Settings for Client Sessions

You can configure global settings that affect the client sessions that are managed by a View Connection Server instance or replicated group. You can set the session-timeout length, require SSL for client connections and View Administrator, display prelogin and warning messages, and set other client-connection options.

Set Options for Client Sessions and Connections

You configure global settings to determine the way client sessions and connections work.

The global settings are not specific to a single View Connection Server instance. They affect all client sessions that are managed by a standalone View Connection Server instance or a group of replicated instances.

You can also configure View Connection Server instances to use direct, nontunneled connections between View clients and View desktops. See "Configure the Secure Tunnel Connection and PCoIP Secure Gateway," on page 20 for information about configuring direct connections.

Prerequisites

Familiarize yourself with the global settings. See "Global Settings for Client Sessions and Connections," on page 18.

Procedure

1 In View Administrator, click **View Configuration > Global Settings**.

2 Click **Edit**.

3 Configure the global settings.

4 Click **OK**.

What to do next

If you change the **Require SSL for client connections and View Administrator** setting, you must restart the View Connection Server service to make your changes take effect. In a group of replicated View Connection Server instances, you must restart the View Connection Server service on all instances in the group. You do not have to restart the Windows Server computer where View Connection Server is installed.

Global Settings for Client Sessions and Connections

Global settings determine session time-out length and whether SSL is used, clients are reauthenticated after interruptions, View components use secure internal communications, prelogin and warning messages are displayed, and SSO is used for local-desktop operations.

Table 1-2. Global Settings for Client Sessions and Connections

Setting	Description
Session timeout	Determines how long a user can keep a session open after logging in to View Connection Server. The value is set in minutes. You must type a value. The default is 600 minutes. When a desktop session times out, the session is terminated and the View client is disconnected from the desktop.
Require SSL for client connections and View Administrator	Determines if a secure SSL communication channel is used between View Connection Server and View desktop clients, and between View Connection Server and clients that access View Administrator. When you select this setting, clients must use SSL connections. You must select this setting if you use smart card authentication. After you change this setting, you must restart the View Connection Server service to make your change take effect. In a group of replicated View Connection Server instances, you must restart each instance to make the change take effect.
Reauthenticate secure tunnel connections after network interruption	Determines if user credentials must be reauthenticated after a network interruption when View clients use secure tunnel connections to View desktops. When you select this setting, if a secure tunnel connection ends during a desktop session, View Client requires the user to reauthenticate before reconnecting. When this setting is not selected, the client reconnects to the desktop without requiring the user to reauthenticate. This setting has no effect when you use direct connection.
Message security mode	Determines the security of communications between View Manager components. Specifically, determines if signing and verification of the JMS messages passed between View Manager components takes place. For details, see "Message Security Mode for View Components," on page 19.
Disable Single Sign-on for Local Mode operations	Determines if single sign-on is enabled when users log in to their local desktops. If you disable this setting, users must manually log in to their desktops to start their Windows sessions after they log in. When you change this setting, the change takes effect for each user at the next user operation.
Enable automatic status updates	Determines if View Manager updates the global status pane in the upper left corner of View Administrator every few minutes. The dashboard page of View Administrator is also updated every few minutes. When you enable this setting, idle sessions do not time out for any user who is logged into View Administrator. IMPORTANT Disabling idle-session timeouts increases the risk of unauthorized use of View Administrator. Use caution when you enable this setting. By default, this setting is not enabled. Idle-session timeouts do occur.

Table 1-2. Global Settings for Client Sessions and Connections (Continued)

Setting	Description
Display a pre-login message	Displays a disclaimer or another message to View Client users when they log in. Type your information or instructions in the text box in the Global Settings dialog window. To display no message, leave the text box blank.
Display warning before forced logoff	Displays a warning message when users are forced to log off because a scheduled or immediate update such as a desktop-refresh operation is about to start. This setting also determines how long to wait after the warning is shown before the user is logged off. Check the box to display a warning message. Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is five minutes. Type your warning message. You can use the default message: `Your desktop is scheduled for an important update and will be restarted in 5 minutes. Please save any unsaved work now.`

Message Security Mode for View Components

You can set the level of security for communications between View components. This setting determines whether to sign and verify JMS messages that are passed between View Manager components. Enabling this setting prevents control messages that did not come from an authorized source from being processed.

In addition to signing and verifying messages, a best practice is to use IPSec to encrypt messages between View Connection Sever instances, and between View Connection Server instances and security servers.

If any component in your View environment predates View Manager 3.0, signing and verification cannot take place.

Table 1-3 shows the options you can select to configure the message security level. To set an option, select it from the **Message security mode** list in the Global Settings dialog window.

Table 1-3. Message Security Mode Options

Option	Description
Disabled	Message security mode is disabled.
Mixed	Message security mode is enabled but not enforced. You can use this mode to detect components in your View environment that predate View Manager 3.0. The log files generated by View Connection Server contain references to these components.
Enabled	Message security mode is enabled. Unsigned messages are rejected by View components. NOTE View components that predate View Manager 3.0 are not allowed to communicate with other View components

Message security mode is supported in View Manager 3.0 and later. If you change the message security mode from **Disabled** or **Mixed** to **Enabled**, you cannot launch a desktop with a View Agent from Virtual Desktop Manager version 2.1 or earlier. If you then change the message security mode from **Enabled** to **Mixed** or **Disabled**, the desktop still fails to launch. To launch a desktop after you change the message security mode from **Enabled** to **Mixed** or **Disabled**, you must restart the desktop.

If you plan to change an active View environment from **Disabled** to **Enabled**, or from **Enabled** to **Disabled**, change to **Mixed** mode for a short time before you make the final change. For example, if your current mode is **Disabled**, change to **Mixed** mode for one day, then change to **Enabled**. In **Mixed** mode, signatures are attached to messages but not verified, which allows the change of message mode to propagate through the environment.

Configure the Secure Tunnel Connection and PCoIP Secure Gateway

When the secure tunnel is enabled, View Client makes a second HTTPS connection to the View Connection Server or security server host when users connect to a View desktop.

When the PCoIP Secure Gateway is enabled, View Client makes a further secure connection to the View Connection Server or security server host when users connect to a View desktop with the PCoIP display protocol.

When the secure tunnel or PCoIP Secure Gateway is not enabled, the desktop session is established directly between the client system and the View desktop virtual machine, bypassing the View Connection Server or security server host. This type of connection is called a direct connection.

IMPORTANT A typical network configuration that provides secure connections for external clients includes a security server. To use View Administrator to enable or disable the secure tunnel and PCoIP Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server.

In a network configuration in which external clients connect directly to a View Connection Server host, you enable or disable the secure tunnel and PCoIP Secure Gateway by editing that View Connection Server instance in View Administrator.

Prerequisites

- If you intend to enable the PCoIP Secure Gateway, verify that the View Connection Server instance and paired security server are View 4.6 or later.
- If you pair a security server to a View Connection Server instance on which you already enabled the PCoIP Secure Gateway, verify that the security server is View 4.6 or later.

Procedure

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

2 In the View Connection Servers panel, select a View Connection Server instance and click **Edit**.

3 Configure use of the secure tunnel.

Option	Description
Disable the secure tunnel	Deselect **Use secure tunnel connection to desktop**.
Enable the secure tunnel	Select **Use secure tunnel connection to desktop**.

The secure tunnel is enabled by default.

4 Configure use of the PCoIP Secure Gateway.

Option	Description
Enable the PCoIP Secure Gateway	Select **Use PCoIP Secure Gateway for PCoIP connections to desktop**
Disable the PCoIP secure Gateway	Deselect **Use PCoIP Secure Gateway for PCoIP connections to desktop**

The PCoIP Secure Gateway is disabled by default.

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

Set a Single Sign-on Timeout Limit for View Users

By default, when a user logs in to View Connection Server from View Client, single sign-on (SSO) is enabled. The user does not have to log in again to connect to the View desktop. During a desktop session, a user can leave the desktop, allow it to become inactive, and return without having to authenticate again. To reduce the chance that someone else could start using the desktop session, you can configure a time limit after which the user's SSO credentials are no longer valid.

You configure the SSO timeout limit by setting a value in View LDAP. When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

The timeout limit is set in minutes. The time limit counter starts when the user logs in to View Connection Server. For example, if you set the value to 10 minutes, the user's SSO credentials are invalidated 10 minutes after the user logs in to View Connection Server.

NOTE On View desktops that are used in local mode, a checkout operation that takes longer than the SSO timeout value causes the user's SSO credentials to expire. For example, you might set the SSO timeout limit to 10 minutes. A user might log in to View Connection Server and check out a desktop. If the checkout takes 20 minutes, the user must log in again to connect to the local desktop, even though the user has not yet spent any time in a desktop session.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

1 Start the ADSI Edit utility on your View Connection Server host.

2 Select or connect to **DC=vdi, DC=vmware, DC=int**.

3 On the object **CN=Common, OU=Global, OU=Properties**, set the **pae-SSOCredentialCacheTimeout** attribute to the new SSO timeout limit in minutes.

The default value is 15. A value of -1 means that no SSO timeout limit is set. A value of 0 disables SSO.

On remote desktops, the new SSO timeout limit takes effect immediately. You do not need to restart the View Connection Server service or the client computer.

On desktops that run in local mode, the new SSO timeout limit takes effect the next time a client computer that hosts the local desktop sends a heartbeat message to View Connection Server.

Disable or Enable View Connection Server

You can disable a View Connection Server instance to prevent users from logging in to their View desktops. After you disable an instance, you can enable it again.

When you disable a View Connection Server instance, users who are currently logged in to View desktops are not affected.

Your View Manager deployment determines how users are affected by disabling an instance.

- If this is a single, standalone View Connection Server instance, users cannot log in to their desktops. They cannot connect to View Connection Server.
- If this is a replicated View Connection Server instance, your network topology determines whether users can be routed to another replicated instance. If users can access another instance, they can log in to their desktops.

Procedure

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

2 In the View Connection Servers panel, select the View Connection Server instance.

3 Click **Disable**.

You can enable the instance again by clicking **Enable**.

Edit the External URLs

You can use View Administrator to edit external URLs for View Connection Server instances and security servers.

By default, a View Connection Server or security server host can be contacted only by tunnel clients that reside within the same network. Tunnel clients that run outside of your network must use a client-resolvable URL to connect to a View Connection Server or security server host.

When users connect to View desktops with the PCoIP display protocol, View Client can make a further connection to the PCoIP Secure Gateway on the View Connection Server or security server host. To use the PCoIP Secure Gateway, a client system must have access to an IP address that allows the client to reach the View Connection Server or security server host. You specify this IP address in the PCoIP external URL.

Both the secure tunnel external URL and PCoIP external URL must be the addresses that client systems use to reach this host. For example, if you configure a View Connection Server host, do not specify the secure tunnel external URL for this host and the PCoIP external URL for a paired security server.

NOTE You cannot edit the external URLs for a security server that has not been upgraded to View Connection Server 4.5 or later.

Procedure

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

Option	Action
View Connection Server instance	Select the View Connection Server instance in the View Connection Servers panel and click **Edit**.
Security server	Select the security server in the Security Servers panel and click **Edit**.

2 Type the secure tunnel external URL in the **External URL** text box.

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

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

3 Type the PCoIP Secure Gateway external URL in the **PCoIP External URL** text box.

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

For example: `100.200.300.400:4172`

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

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

The external URLs are updated immediately. You do not need to restart the View Connection Server service or the security server service for the changes to take effect.

View LDAP Directory

View LDAP is the data repository for all View Manager configuration information. View LDAP is an embedded Lightweight Directory Access Protocol (LDAP) directory that is provided with the View Connection Server installation.

View LDAP contains standard LDAP directory components that are used by View Manager.

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

View LDAP contains directory entries that represent View Manager objects.

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

View LDAP also contains 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 a View LDAP directory.

Configuring View Connection Server Settings

You can use View Administrator to modify configuration settings for View Connection Server instances.

Configuring Role-Based Delegated Administration 2

One key management task in a View environment is to determine who can use View Administrator and what tasks those users are authorized to perform. With role-based delegated administration, you can selectively assign administrative rights by assigning administrator roles to specific Active Directory users and groups.

This chapter includes the following topics:

Understanding Roles and Privileges

The ability to perform tasks in View Administrator is governed by an access control system that consists of administrator roles and privileges. This system is similar to the vCenter Server access control system.

An administrator role is a collection of privileges. Privileges grant the ability to perform specific actions, such as entitling a user to a desktop pool. Privileges also control what an administrator can see in View Administrator. For example, if an administrator does not have privileges to view or modify global policies, the **Global Policies** setting is not visible in the navigation panel when the administrator logs in to View Administrator.

Administrator privileges are either global or object-specific. Global privileges control system-wide operations, such as viewing and changing global settings. Object-specific privileges control operations on specific types of inventory objects.

Administrator roles typically combine all of the individual privileges required to perform a higher-level administration task. View Administrator includes predefined roles that contain the privileges required to perform common administration tasks. You can assign these predefined roles to your administrator users and groups, or you can create your own roles by combining selected privileges. You cannot modify the predefined roles.

To create administrators, you select users and groups from your Active Directory users and groups and assign administrator roles. Administrators obtain privileges through their role assignments. You cannot assign privileges directly to administrators. An administrator that has multiple role assignments acquires the sum of all the privileges contained in those roles.

Using Folders to Delegate Administration

By default, desktop pools are created in the root folder, which appears as / or Root(/) in View Administrator. You can create folders under the root folder to subdivide your desktop pools and then delegate the administration of specific desktop pools to different administrators.

A desktop inherits the folder from its pool. An attached persistent disk inherits the folder from its desktop. You can have a maximum of 100 folders, including the root folder.

You configure administrator access to the resources in a folder by assigning a role to an administrator on that folder. Administrators can access the resources that reside only in folders for which they have assigned roles. The role that an administrator has on a folder determines the level of access that the administrator has to the resources in that folder.

Because roles are inherited from the root folder, an administrator that has a role on the root folder has that role on all folders. Administrators that have the Administrators role on the root folder are super administrators because they have full access to all of the inventory objects in the system.

A role must contain at least one object-specific privilege to apply to a folder. Roles that contain only global privileges cannot be applied to folders.

You can use View Administrator to create folders and to move existing pools to folders. You can also select a folder when you create a desktop pool. If you do not select a folder during pool creation, the pool is created in the root folder by default.

- Different Administrators for Different Folders on page 26

  You can create a different administrator to manage each folder in your configuration.

- Different Administrators for the Same Folder on page 27

  You can create different administrators to manage the same folder.

Different Administrators for Different Folders

You can create a different administrator to manage each folder in your configuration.

For example, if your corporate desktop pools are in one folder and your desktop pools for software developers are in another folder, you can create different administrators to manage the resources in each folder.

Table 2-1 shows an example of this type of configuration.

Table 2-1. Different Administrators for Different Folders

Administrator	Role	Folder
view-domain.com\Admin1	Inventory Administrators	`/CorporateDesktops`
view-domain.com\Admin2	Inventory Administrators	`/DeveloperDesktops`

In this example, the administrator called Admin1 has the Inventory Administrators role on the folder called `CorporateDesktops` and the administrator called Admin2 has the Inventory Administrators role on the folder called `DeveloperDesktops`.

Different Administrators for the Same Folder

You can create different administrators to manage the same folder.

For example, if your corporate desktop pools are in one folder, you can create one administrator that can view and modify those pools and another administrator that can only view them.

Table 2-2 shows an example of this type of configuration.

Table 2-2. Different Administrators for the Same Folder

Administrator	Role	Folder
view-domain.com\Admin1	Inventory Administrators	/CorporateDesktops
view-domain.com\Admin2	Inventory Administrators (Read only)	/CorporateDesktops

In this example, the administrator called Admin1 has the Inventory Administrators role on the folder called CorporateDesktops and the administrator called Admin2 has the Inventory Administrators (Read only) role on the same folder.

Understanding Permissions

View Administrator presents the combination of a role, an administrator user or group, and a folder as a permission. The role defines the actions that can be performed, the user or group indicates who can perform the action, and the folder contains the objects that are the target of the action.

Permissions appear differently in View Administrator depending on whether you select an administrator user or group, a folder, or a role.

Table 2-3 shows how permissions appear in View Administrator when you select an administrator user or group. The administrator user is called Admin 1 and it has two permissions.

Table 2-3. Permissions on the Administrators and Groups Tab for Admin 1

Role	Folder
Inventory Administrators	MarketingDesktops
Administrators (Read only)	/

The first permission shows that Admin 1 has the Inventory Administrators role on the folder called MarketingDesktops. The second permission shows that Admin 1 has the Administrators (Read only) role on the root folder.

Table 2-4 shows how the same permissions appear in View Administrator when you select the MarketingDesktops folder.

Table 2-4. Permissions on the Folders Tab for MarketingDesktops

Admin	Role	Inherited
view-domain.com\Admin1	Inventory Administrators	
view-domain.com\Admin1	Administrators (Read only)	Yes

The first permission is the same as the first permission shown in Table 2-3. The second permission is inherited from the second permission shown in Table 2-3. Because folders inherit permissions from the root folder, Admin1 has the Administrators (Read only) role on the MarketingDesktops folder. When a permission is inherited, Yes appears in the Inherited column.

Table 2-5 shows how the first permission in Table 2-3 appears in View Administrator when you select the Inventory Administrators role.

Table 2-5. Permissions on the Role Tab for Inventory Administrators

Administrator	Folder
view-domain.com\Admin1	/MarketingDesktops

Manage Administrators

Users who have the Administrators role can use View Administrator to add and remove administrator users and groups.

The Administrators role is the most powerful role in View Administrator. Initially, members of the local Administrators group (BUILTIN\Administrators) on your View Connection Server host are given the Administrators role in View Administrator.

NOTE By default, the Domain Admins group is a member of the local Administrators group. If you do not want domain administrators to have full access to inventory objects and View configuration settings, you must remove the Domain Admins group from the local Administrators group.

- Create an Administrator on page 28

  To create an administrator, you select a user or group from your Active Directory users and groups in View Administrator and assign an administrator role.

- Remove an Administrator on page 29

  You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root folder.

Create an Administrator

To create an administrator, you select a user or group from your Active Directory users and groups in View Administrator and assign an administrator role.

Prerequisites

- Familiarize yourself with the predefined administrator roles. See "Predefined Roles and Privileges," on page 34.
- Familiarize yourself with the best practices for creating administrator users and groups. See "Best Practices for Administrator Users and Groups," on page 39.
- To assign a custom role to the administrator, create the custom role. See "Add a Custom Role," on page 33.
- To create an administrator that can manage specific desktop pools, create a folder and move the desktop pools to that folder. See "Manage and Review Folders," on page 31.

Procedure

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

2 On the **Administrators and Groups** tab, click **Add User or Group**.

3 Click **Add**, select one or more search criteria, and click **Find** to filter Active Directory users or groups based on your search criteria.

4 Select the Active Directory user or group that you want to be an administrator user or group, click **OK** and click **Next**.

You can press the Ctrl and Shift keys to select multiple users and groups.

5 Select a role to assign to the administrator user or group.

The Apply to Folder column indicates whether a role applies to folders. Only roles that contain object-specific privileges apply to folders. Roles that contain only global privileges do not apply to folders.

Option	Action
The role you selected applies to folders	Select one or more folders and click **Next**.
You want the permission to apply to all folders	Select the root folder and click **Next**.

6 Click **Finish** to create the administrator user or group.

The new administrator user or group appears in the left pane and the role and folder that you selected appear in the right pane on the **Administrators and Groups** tab.

Remove an Administrator

You can remove an administrator user or group. You cannot remove the last super administrator in the system. A super administrator is an administrator that has the Administrators role on the root folder.

Procedure

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

2 On the **Administrators and Groups** tab, select the administrator user or group, click **Remove User or Group**, and click **OK**.

The administrator user or group no longer appears on the **Administrators and Groups** tab.

Manage and Review Permissions

You can use View Administrator to add, delete, and review permissions for specific administrator users and groups, for specific roles, and for specific folders.

- Add a Permission on page 29

  You can add a permission that includes a specific administrator user or group, a specific role, or a specific folder.

- Delete a Permission on page 30

  You can delete a permission that includes a specific administrator user or group, a specific role, or a specific folder.

- Review Permissions on page 31

  You can review the permissions that include a specific administrator or group, a specific role, or a specific folder.

Add a Permission

You can add a permission that includes a specific administrator user or group, a specific role, or a specific folder.

Procedure

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

2 Create the permission.

Option	Action
Create a permission that includes a specific administrator user or group	a On the **Administrators and Groups** tab, select the administrator or group and click **Add Permission**. b Select a role. c If the role does not apply to folders, click **Finish**. d If the role applies to folders, click **Next**, select one or more folders, and click **Finish**. A role must contain at least one object-specific privilege to apply to a folder.
Create a permission that includes a specific role	a On the **Roles** tab, select the role, click **Permissions**, and click**Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d If the role does not apply to folders, click **Finish**. e If the role applies to folders, click **Next**, select one or more folders, and click **Finish**. A role must contain at least one object-specific privilege to apply to a folder.
Create a permission that includes a specific folder	a On the **Folders** tab, select the folder and click **Add Permission**. b Click **Add**, select one or more search criteria, and click **Find** to find administrator users or groups that match your search criteria. c Select an administrator user or group to include in the permission and click **OK**. You can press the Ctrl and Shift keys to select multiple users and groups. d Click **Next**, select a role, and click **Finish**. A role must contain at least one object-specific privilege to apply to a folder.

Delete a Permission

You can delete a permission that includes a specific administrator user or group, a specific role, or a specific folder.

If you remove the last permission for an administrator user or group, that administrator user or group is also removed. Because at least one administrator must have the Administrators role on the root folder, you cannot remove a permission that would cause that administrator to be removed. You cannot delete an inherited permission.

Procedure

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

2 Select the permission to delete.

Option	Action
Delete a permission that applies to a specific administrator or group	Select the administrator or group on the **Administrators and Groups** tab.
Delete a permission that applies to a specific role	Select the role on the **Roles** tab.
Delete a permission that applies to a specific folder	Select the folder on the **Folders** tab.

3 Select the permission and click **Delete Permission**.

Review Permissions

You can review the permissions that include a specific administrator or group, a specific role, or a specific folder.

Procedure

1 Select **View Configuration > Administrators**.

2 Review the permissions.

Option	Action
Review the permissions that include a specific administrator or group	Select the administrator or group on the **Administrators and Groups** tab.
Review the permissions that include a specific role	Select the role on the **Roles** tab and click **Permissions**.
Review the permissions that include a specific folder	Select the folder on the **Folders** tab.

Manage and Review Folders

You can use View Administrator to add and delete folders and to review the desktop pools and desktops in a particular folder.

- Add a Folder on page 31

  If you want to delegate the administration of specific desktops or pools to different administrators, you must create folders to subdivide your desktops or pools. If you do not create folders, all desktops and pools reside in the root folder.

- Move a Desktop Pool to a Different Folder on page 32

  After you create a folder to subdivide your desktop pools, you must manually move desktop pools to the new folder. If you decide to change the way your desktop pools are subdivided, you can move desktops pools from one folder to another.

- Remove a Folder on page 32

  You can remove a folder if it does not contain inventory objects. You cannot remove the root folder.

- Review the Desktop Pools in a Folder on page 32

  You can see all of the desktop pools in a particular folder in View Administrator.

- Review the Desktops in a Folder on page 32

  You can see all of the desktops in a particular folder in View Administrator. A desktop inherits the folder from its pool.

Add a Folder

If you want to delegate the administration of specific desktops or pools to different administrators, you must create folders to subdivide your desktops or pools. If you do not create folders, all desktops and pools reside in the root folder.

You can have a maximum of 100 folders, including the root folder.

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 From the **Folder** drop-down menu on the command bar, select **New Folder**.

3 Type a name and description for the folder and click **OK**.

The description is optional.

What to do next

Move one or more desktop pools to the folder.

Move a Desktop Pool to a Different Folder

After you create a folder to subdivide your desktop pools, you must manually move desktop pools to the new folder. If you decide to change the way your desktop pools are subdivided, you can move desktops pools from one folder to another.

Procedure

1 In View Administrator, select **Inventory > Pools** and select the pool.

2 From the **Folder** drop-down menu, select **Change Folder**.

3 Select the folder and click **OK**.

View Administrator moves the pool to the folder that you selected.

Remove a Folder

You can remove a folder if it does not contain inventory objects. You cannot remove the root folder.

Prerequisites

If the folder contains inventory objects, move the objects to another folder or to the root folder. See "Move a Desktop Pool to a Different Folder," on page 32.

Procedure

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

2 On the **Folders** tab, select the folder and click **Remove Folder**.

3 Click **OK** to remove the folder.

Review the Desktop Pools in a Folder

You can see all of the desktop pools in a particular folder in View Administrator.

Procedure

1 In View Administrator, select **Inventory > Pools**.

The Pools page shows the pools in all folders by default.

2 Select the folder from the **Folder** drop-down menu.

The Pools page shows the pools in the folder that you selected.

Review the Desktops in a Folder

You can see all of the desktops in a particular folder in View Administrator. A desktop inherits the folder from its pool.

Procedure

1 In View Administrator, select **Inventory > Desktops**.

The Desktops page shows the desktops in all folders by default.

2 Select the folder from the **Folder** drop-down menu.

The Desktops page shows the pools in the folder that you selected.

Manage Custom Roles

You can use View Administrator to add, modify, and delete custom roles.

- Add a Custom Role on page 33

  If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in View Administrator.

- Modify the Privileges in a Custom Role on page 33

  You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

- Remove a Custom Role on page 34

  You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

Add a Custom Role

If the predefined administrator roles do not meet your needs, you can combine specific privileges to create your own roles in View Administrator.

Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See "Predefined Roles and Privileges," on page 34.

Procedure

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

2 On the **Roles** tab, click **Add Role**.

3 Type a name and description for the new role, select one or more privileges, and click **OK**.

The new role appears in the left pane.

Modify the Privileges in a Custom Role

You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

Prerequisites

Familiarize yourself with the administrator privileges that you can use to create custom roles. See "Predefined Roles and Privileges," on page 34.

Procedure

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

2 On the **Roles** tab, select the role.

3 Click **Usage** to display the privileges in the role and click **Edit**.

4 Select or deselect privileges.

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

Remove a Custom Role

You can remove a custom role if it is not included in a permission. You cannot remove the predefined administrator roles.

Prerequisites

If the role is included in a permission, delete the permission. See "Delete a Permission," on page 30.

Procedure

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

2 On the **Roles** tab, select the role and click **Remove Role**.

The **Remove Role** button is not available for predefined roles or for custom roles that are included in a permission.

3 Click **OK** to remove the role.

Predefined Roles and Privileges

View Administrator includes predefined roles that you can assign to your administrator users and groups. You can also create your own administrator roles by combining selected privileges.

- Predefined Administrator Roles on page 34

  The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.

- Global Privileges on page 35

  Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to folders.

- Object-Specific Privileges on page 36

  Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to folders.

- Internal Privileges on page 37

  Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

Predefined Administrator Roles

The predefined administrator roles combine all of the individual privileges required to perform common administration tasks. You cannot modify the predefined roles.

Table 2-6 describes the predefined roles and indicates whether a role can be applied to a folder.

Table 2-6. Predefined Roles in View Administrator

Role	User Capabilities	Applies to a Folder
Administrators	Perform all administrator operations, including creating additional administrator users and groups. Administrators that have the Administrators role on the root folder are super administrators because they have full access to all of the inventory objects in the system. Because the Administrators role contains all privileges, you should assign it to a limited set of users. Initially, members of the local Administrators group on your View Connection Server host are given this role on the root folder. IMPORTANT An administrator must have the Administrators role on the root folder to perform the following tasks: ■ Add and delete folders. ■ Manage ThinApp applications and configuration settings in View Administrator. ■ View and modify View Transfer Server instances and the Transfer Server repository. ■ Use the `vdmadmin` and `vdmimport` commands.	Yes
Administrators (Read only)	■ View, but not modify, global settings and inventory objects. ■ View, but not modify, ThinApp applications and settings, View Transfer Server instances, and the Transfer Server repository. ■ Run all PowerShell commands and command line utilities, including `vdmexport` but excluding `vdmadmin` and `vdmimport`. When administrators have this role on a folder, they can only view the inventory objects in that folder.	Yes
Agent Registration Administrators	Register unmanaged desktop sources such as physical systems, standalone virtual machines, and terminal servers.	No
Global Configuration and Policy Administrators	View and modify global policies and configuration settings except for administrator roles and permissions, ThinApp applications and settings, View Transfer Server instances, and the Transfer Server repository.	No
Global Configuration and Policy Administrators (Read only)	View, but not modify, global policies and configuration settings except for administrator roles and permissions, ThinApp applications and settings, View Transfer Server instances, and the Transfer Server repository.	No
Inventory Administrators	■ Perform all desktop, session, and pool-related operations. ■ Manage persistent disks. ■ Resync, Refresh, and Rebalance linked-clone pools and change the default pool image. When administrators have this role on a folder, they can only perform these operations on the inventory objects in that folder.	Yes
Inventory Administrators (Read only)	View, but not modify, inventory objects. When administrators have this role on a folder, they can only view the inventory objects in that folder.	Yes

Global Privileges

Global privileges control system-wide operations, such as viewing and changing global settings. Roles that contain only global privileges cannot be applied to folders.

Table 2-7 describes the global privileges and lists the predefined roles that contain each privilege.

Table 2-7. Global Privileges

Privilege	User Capabilities	Predefined Roles
Console Interaction	Log in to and use View Administrator.	Administrators Administrators (Read only) Inventory Administrators Inventory Administrators (Read only) Global Configuration and Policy Administrators Global Configuration and Policy Administrators (Read only)
Direct Interaction	Run all PowerShell commands and command line utilities, except for `vdmadmin` and `vdmimport`. Administrators must have the Administrators role on the root folder to use the `vdmadmin` and `vdmimport` commands.	Administrators Administrators (Read only)
Manage Global Configuration and Policies	View and modify global policies and configuration settings except for administrator roles and permissions.	Administrators Global Configuration and Policy Administrators
Manage Roles and Permissions	Create, modify, and delete administrator roles and permissions.	Administrators
Register Agent	Install View Agent on unmanaged desktop sources such as physical systems, standalone virtual machines, and terminal servers. During View Agent installation, you must provide your administrator login credentials to register the unmanaged desktop source with the View Connection Server instance.	Administrators Agent Registration Administrators

Object-Specific Privileges

Object-specific privileges control operations on specific types of inventory objects. Roles that contain object-specific privileges can be applied to folders.

Table 2-8 describes the object-specific privileges. The predefined roles Administrators and Inventory Administrators contain all of these privileges.

Table 2-8. Object-Specific Privileges

Privilege	User Capabilities	Object
Enable Pool	Enable and disable desktop pools.	Desktop pool
Entitle Pool	Add and remove user entitlements.	Desktop pool
Manage Composer Pool Image	Resync, Refresh, and Rebalance linked-clone pools and change the default pool image.	Desktop pool
Manage Desktop	Perform all desktop and session-related operations.	Desktop
Manage Local Sessions	Roll back and initiate replications for local desktops.	Desktop
Manage Persistent Disks	Perform all View Composer persistent disk operations, including attaching, detaching, and importing persistent disks.	Persistent disk
Manage Pool	Add, modify, and delete desktop pools and add and remove desktops.	Desktop pool
Manage Remote Sessions	Disconnect and log off remote sessions and send messages to desktop users.	Desktop
Manage Reboot Operation	Reset desktops.	Desktop

Internal Privileges

Some of the predefined administrator roles contain internal privileges. You cannot select internal privileges when you create custom roles.

Table 2-9 describes the internal privileges and lists the predefined roles that contain each privilege.

Table 2-9. Internal Privileges

Privilege	Description	Predefined Roles
Full (Read only)	Grants read-only access to all settings.	Administrators (Read only)
Manage Inventory (Read only)	Grants read-only access to inventory objects.	Inventory Administrators (Read only)
Manage Global Configuration and Policies (Read only)	Grants read-only access to configuration settings and global policies except for administrators and roles.	Global Configuration and Policy Administrators (Read only)

Required Privileges for Common Tasks

Many common administration tasks require a coordinated set of privileges. Some operations require permission at the root folder in addition to access to the object that is being manipulated.

Privileges for Managing Pools

An administrator must have certain privileges to manage pools in View Administrator.

Table 2-10 lists common pool management tasks and shows the privileges that are required to perform each task. You perform these tasks on the Pools page in View Administrator.

Table 2-10. Pool Management Tasks and Privileges

Task	Required Privileges
Enable or disable a pool	**Enable Pool** on the pool.
Entitle or unentitle users to a pool	**Entitle Pool** on the pool.
Add a pool	**Manage Pool** IMPORTANT When adding a linked-clone pool, you must have the Administrators role on the root folder to publish the base image to the Transfer Server repository.
Modify or delete a pool	**Manage Pool** on the pool.
Add or remove desktops from a pool	**Manage Pool** on the pool.
Refresh, Recompose, Rebalance, or change the default View Composer image	**Manage Composer Pool Image** on the pool.
Change folders	**Manage Pool** on both the source and target folders.

Privileges for Managing Desktops

An administrator must have certain privileges to manage desktops in View Administrator.

Table 2-11 lists common desktop management tasks and shows the privileges that are required to perform each task. You perform these tasks on the Desktops page in View Administrator.

Table 2-11. Desktop Management Tasks and Privileges

Task	Required Privileges
Remove a virtual machine	**Manage Pool** on the pool.
Reset a virtual machine	**Manage Reboot Operation** on the desktop.
Cancel, pause, or resume a task	**Manage Composer Pool Image**
Assign or remove user ownership	**Manage Desktop** on the desktop.
Enter or exit maintenance mode	**Manage Desktop** on the desktop.
Roll back or initiate replications	**Manage Local Sessions** on the desktop.
Disconnect or log off a remote session	**Manage Remote Sessions** on the desktop.

Privileges for Managing Persistent Disks

An administrator must have certain privileges to manage persistent disks in View Administrator.

Table 2-12 lists common persistent disk management tasks and shows the privileges that are required to perform each task. You perform these tasks on the Persistent Disks page in View Administrator.

Table 2-12. Persistent Disk Management Tasks and Privileges

Task	Required Privileges
Detach a disk	**Manage Persistent Disks** on the disk and **Manage Pool** on the pool.
Attach a disk	**Manage Persistent Disks** on the disk and **Manage Pool** on the desktop.
Edit a disk	**Manage Persistent Disks** on the disk and **Manage Pool** on the selected pool.
Change folders	**Manage Persistent Disks** on the source and target folders.
Recreate desktop	**Manage Persistent Disks** on the disk and **Manage Pool** on the last pool.
Import from vCenter	**Manage Persistent Disks** on the folder and **Manage Pool** on the pool.
Delete a disk	**Manage Persistent Disks** on the disk.

Privileges for Managing Users and Administrators

An administrator must have certain privileges to manage users and administrators in View Administrator.

Table 2-13 lists common user and administrator management tasks and shows the privileges that are required to perform each task. You manage users on the Users and Groups page in View Administrator. You manage administrators on the Global Administrators View page in View Administrator.

Table 2-13. User and Administrator Management Tasks and Privileges

Task	Required Privileges
Update general user information	**Manage Global Configuration and Policies**
Send messages to desktop users	**Manage Remote Sessions** on the desktop.
Add an administrator user or group	**Manage Roles and Permissions**
Add, modify, or delete an administrator permission	**Manage Roles and Permissions**
Add, modify, or delete an administrator role	**Manage Roles and Permissions**

Privileges for General Administration Tasks and Commands

An administrator must have certain privileges to perform general administration tasks and run command line utilities.

Table 2-14 shows the privileges that are required to perform general administration tasks and run command line utilities.

Table 2-14. Privileges for General Administration Tasks and Commands

Task	Required Privileges
Add or delete a folder	Must have the Administrators role on the root folder.
Manage ThinApp applications and settings in View Administrator	Must have the Administrators role on the root folder.
View and modify View Transfer Server instances and the Transfer Server repository	Must have the Administrators role on the root folder.
Install View Agent on an unmanaged desktop source, such as a physical system, standalone virtual machine, or terminal server	**Register Agent**
View or modify configuration settings (except for administrators) in View Administrator	**Manage Global Configuration and Policies**
Run all PowerShell commands and command line utilities except for `vdmadmin` and `vdmimport`.	**Direct Interaction**
Use the `vdmadmin` and `vdmimport` commands	Must have the Administrators role on the root folder.
Use the `vdmexport` command	Must have the Administrators role or the Administrators (Read only) role on the root folder.

Best Practices for Administrator Users and Groups

To increase the security and manageability of your View environment, you should follow best practices when managing administrator users and groups.

- Because the Administrators role contains all privileges, assign it to a single user or to a limited set of users.
- Choose a local Windows user or group to have the Administrators role.
- Create new user groups for administrators. Avoid using Windows built-in groups or other existing groups that might contain additional users or groups.
- Because it is highly visible and easily guessed, avoid using the name Administrator when creating administrator users and groups.
- Create folders to segregate sensitive desktops. Delegate the administration of those folders to a limited set of users.
- Create separate administrators that can modify global policies and View configuration settings.

Preparing Unmanaged Desktop Sources

3

Users can access View desktops delivered by machines that are not managed by vCenter Server. These unmanaged desktop sources can include physical computers, terminal servers, and virtual machines running on VMware Server and other virtualization platforms. You must prepare an unmanaged desktop source to deliver View desktop access.

This chapter includes the following topics:

Prepare an Unmanaged Desktop Source for View Desktop Deployment

You must perform certain tasks to prepare an unmanaged desktop source for View desktop deployment.

Prerequisites

- Verify that you have administrative rights on the unmanaged desktop source.
- To make sure that View desktop users are added to the local Remote Desktop Users group of the unmanaged desktop source, create a restricted Remote Desktop Users group in Active Directory. See the *VMware View Installation* document for more information.

Procedure

1 Power on the unmanaged desktop source and verify that it is accessible to the View Connection Server instance.

2 Join the unmanaged desktop source to the Active Directory domain for your View desktops.

3 Configure the Windows firewall to allow Remote Desktop connections to the unmanaged desktop source.

What to do next

Install View Agent on the unmanaged desktop source. See "Install View Agent on an Unmanaged Desktop Source," on page 41.

Install View Agent on an Unmanaged Desktop Source

You must install View Agent on an all unmanaged desktop sources. View cannot manage an unmanaged desktop source unless View Agent is installed.

To install View Agent on multiple Windows physical computers without having to respond to wizard prompts, you can install View Agent silently. See "Install View Agent Silently," on page 51.

Prerequisites

- Verify that you have administrative rights on the unmanaged desktop source.
- Familiarize yourself with the View Agent custom setup options for unmanaged desktop sources. See "View Agent Custom Setup Options for Unmanaged Desktop Sources," on page 43.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the *VMware View Architecture Planning* document for more information.
- Download the View Agent installer file from the VMware product page at http://www.vmware.com/products/.

Procedure

1 To start the View Agent installation program, double-click the installer file.

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

2 Accept the VMware license terms.

3 Select your custom setup options.

4 Accept or change the destination folder.

5 In the **Server** text box, type the host name or IP address of a View Connection Server host.

During installation, the installer registers the unmanaged desktop source with this View Connection Server instance. After registration, the specified View Connection Server instance, and any additional instances in the same View Connection Server group, can communicate with the unmanaged desktop source.

6 Select an authentication method to register the unmanaged desktop source with the View Connection Server instance.

Option	Action
Authenticate as the currently logged in user	The **Username** and **Password** text boxes are disabled and you are logged in to the View Connection Server instance with your current username and password.
Specify administrator credentials	You must provide the username and password of a View Connection Server administrator in the **Username** and **Password** text boxes.

7 Follow the prompts in the View Agent installation program and finish the installation.

8 If you selected the USB redirection option, restart the unmanaged desktop source to enable USB support.

In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the unmanaged desktop source.

The VMware View Agent service is started on the unmanaged desktop source.

If Windows Media Player is not installed, the View Agent installation program does not install the multimedia redirection (MMR) feature. If you install Windows Media Player after installing View Agent, you can install the MMR feature by running the View Agent installation program again and selecting the Repair option.

What to do next

Use the unmanaged desktop source to create a View desktop. See "Manual Desktop Pools," on page 93.

View Agent Custom Setup Options for Unmanaged Desktop Sources

When you install View Agent on an unmanaged desktop source, you can select certain custom setup options.

Table 3-1. View Agent Custom Setup Options for Unmanaged Desktop Sources

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. Windows 2003 and Windows 2008 do not support USB redirection. **NOTE** You can use group policy settings to disable USB redirection for specific users.
PCoIP Server	Lets users connect to the View desktop with the PCoIP display protocol. **NOTE** On Windows Vista, if you install the PCoIP Server component, the Windows group policy **Disable or enable software Secure Attention Sequence** is enabled and set to **Services** and **Ease of Access applications**. If you change this setting, single sign-on does not work correctly.
PCoIP Smartcard	Lets users authenticate with smart cards when they use the PCoIP display protocol.

Creating and Preparing Virtual Machines

4

You can use virtual machines managed by vCenter Server to provision and deploy View desktops. You can use a virtual machine managed by vCenter Server as a template for an automated pool, a parent for a linked-clone pool, or a desktop source in a manual pool. You must prepare virtual machines to deliver View desktop access.

This chapter includes the following topics:

Creating Virtual Machines for View Desktop Deployment

The initial virtual machine establishes a virtual hardware profile and operating system to be used for rapid deployment of View desktops.

1 Create a Virtual Machine for View Desktop Deployment on page 45

You use vSphere Client to create virtual machines in vCenter Server for View desktops.

2 Install a Guest Operating System on page 47

After you create a virtual machine, you must install a guest operating system.

3 Prepare a Guest Operating System for View Desktop Deployment on page 48

You must perform certain tasks to prepare a guest operating system for View desktop deployment.

Create a Virtual Machine for View Desktop Deployment

You use vSphere Client to create virtual machines in vCenter Server for View desktops.

Prerequisites

- Upload an ISO image file of the guest operating system to a datastore on your ESX server.

- Familiarize yourself with the custom configuration parameters for virtual machines. See "Virtual Machine Custom Configuration Parameters," on page 46.

Procedure

1 In vSphere Client, log in to the vCenter Server system.

2 Select **File > New > Virtual Machine** to start the New Virtual Machine wizard.

3 Select **Custom** and configure custom configuration parameters.

4 Select **Edit the virtual machine settings before completion** and click **Continue** to configure hardware settings.

   a Add a CD/DVD drive, set the media type to use an ISO image file, select the ISO image file of the guest operating system that you uploaded to your datastore, and select **Connect at power on**.

   b If you are installing a Windows XP guest operating system, add a floppy drive and set the **Device Type** to **Client Device**.

   c Set **Power-on Boot Delay** to 10,000 milliseconds.

5 Click **Finish** to create the virtual machine.

What to do next

Install a guest operating system on the virtual machine.

Virtual Machine Custom Configuration Parameters

You can use virtual machine custom configuration parameters as baseline settings when you create a virtual machine for View desktop deployment.

If you use View Administrator as your View desktop manager for deploying pooled desktops, you can change these settings when deploying template-based View desktops.

Table 4-1. Custom Configuration Parameters

Parameter	Description and Recommendations
`Name and Location`	The name and location of the virtual machine. If you plan to use the virtual machine as a template, assign a generic name. The location can be any folder within your datacenter inventory.
`Host/Cluster`	The ESX server or cluster of server resources that will run the virtual machine. If you plan to use the virtual machine as a template, the location of the initial virtual machine does not necessarily specify where future virtual machines created from template will reside.
`Resource Pool`	If the physical ESX server resources are divided into resource pools, you can assign them to the virtual machine.
`Datastore`	The location of files associated with the virtual machine.
`Hardware Machine Version`	If you create the virtual machine on an ESXi 5.0 or later host or cluster, you can select virtual hardware version 8 or 7. Version 8 provides greater virtual machine functionality. For desktops that run in local mode, you must create virtual machines that use hardware version 7. Virtual machines that use hardware version 8 cannot be checked out for use in local mode. If the host or cluster is ESX/ESXi 4.0 or later, you can select virtual hardware version 7 only.

Table 4-1. Custom Configuration Parameters (Continued)

Parameter	Description and Recommendations
`Guest Operating System`	The type of operating system that you will install in the virtual machine.
`CPUs`	The number of virtual processors in the virtual machine. For most guest operating systems, a single processor is sufficient.
`Memory`	The amount of memory to allocate to the virtual machine. In most cases, 512MB is sufficient.
`Network`	The number of virtual network adapters (NICs) in the virtual machine. One NIC is usually sufficient. The network name should be consistent across virtual infrastructures. An incorrect network name in a template can cause failures during the instance customization phases. When you install View Agent on a virtual machine that has more than one NIC, you must configure the subnet that View Agent uses. See "Configure a Virtual Machine with Multiple NICs for View Agent," on page 56 for more information. **IMPORTANT** For Windows 7 and Windows Vista operating systems, you must select the VMXNET 3 network adapter. Using the default E1000 adapter can cause customization timeout errors on virtual machines. To use the VMXNET 3 adapter, you must install a Microsoft hotfix patch: ■ For Windows 7 SP1: http://support.microsoft.com/kb/2550978 ■ For Windows 7 versions previous to SP1: http://support.microsoft.com/kb/2344941
`SCSI Controller`	The type of SCSI adapter to use with the virtual machine. For Windows 7 and Windows XP guest operating systems, you should specify the LSI Logic adapter. The LSI Logic adapter has improved performance and works better with generic SCSI devices. LSI Logic SAS is available only for virtual machines with hardware version 7. **NOTE** Windows XP does not include a driver for the LSI Logic adapter. You must download the driver from the LSI Logic Web site.
`Select a Disk`	The disk to use with the virtual machine. Create a new virtual disk based on the amount of local storage that you decide to allocate to each user. Allow enough storage space for the OS installation, patches, and locally installed applications. To reduce the need for disk space and management of local data, you should store the user's information, profile, and documents on network shares rather than on a local disk.

Install a Guest Operating System

After you create a virtual machine, you must install a guest operating system.

Prerequisites

- Verify that an ISO image file of the guest operating system is on a datastore on your ESX server.
- Verify that the CD/DVD drive in the virtual machine points to the ISO image file of the guest operating system and that the CD/DVD drive is configured to connect at power on.

- If you are installing Windows XP and you selected the LSI Logic adapter for the virtual machine, download the LSI20320-R controller driver from the LSI Logic Web site, create a floppy image (`.flp`) file that contains the driver, and upload the file to a datastore on your ESX server.

Procedure

1 In vSphere Client, log in to the vCenter Server system where the virtual machine resides.

2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

Because you configured the CD/DVD drive to point to the ISO image of the guest operating system and to connect at power on, the guest operating system installation process begins automatically.

3 Click the **Console** tab and follow the installation instructions provided by the operating system vendor.

4 If you are installing Windows XP and you selected the LSI Logic adapter for the virtual machine, install the LSI Logic driver during the Windows setup process.

a Press F6 to select additional SCSI drivers.

b Type **S** to specify an additional device.

c On the vSphere Client toolbar, click **Connect Floppy** to select the LSI Logic driver floppy image (`.flp`) file.

d Return to the Windows Setup screen and press Enter to continue the Windows setup process.

e When the Windows setup process has finished, disconnect the virtual floppy disk drive.

5 If you are installing Windows 7, activate Windows online.

What to do next

Prepare the guest operating system for View desktop deployment.

Prepare a Guest Operating System for View Desktop Deployment

You must perform certain tasks to prepare a guest operating system for View desktop deployment.

Prerequisites

- Create a virtual machine and install a guest operating system.
- Configure an Active Directory domain controller for your View desktops. See the *VMware View Installation* document for more information.
- To make sure that View desktop users are added to the local Remote Desktop Users group of the virtual machine, create a restricted Remote Desktop Users group in Active Directory. See the *VMware View Installation* document for more information.
- Verify that Remote Desktop Services, called Terminal Services on Windows XP systems, are started on the virtual machine. Remote Desktop Services are required for View Agent installation, SSO, and other View operations. You can disable RDP access to your View desktops by configuring desktop pool settings and group policy settings. See "Prevent Access to View Desktops Through RDP," on page 110.
- Verify that you have administrative rights on the guest operating system.

Procedure

1 In vSphere Client, log in to the vCenter Server system where the virtual machine resides.

2 Right-click the virtual machine, select **Power**, and select **Power On** to start the virtual machine.

3 Right-click the virtual machine, select **Guest**, and select **Install/Upgrade VMware Tools** to install the latest version of VMware Tools.

4 Use the VMware Tools time synchronization function to ensure that the virtual machine is synchronized to ESX.

   ESX must synchronize to an external NTP source, for example, the same time source as Active Directory.

   Disable other time synchronization mechanisms such as Windows Time Service.

   The VMware Tools online help provides information on configuring time synchronization between guest and host.

5 Install service packs and updates.

6 Install antivirus software.

7 Install other applications and software, such as Windows Media Player if you are using MMR and smart card drivers if you are using smart card authentication.

   On Windows XP systems, install all third-party applications and software (except Microsoft .NET Framework) before you install View Agent.

   IMPORTANT If you are installing Microsoft .NET Framework, you must install it after you install View Agent.

8 If View clients will connect to the virtual machine with the PCoIP display protocol, set the power option **Turn off the display** to **Never**.

   If you do not disable this setting, the display will appear to freeze in its last state when power savings mode starts.

9 If a proxy server is used in your network environment, configure network proxy settings.

10 Configure network connection properties.

   a Assign a static IP address or specify that an IP address is assigned by a DHCP server.

      View does not support link-local (169.254.x.x) addresses for View desktops.

   b Set the preferred and alternate DNS server addresses to your Active Directory server address.

11 Join the virtual machine to the Active Directory domain for your View desktops.

   A parent virtual machine that you use for View Composer must either belong to the same Active Directory domain as the domain that the linked-clone desktops will join or be a member of the local WORKGROUP.

12 Configure the Windows firewall to allow Remote Desktop connections to the virtual machine.

13 (Optional) Disable Hot Plug PCI devices.

   This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the virtual machine.

14 (Optional) Configure user customization scripts.

What to do next

Install View Agent. See "Install View Agent on a Virtual Machine," on page 49.

Install View Agent on a Virtual Machine

You must install View Agent on virtual machines that are managed by vCenter Server so that View Connection Server can communicate with them. Install View Agent on all virtual machines that you use as templates for automated desktop pools, parents for linked-clone desktop pools, and desktop sources in manual desktop pools.

To install View Agent on multiple Windows virtual machines without having to respond to wizard prompts, you can install View Agent silently. See "Install View Agent Silently," on page 51.

Prerequisites

- Prepare the guest operating system for View desktop deployment. See "Prepare a Guest Operating System for View Desktop Deployment," on page 48.
- Download the View Agent installer file from the VMware product page at http://www.vmware.com/products/.
- Verify that you have administrative rights on the virtual machine.
- Familiarize yourself with the View Agent custom setup options. See "View Agent Custom Setup Options," on page 51.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the *VMware View Architecture Planning* document for more information.
- If you select the View Composer Agent custom setup option, verify that you have a license to use View Composer.

Procedure

1 To start the View Agent installation program, double-click the installer file.

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

2 Accept the VMware license terms.

3 Select your custom setup options.

  To deploy linked-clone desktops, select the **View Composer Agent** option.

4 Accept or change the destination folder.

5 Follow the prompts in the View Agent installation program and finish the installation.

  NOTE If you did not enable Remote Desktop support during guest operating system preparation, the View Agent installation program prompts you to enable it. If you do not enable Remote Desktop support during View Agent installation, you must enable it manually after the installation is finished.

6 If you selected the USB redirection option, restart the virtual machine to enable USB support.

  In addition, the **Found New Hardware** wizard might start. Follow the prompts in the wizard to configure the hardware before you restart the virtual machine.

The VMware View Agent service is started on the virtual machine.

If you selected the **View Composer Agent** option, the VMware View Composer Guest Agent Server service is started on the virtual machine.

If Windows Media Player is not installed, the View Agent installation program does not install the multimedia redirection (MMR) feature. If you install Windows Media Player after installing View Agent, you can install the MMR feature by running the View Agent installation program again and selecting the Repair option.

What to do next

If the virtual machine has multiple NICs, configure the subnet that View Agent uses. See "Configure a Virtual Machine with Multiple NICs for View Agent," on page 56.

View Agent Custom Setup Options

When you install View Agent on a virtual machine, you can select custom setup options.

Table 4-2. View Agent Custom Setup Options

Option	Description
USB Redirection	Gives users access to locally connected USB devices on their desktops. Windows 2000 does not support USB redirection. NOTE You can use group policy settings to disable USB redirection for specific users.
View Composer Agent	Lets View Agent run on the linked-clone desktops that are deployed from this virtual machine.
Virtual Printing	Lets users print to any printer available on their Windows client computers. Users do not have to install additional drivers on their desktops.
PCoIP Server	Lets users connect to the View desktop using the PCoIP display protocol. Installing the PCoIP Server feature disables sleep mode on Windows 7 and Windows Vista desktops and standby mode on Windows XP desktops. When a user navigates to the Power Options or Shut Down menu, sleep mode or standby mode is inactive. Desktops do not go into sleep or standby mode after a default period of inactivity. Desktops remain in active mode. NOTE If you install the PCoIP Server feature on Windows Vista, the Windows group policy **Disable or enable software Secure Attention Sequence** is enabled and set to **Services** and **Ease of Access applications**. If you change this setting, single sign-on does not work correctly.
PCoIP Smartcard	Lets users authenticate with smart cards when they use the PCoIP display protocol.
View Persona Management	Synchronizes the user profile on the local desktop with a remote profile repository, so that users have access to their profiles whenever they log in to a desktop.

Install View Agent Silently

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

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

Prerequisites

- Prepare the guest operating system for View desktop deployment. See "Prepare a Guest Operating System for View Desktop Deployment," on page 48.
- Download the View Agent installer file from the VMware product page at http://www.vmware.com/products/.

  The installer filename is `VMware-viewagent-y.y.y-xxxxxx.exe` or `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, where *y.y.y* is the version number and *xxxxxx* is the build number.
- Verify that you have administrative rights on the virtual machine or physical PC.

- Familiarize yourself with the View Agent custom setup options. See "View Agent Custom Setup Options," on page 51.
- If you select the View Composer Agent custom setup option, verify that you have a license to use View Composer.
- Familiarize yourself with the MSI installer command-line options. See "Microsoft Windows Installer Command-Line Options," on page 52.
- Familiarize yourself with the silent installation properties available with View Agent. See "Silent Installation Properties for View Agent," on page 54.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the *VMware View Architecture Planning* document for more information.

Procedure

1 Open a Windows command prompt on the virtual machine or physical PC.

2 Type the installation command on one line.

This example installs View Agent in a virtual machine that is managed by vCenter Server. The installer configures the PCoIP, View Composer Agent, Virtual Printing, and USB redirection custom setup options.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
ADDLOCAL=Core,PCoIP,SVIAgent,ThinPrint,USB"
```

This example installs View Agent on an unmanaged computer and registers the desktop with the specified View Connection Server, `cs1.companydomain.com`. The installer configures the SSO, Virtual Printing, and USB redirection custom setup options.

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

The VMware View Agent service is started on the virtual machine.

If you selected the **View Composer Agent** option, the VMware View Composer Guest Agent Server service is started on the virtual machine.

If Windows Media Player is not installed, the View Agent installation program does not install the multimedia redirection (MMR) feature. If you install Windows Media Player after installing View Agent, you can install the MMR feature by running the View Agent installation program again and selecting the Repair option.

What to do next

If the virtual machine has multiple NICs, configure the subnet that View Agent uses. See "Configure a Virtual Machine with Multiple NICs for View Agent," on page 56.

Microsoft Windows Installer Command-Line Options

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

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

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

At the command line, you must enter command-line options that control the installer's bootstrap program.

Table 4-3. Command-Line Options for a View Component's Bootstrap Program

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

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

Table 4-4. MSI Command-Line Options and MSI Properties

MSI Option or Property	Description
/qn	Instructs the MSI installer not to display the installer wizard pages. For example, you might want to install View Agent silently and use only default setup options and features: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" Alternatively, you can use the /qb option to display the wizard pages in a noninteractive, automated installation. As the installation proceeds, the wizard pages are displayed, but you cannot respond to them. The /qn or /qb option is required to run a silent installation.
INSTALLDIR	Specifies an alternative installation path for the View component. Use the format *INSTALLDIR=path* to specify an installation path. You can ignore this MSI property if you want to install the View component in the default path. This MSI property is optional.
ADDLOCAL	Determines the component-specific features to install. In an interactive installation, the View installer displays custom setup options to select. The MSI property, ADDLOCAL, lets you specify these setup options on the command line. To install all available custom setup options, enter ADDLOCAL=ALL. For example: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" If you do not use the MSI property, ADDLOCAL, the default setup options are installed. To specify individual setup options, enter a comma-separated list of setup option names. Do not use spaces between names. Use the format *ADDLOCAL=value,value,value...*. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **NOTE** The Core feature is required in View Agent. This MSI property is optional.

Table 4-4. MSI Command-Line Options and MSI Properties (Continued)

MSI Option or Property	Description
REBOOT	You can use the REBOOT=ReallySuppress option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.
/l*v *log_file*	Writes logging information into the specified log file with verbose output. For example: /l*v ""%TEMP%\vmmsi.log"" This example generates a detailed log file that is similar to the log generated during an interactive installation. You can use this option to record custom features that might apply uniquely to your installation. You can use the recorded information to specify installation features in future silent installations. The /l*v option is optional.

Silent Installation Properties for View Agent

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

Table 4-5 shows the View Agent silent installation properties that you can use at the command-line.

Table 4-5. MSI Properties for Silently Installing View Agent

MSI Property	Description	Default Value
INSTALLDIR	The path and folder in which the View Agent software is installed. For example: INSTALLDIR=""D:\abc\my folder"" The sets of two double quotes that enclose the path permit the MSI installer to ignore the space in the path. This MSI property is optional.	%ProgramFiles %\VMware\VMware View\Agent
RDPCHOICE	Determines whether to enable Remote Desktop Protocol (RDP) on the desktop. A value of 1 enables RDP. A value of 0 leaves the RDP setting disabled. This MSI property is optional.	1
VDM_VC_MANAGED_AGENT	Determines whether vCenter Server manages the virtual machine on which View Agent is installed. A value of 1 configures the desktop as a vCenter Server-managed virtual machine. A value of 0 configures the desktop as unmanaged by vCenter Server. This MSI property is required.	None
VDM_SERVER_NAME	The host name or IP address of the View Connection Server computer on which the View Agent installer registers an unmanaged desktop. This property applies to unmanaged desktops only. For example: VDM_SERVER_NAME=10.123.01.01 This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None

Table 4-5. MSI Properties for Silently Installing View Agent (Continued)

MSI Property	Description	Default Value
VDM_SERVER_USERNAME	The user name of the administrator on the View Connection Server computer. This MSI property applies to unmanaged desktops only. For example: VDM_SERVER_USERNAME=admin.companydomain.com This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None
VDM_SERVER_PASSWORD	The View Connection Server administrator user password. For example: VDM_SERVER_PASSWORD=secret This MSI property is required for unmanaged desktops. Do not use this MSI property for virtual-machine desktops that are managed by vCenter Server.	None

In a silent installation command, you can use the MSI property, ADDLOCAL=, to specify custom features that the View Agent installer configures. Each silent-installation feature corresponds to a custom setup option that you can select during an interactive installation.

Table 4-6 shows the View Agent features you can type at the command line and the corresponding custom setup options.

Table 4-6. View Agent Silent Installation Features and Interactive Custom Setup Options

Silent Installation Feature	Custom Setup Option in an Interactive Installation
Core. If you specify individual features with the MSI property, ADDLOCAL=, you must include Core. If you specify ADDLOCAL=ALL, all features, including Core, are installed.	None. During an interactive installation, the core View Agent functions are installed by default.
SVIAgent	View Composer Agent
ThinPrint	Virtual Printing
ThinPrintPCoIP	Virtual Printing with PCoIP
PCoIP	PCoIP Protocol
USB	USB Redirection
VPA	View Persona Management
VmVideo	In an interactive installation, this feature is not a separate custom setup option.
VmwAudio	In an interactive installation, this feature is not a separate custom setup option.
SmartCard	In an interactive installation, the SmartCard feature is not a separate custom setup option.
VMCI	In an interactive installation, the VMCI feature is not a separate custom setup option.

For details about the custom setup options, see "View Agent Custom Setup Options," on page 51.

Configure a Virtual Machine with Multiple NICs for View Agent

When you install View Agent on a virtual machine that has more than one NIC, you must configure the subnet that View Agent uses. The subnet determines which network address View Agent provides to the View Connection Server instance for client protocol connections.

Procedure

- On the virtual machine on which View Agent is installed, open a command prompt, type **regedit.exe**, and create a registry entry to configure the subnet.

  For example: **HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = *n.n.n.n/m* (REG_SZ)**

  In this example, *n.n.n.n* is the TCP/IP subnet and *m* is the number of bits in the subnet mask.

Optimize Windows Guest Operating System Performance

You can perform certain steps to optimize guest operating system performance for View desktop deployment. The steps apply to all Windows operating systems. All of the steps are optional.

These recommendations include turning off the screen saver and not specifying a sleep timer. Your organization might require the use of screen savers. For example, you might have a GPO-managed security policy that locks a desktop a certain time after the screen saver starts. In this case, use a blank screen saver.

Prerequisites

Prepare a guest operating system for View desktop deployment.

Procedure

- Disable any unused ports, such as COM1, COM2, and LPT.
- Adjust display properties.
  a. Choose a basic theme.
  b. Set the background to a solid color.
  c. Set the screen saver to **None**.
  d. Verify that hardware acceleration is enabled.
- Select a high-performance power option and do not specify a sleep timer.
- Disable the Indexing Service component.

  NOTE Indexing improves searches by cataloging files. Do not disable this feature for users that search often.
- Remove or minimize System Restore points.
- Turn off system protection on `C:\`.
- Disable any unnecessary services.
- Set the sound scheme to **No Sounds**.
- Set visual effects to **Adjust for best performance**.
- Open Windows Media Player and use the default settings.
- Turn off automatic computer maintenance.
- Adjust performance settings for best performance.

- Delete any hidden uninstall folders in `C:\Windows`, such `$NtUninstallKB893756$`.
- Delete all event logs.
- Run Disk Cleanup to remove temporary files, empty the Recycle Bin, and remove system files and other items that are no longer needed.
- Run Disk Defragmenter to rearrange fragmented data.

What to do next

For Windows 7 guest operating systems, perform additional optimization tasks. See "Optimize Windows 7 Guest Operating System Performance," on page 57.

Optimize Windows 7 Guest Operating System Performance

You can perform additional steps to optimize Windows 7 guest operating system performance for View desktop deployment. All of the steps are optional.

Prerequisites

Perform the guest operating system optimization steps that apply to all Windows operating systems. See "Optimize Windows Guest Operating System Performance," on page 56.

Procedure

1. Uninstall Tablet PC Components, unless this feature is needed.
2. Disable IPv6, unless it is needed.
3. Use the File System Utility (`fsutil`) command to disable the setting that keeps track of the last time a file was accessed.

   For example: `fsutil behavior set disablelastaccess 1`
4. Start the Registry Editor (`regedit.exe`) and change the **TimeOutValue** REG_DWORD in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk` to **`0x000000be(190)`**.
5. Shut down the guest operating system and power off the virtual machine.
6. Change the virtual machine video card RAM setting to 128 MB.
7. Power on the virtual machine.

What to do next

See "Optimizing Windows 7 for Linked-Clone Desktops," on page 57 for information on disabling certain Windows 7 services and tasks to reduce the growth of View Composer linked-clone desktops. Disabling certain services and tasks can also result in performance benefits for full virtual machines.

Optimizing Windows 7 for Linked-Clone Desktops

By disabling certain Windows 7 services and tasks, you can reduce the growth of View Composer linked-clone desktops. Disabling certain services and tasks can also result in performance benefits for full virtual machines.

Benefits of Disabling Windows 7 Services and Tasks

Windows 7 schedules services and tasks that can cause View Composer linked clones to grow, even when the linked-clone desktops are idle. The incremental growth of linked-clone OS disks can undo the storage savings that you achieve when you first create the linked-clone desktops. You can reduce linked-clone growth by disabling these Windows 7 services.

Windows 7 introduces new services and schedules older services, such as disk defragmentation, to run by default. These services run in the background if you do not disable them.

Services that affect OS disk growth also generate input/output operations per second (IOPS) on the Windows 7 virtual machines. Disabling these services can reduce IOPS and improve performance on full virtual machines and linked clones.

Disabling certain services also might benefit Windows XP and Windows Vista operating systems.

These best practices for optimizing Windows 7 apply to most user environments. However, you must evaluate the effect of disabling each service on your users, applications, and desktops. You might require certain services to stay active.

For example, disabling Windows Update Service makes sense if you refresh and recompose the linked-clone desktops. A refresh operation restores the OS disks to their last snapshots, deleting all automatic Windows updates since the last snapshots were taken. A recompose operation recreates the OS disks from a new snapshot that can contain the current Windows updates, making automatic Windows updates redundant.

If you do not use refresh and recompose regularly, you might decide to keep Windows Update Service active.

Overview of Windows 7 Services and Tasks That Cause Linked-Clone Growth

Certain Windows 7 services and tasks can cause linked-clone OS disks to grow incrementally every few hours, even when the linked-clone desktops are idle. If you disable these services and tasks, you can control the OS disk growth.

Services that affect OS disk growth also generate IOPS on the Windows 7 virtual machines. You can evaluate the benefits of disabling these services on full virtual machines as well as linked clones.

Before you disable the Windows 7 services that are shown in Table 4-7, verify that you took the optimization steps in "Optimize Windows Guest Operating System Performance," on page 56 and "Optimize Windows 7 Guest Operating System Performance," on page 57.

Table 4-7. Impact of Windows 7 Services and Tasks on OS Disk Growth and IOPS When OS Is Left Idle

Service or Task	Description	Default Occurrence or Startup	Impact on Linked-Clone OS Disks	Impact on IOPS	Turn Off This Service or Task?
Windows Hibernation	Provides a power-saving state by storing open documents and programs in a file before the computer is powered off. The file is reloaded into memory when the computer is restarted, restoring the state when the hibernation was invoked.	Default power-plan settings disable hibernation.	High. By default, the size of the hibernation file, `hiberfil.sys`, is the same as the installed RAM on the virtual machine. This feature affects all guest operating systems.	High. When hibernation is triggered, the system writes a `hiberfil.sys` file the size of the installed RAM.	Yes Hibernation provides no benefit in a virtual environment. For instructions, see "Disable Windows Hibernation in the Parent Virtual Machine," on page 66..
Windows Scheduled Disk Defragmentation	Disk defragmentation is scheduled as a background process.	Once a week	High. Repeated defragmentation operations can increase the size of linked-clone OS disks by several GB and do little to make disk access more efficient on linked clones.	High	Yes

Table 4-7. Impact of Windows 7 Services and Tasks on OS Disk Growth and IOPS When OS Is Left Idle (Continued)

Service or Task	Description	Default Occurrence or Startup	Impact on Linked-Clone OS Disks	Impact on IOPS	Turn Off This Service or Task?
Windows Update Service	Detects, downloads, and installs updates for Windows and other programs.	Automatic startup	Medium to high. Causes frequent writes to the linked-clones' OS disks because update checks occur often. The impact depends on the updates that are downloaded.	Medium to high	Yes, if you use View Composer recompose to install Windows updates and refresh to return OS disks to their original snapshots.
Windows Diagnostic Policy Service	Detects, troubleshoots, and resolves problems in Windows components. If you stop this service, diagnostics no longer function.	Automatic startup	Medium to high. The service is triggered on demand. The write frequency varies, depending on demand.	Small to medium	Yes, if you do not need the diagnostic tools to function on the desktops.
Prefetch/Superfetch	Stores specific information about applications that you run to help them start faster. This feature was introduced in Windows XP.	Always on, unless it is disabled.	Medium Causes periodic updates to its layout and database information and individual prefetch files, which are generated on demand.	Medium	Yes, if application startup times are acceptable after you disable this feature.
Windows Registry Backup (`RegIdleBackup`)	Automatically backs up the Windows registry when the system is idle.	Every 10 days at 12:00 am	Medium. Each time this task runs, it generates registry backup files.	Medium.	Yes. There is no need for Windows Registry Backup. To restore registry data, you can use the View Composer refresh operation.
System Restore	Reverts the Windows system to a previous, healthy state.	When Windows starts up and once a day thereafter.	Small to medium. Captures a system restore point whenever the system detects that it is needed. When the linked clone is idle, this overhead is small.	No major impact.	Yes Although its impact is small, this task is redundant if you use View Composer refresh to return OS disks to their original snapshots.

Table 4-7. Impact of Windows 7 Services and Tasks on OS Disk Growth and IOPS When OS Is Left Idle (Continued)

Service or Task	Description	Default Occurrence or Startup	Impact on Linked-Clone OS Disks	Impact on IOPS	Turn Off This Service or Task?
Windows Defender	Provides anti-spyware features.	When Windows starts up. Performs a quick scan once a day. Checks for updates before each scan.	Medium to high. Performs definition updates, scheduled scans, and scans that are started on demand.	Medium to high.	Yes, if other anti-spyware software is installed.
Microsoft Feeds Synchronization task (`msfeedssync.exe`)	Periodically updates RSS feeds in Windows Internet Explorer 7 and 8 Web browsers. This task updates RSS feeds that have automatic RSS feeds synchronization turned on. The process appears in Windows Task Manager only when Internet Explorer 7 or 8 is running.	Once a day.	Medium. Affects OS-disk growth if persistent disks are not configured. If persistent disks are configured, the impact is diverted to the persistent disks.	Medium	Yes, if your users do not require automatic RSS feed updates on their desktops.

Disable Scheduled Disk Defragmentation on Windows 7 Parent Virtual Machines

Before you create linked clones, you must disable scheduled defragmentations on Windows 7 parent virtual machines. Windows 7 schedules weekly disk defragmentations by default. Repeated defragmentation operations significantly increase the size of linked-clone OS disks and do not make disk access more efficient on linked clones.

When you create a linked-clone pool from the parent virtual machine, the linked clones share the replica's disk. Subsequent defragmentation operations do not affect the replica's disk, which is read-only. Instead, defragmentations expand each clone's OS disk.

As a best practice, defragment the parent virtual machine one time, before you take a snapshot and create the pool. The linked clones benefit from the defragmentation because they share the replica's optimized, read-only disk.

Prerequisites

- Verify that the applications that you intend to deploy to the linked clones are installed on the virtual machine.
- Verify that View Agent with View Composer Agent is installed on the virtual machine.

Procedure

1. In vSphere Client, select the parent virtual machine and select **Open Console**.
2. Log in to the Windows 7 guest operating system as an administrator.
3. Click **Start** and type **`defrag`** in the **Search programs and files** box.
4. In the Programs pane, click **Disk Defragmenter**.

5 In the **Disk Defragmenter** dialog box, click **Defragment disk**.

The Disk Defragmenter consolidates defragmented files on the virtual machine's hard disk.

6 In the **Disk Defragmenter** dialog box, click **Configure schedule**.

7 Deselect **Run on a schedule (recommended)** and click **OK**.

Defragmentation operations will not take place on linked-clone virtual machines that are created from this parent virtual machine.

Disable the Windows Update Service on Windows 7 Virtual Machines

Disabling the Windows Update Service can reduce the number of files that are created and writes that occur when updates are downloaded and installed. This action can reduce linked-clone growth and reduce IOPS in linked clones and full virtual machines.

Disable Windows Update Service if you refresh and recompose the linked-clone desktops. A refresh operation restores the OS disks to their original snapshots, deleting the automatic Windows updates. A recompose operation recreates the OS disks from a new snapshot that can contain Windows updates, making automatic Windows updates redundant.

Do not disable the Windows Update Service if you do not use recompose to install Windows updates in the linked clones.

Prerequisites

Verify that the most recent Windows updates are downloaded and installed on the virtual machine.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start > Control Panel > System and Security > Turn automatic updating on or off**.

4 In the Important updates menu, select **Never check for updates**.

5 Deselect **Give me recommended updates the same way I receive important updates**.

6 Deselect **Allow all users to install updates on this computer** and click **OK**.

Disable the Diagnostic Policy Service on Windows 7 Virtual Machines

Disabling the Windows Diagnostic Policy Service can minimize the number of system writes and reduce the growth of linked-clone desktops.

Do no disable the Windows Diagnostic Policy Service if your users require the diagnostic tools on their desktops.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Services** and click **Open**.

5 Double-click **Diagnostic Policy Service**.

6 In the Diagnostic Policy Service Properties (Local Computer) dialog, click **Stop**.

7 In the Startup type menu, select **Disabled**.

8 Click **OK**.

Disable the Prefetch and Superfetch Features on Windows 7 Virtual Machines

By disabling the Windows prefetch and superfetch features, you can avoid generating prefetch files and the overhead associated with prefetch and superfetch operations. This action can reduce the growth of linked-clone desktops and minimize IOPS on full virtual machines and linked clones.

To disable the prefetch and superfetch features, you must edit a Windows registry key and disable the Prefetch service on the virtual machine.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the Windows Registry Editor on Windows 7.

Procedure

1 Start the Windows Registry Editor on the local Windows 7 virtual machine.

2 Navigate to the registry key called **PrefetchParameters**.

The registry key is located in the following path:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`.

3 Set the **EnablePrefetcher** and **EnableSuperfetch** values to **`0`**.

4 Click **Start > Control Panel > System and Security > Administrative Tools**.

5 Select **Services** and click **Open**.

6 Double-click the **Superfetch** service.

7 In the Superfetch Properties (Local Computer) dialog, click **Stop**.

8 In the Startup type menu, select **Disabled**.

9 Click **OK**.

Disable Windows Registry Backup on Windows 7 Virtual Machines

Disabling the Windows registry backup feature, `RegIdleBackup`, can minimize the number of system writes and reduce the growth of linked-clone desktops.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Task Scheduler** and click **Open**.

5 In the left pane, expand **Task Scheduler Library**, **Microsoft**, **Windows**.

6 Double-click **Registry** and select **RegIdleBackup**.

7 In the Actions pane, click **Disable**.

Disable the System Restore on Windows 7 Virtual Machines

You do not need to use the Windows System Restore feature if you use View Composer refresh to restore linked-clone OS disks to their original snapshots.

When the operating system is idle, System Restore does not have a visible impact on OS-disk growth. However, when the operating system is in use, System Restore generates restore points based on system use, which can have a significant impact on OS-disk growth.

The function of Windows System Restore is the same as View Composer refresh.

As a best practice, you can disable Windows System Restore and avoid unnecessary growth in your linked clones.

If you do not use refresh, evaluate whether it is best to leave System Restore active in your View environment.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start > Control Panel > System and Security > Administrative Tools**.

4 Select **Task Scheduler** and click **Open**.

5 In the left pane, expand **Task Scheduler Library**, **Microsoft**, **Windows**.

6 Double-click **SystemRestore** and select **SR**.

7 In the Actions pane, click **Disable**.

Disable Windows Defender on Windows 7 Virtual Machines

Microsoft Windows Defender can contribute to linked-clone OS disk growth and increase IOPS in linked clones and full virtual machines. Disable Windows Defender if you install other anti-spyware software on the virtual machine.

If Windows Defender is the only anti-spyware installed on the virtual machine, you might prefer to keep Windows Defender active on the desktops in your environment.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start** and type `Windows Defender` in the Search programs and files box.

4 Click **Tools > Options > Administrator**.

5 Deselect **Use this program** and click **Save**.

Disable Microsoft Feeds Synchronization on Windows 7 Virtual Machines

Windows Internet Explorer 7 or 8 uses the Microsoft Feeds Synchronization task to update RSS feeds in users' Web browsers. This task can contribute to linked-clone growth. Disable this task if your users do not require automatic RSS feed updates in their browsers.

Microsoft Feeds Synchronization can cause OS-disk growth if persistent disks are not configured. If persistent disks are configured, the impact is diverted to the persistent disks. In this situation, you should still disable Microsoft Feeds Synchronization to control persistent-disk growth.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows 7 guest operating system as an administrator.

3 Click **Start > Control Panel > Network and Internet > Internet Options**.

4 Click the **Content** tab.

5 Under Feeds and Web Slices, click **Settings**.

6 Deselect **Automatically check feeds and Web Slices for updates** and click **OK**.

7 In the Internet Properties dialog, click **OK**.

Preparing Virtual Machines for View Composer

To deploy linked-clone desktops, you must prepare a parent virtual machine that meets the requirements of the View Composer service.

- Prepare a Parent Virtual Machine on page 64

  The View Composer service requires a parent virtual machine from which you generate a base image for creating and managing linked-clone desktops.

- Activating Windows 7 and Windows Vista on Linked-Clone Desktops on page 66

  To make sure that View Composer properly activates Windows 7 and Windows Vista operating systems on linked-clone desktops, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

- Disable Windows Hibernation in the Parent Virtual Machine on page 66

  The Windows hibernation option creates a large system file that can increase the size of the linked-clone OS disks that are created from the parent virtual machine. Disabling the hibernation option reduces the size of linked-clones.

- Configure a Parent Virtual Machine to Use Local Storage on page 67

  When you prepare a parent virtual machine for View Composer, you can configure the parent virtual machine and linked-clone desktops to store virtual-machine swap files on the local datastore. This optional strategy lets you take advantage of local storage.

- Keep a Record of the Parent Virtual Machine's Paging-File Size on page 68

  When you create a linked-clone pool, you can redirect the linked clones' guest OS paging and temp files to a separate disk. You must configure this disk to be larger than the paging file in the guest OS.

- Increase the Timeout Limit of QuickPrep Customization Scripts on page 69

  View Composer terminates a QuickPrep post-synchronization or power-off script that takes longer than 20 seconds. You can increase the timeout limit for these scripts by changing the `ExecScriptTimeout` Windows registry value on the parent virtual machine.

Prepare a Parent Virtual Machine

The View Composer service requires a parent virtual machine from which you generate a base image for creating and managing linked-clone desktops.

Prerequisites

- Verify that you prepared a virtual machine to use for deploying View desktops. See "Creating Virtual Machines for View Desktop Deployment," on page 45.

A parent virtual machine that you use for View Composer must either belong to the same Active Directory domain as the domain that the linked-clone desktops will join or be a member of the local WORKGROUP.

IMPORTANT To use features that are supported in View Manager 4.5 or later, such as redirecting disposable data to a separate disk and customizing linked-clone desktops with Sysprep, you must deploy the desktops from a parent virtual machine on which View Agent 4.5 or later is installed.

You cannot use View Composer to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1.

- Verify that the virtual machine was not converted from a View Composer linked clone. A virtual machine that is converted from a linked clone has the clone's internal disk and state information. A parent virtual machine cannot have state information.
- If the parent virtual machine runs Windows XP, and your Active Directory runs on Windows Server 2008, apply an update patch on the Windows XP virtual machine. See the Microsoft Support Article 944043 at the following location: http://support.microsoft.com/kb/944043/en-us.

  If you do not install the Windows Server 2008 read-only domain controller (RODC) compatibility pack for Windows XP, linked clones that are deployed from this parent virtual machine fail to join the domain.
- When you install View Agent on the parent virtual machine, select the **View Composer Agent** option. See "Install View Agent on a Virtual Machine," on page 49.

  To update View Agent in a large environment, you can use standard Windows update mechanisms such as Altiris, SMS, LanDesk, BMC, or other systems management software. You can also use the recompose operation to update View Agent.

  NOTE Do not change the log on account for the VMware View Composer Guest Agent Server service in a parent virtual machine. By default, this is the Local System account. If you change this account, the linked clones created from the parent do not start.

- To deploy desktops that run Windows 7 or Windows Vista, configure a volume license key and activate the parent virtual machine's operating system with volume activation. See "Activating Windows 7 and Windows Vista on Linked-Clone Desktops," on page 66.
- If the parent virtual machine runs Windows 7, verify that you followed the best practices for optimizing the operating system. See "Optimizing Windows 7 for Linked-Clone Desktops," on page 57.

Procedure

- Remove the DHCP lease on the parent virtual machine to avoid copying a leased IP address to the linked clones in the pool.

  a On the parent virtual machine, open a command prompt.

  b Type the **`ipconfig /release`** command.
- Verify that the system disk contains a single volume.

  You cannot deploy linked clones from a parent virtual machine that contains more than one volume. The View Composer service does not support multiple disk partitions. Multiple virtual disks are supported.
- Disable the hibernation option to reduce the size of linked-clone OS disks that are created from the parent virtual machine.
- In vSphere Client, disable the vApp Options setting on the parent virtual machine.

You can deploy a linked-clone pool from the parent virtual machine.

What to do next

Use vSphere Client to take a snapshot of the parent virtual machine in its powered-down state. This snapshot is used as the baseline configuration for the first set of linked-clone desktops that are anchored to the parent virtual machine.

IMPORTANT Before you take a snapshot, completely shut down the parent virtual machine by using the **Shut Down** command in the guest operating system.

Activating Windows 7 and Windows Vista on Linked-Clone Desktops

To make sure that View Composer properly activates Windows 7 and Windows Vista operating systems on linked-clone desktops, you must use Microsoft volume activation on the parent virtual machine. The volume-activation technology requires a volume license key.

To activate Windows 7 or Windows Vista with volume activation, you use Key Management Service (KMS), which requires a KMS license key. See your Microsoft dealer to acquire a volume license key and configure volume activation.

NOTE View Composer does not support Multiple Activation Key (MAK) licensing.

Before you create linked-clone desktops with View Composer, you must use volume activation to activate the operating system on the parent virtual machine.

NOTE Windows XP desktops with volume licenses do not require an activation.

When a linked-clone desktop is created, and each time the linked clone is recomposed, the View Composer agent uses the parent virtual machine's KMS server to activate the operating system on the linked clone.

The View Composer QuickPrep tool implements the activation through these steps:

1 Invokes a script to remove the existing license status on the linked-clone virtual machine

2 Restarts the guest operating system

3 Invokes a script that uses KMS licensing to activate the operating system on the clone.

Each time QuickPrep runs on a linked clone, the activation takes place.

For KMS licensing, View Composer uses the KMS server that is configured to activate the parent virtual machine. The KMS server treats an activated linked clone as a computer with a newly issued license.

Disable Windows Hibernation in the Parent Virtual Machine

The Windows hibernation option creates a large system file that can increase the size of the linked-clone OS disks that are created from the parent virtual machine. Disabling the hibernation option reduces the size of linked-clones.

The Windows hibernation option creates a hidden system file, `Hiberfil.sys`. Windows uses this file to store a copy of system memory on the hard disk when the hybrid sleep setting is turned on. When you create a linked-clone pool, the file is created on each linked clone's OS disk.

On Windows 7 virtual machines, this file can be 10GB.

CAUTION When you make hibernation unavailable, the hybrid sleep setting does not work. Users can lose data if the hybrid sleep setting is turned on and a power loss occurs.

Prerequisites

Familiarize yourself with the Windows hibernation feature. See the Microsoft Support Web site. For information about disabling hibernation on Windows 7 or Windows Vista, see the Microsoft Support Web site and search for how to disable and re-enable hibernation on a computer that is running Windows.

Procedure

1 In vSphere Client, select the parent virtual machine and select **Open Console**.

2 Log in to the Windows guest operating system as an administrator.

3 Disable the hibernation option.

Operating System	Action
Windows 7 or Windows Vista	a Click **Start** and type **`cmd`** in the **Start Search** box. b In the search results list, right-click **Command Prompt** and click **Run as Administrator**. c At the User Account Control prompt, click **Continue**. d At the command prompt, type **`powercfg.exe /hibernate off`** and press Enter. e Type **`exit`** and press Enter.
Windows XP	a Click **Start > Run**. b Type **`cmd`** and click **OK**. c At the command prompt, type **`powercfg.exe /hibernate off`** and press Enter. d Type **`exit`** and press Enter.

4 Log out of the guest operating system.

When you create linked clone desktops from the parent virtual machine, the `Hiberfil.sys` file is not created on the linked-clone OS disks.

Configure a Parent Virtual Machine to Use Local Storage

When you prepare a parent virtual machine for View Composer, you can configure the parent virtual machine and linked-clone desktops to store virtual-machine swap files on the local datastore. This optional strategy lets you take advantage of local storage.

In this procedure, you configure local storage for the virtual-machine swap files, not the paging and temp files in the guest OS. When you create a linked-clone pool, you also can redirect guest OS paging and temp files to a separate disk. See "Worksheet for Creating a Linked-Clone Desktop Pool," on page 75.

Prerequisites

Prepare the parent virtual machine to meet the requirements of the View Composer service. See "Prepare a Parent Virtual Machine," on page 64.

Procedure

1 Configure a swapfile datastore on the ESX/ESXi host or cluster on which you will deploy the linked-clone pool.

2 When you create the parent virtual machine in vCenter Server, store the virtual-machine swap files on the swapfile datastore on the local ESX/ESXi host or cluster:

   a In vSphere Client, select the parent virtual machine.

   b Click **Edit Settings** and click the **Options** tab.

   c Click **Swapfile location** and click **Store in the host's swapfile datastore**.

   For detailed instructions, see the VMware vSphere documentation.

When you deploy a pool from this parent virtual machine, the linked-clone desktops use the local ESX host's swapfile datastore.

Keep a Record of the Parent Virtual Machine's Paging-File Size

When you create a linked-clone pool, you can redirect the linked clones' guest OS paging and temp files to a separate disk. You must configure this disk to be larger than the paging file in the guest OS.

When a linked clone that is configured with a separate disk for the disposable files is powered off, View Manager replaces the temporary disk with a copy of the original temporary disk that View Composer created with the linked-clone pool. This feature can slow the growth of linked clones. However, this feature can work only if you configure the disposable-file disk to be large enough to hold the guest OS's paging files.

Before you can configure the disposable-file disk, you must know the maximum paging-file size in the parent virtual machine. The linked clones have the same paging-file size as the parent virtual machine from which they are created.

NOTE This feature is not that same as configuring local storage for the virtual-machine swap files. See "Configure a Parent Virtual Machine to Use Local Storage," on page 67.

Procedure

1 In vSphere Client, right-click the parent virtual machine and click **Open Console**.

2 Select **Start > Settings > Control Panel > System**.

3 Click the **Advanced** tab.

4 In the Performance pane, click **Settings**.

5 Click the **Advanced** tab.

6 In the Virtual memory pane, click **Change**.

   The Virtual Memory page appears.

7 Set the paging file size to a larger value than the size of the memory that is assigned to the virtual machine.

   IMPORTANT If the **Maximum size (MB)** setting is smaller than the virtual-machine memory size, type a larger value and save the new value.

   ---

8 Keep a record of the **Maximum size (MB)** setting that is configured in the Paging file size for selected drive pane.

What to do next

When you configure a linked-clone pool from this parent virtual machine, configure a disposable-file disk that is larger than the paging-file size.

Increase the Timeout Limit of QuickPrep Customization Scripts

View Composer terminates a QuickPrep post-synchronization or power-off script that takes longer than 20 seconds. You can increase the timeout limit for these scripts by changing the `ExecScriptTimeout` Windows registry value on the parent virtual machine.

The increased timeout limit is propagated to linked clones that are created from the parent virtual machine. QuickPrep customization scripts can run on the linked clones for the time that you specify.

Alternatively, you can use your customization script to launch another script or process that performs the long-running task.

NOTE Most QuickPrep customization scripts can finish running within the 20-second limit. Test your scripts before you increase the limit.

Prerequisites

- Install View Agent with the **View Composer Agent** option on the parent virtual machine.
- Verify that the parent virtual machine is prepared to create a linked-clone pool. See "Prepare a Parent Virtual Machine," on page 64.

Procedure

1 On the parent virtual machine, start the Windows Registry Editor.

   a Select **Start > Command Prompt**.

   b At the command prompt, type **regedit**.

2 In the Windows registry, locate the `vmware-viewcomposer-ga` registry key.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
```

3 Click **Edit** and modify the registry value.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

   The default value is 20000 milliseconds.

The timeout value is increased. You do not have to restart Windows for this value to take effect.

What to do next

Take a snapshot of the parent virtual machine and create a linked-clone pool.

Creating Virtual Machine Templates

You must create a virtual machine template before you can create an automated pool that contains full virtual machines.

A virtual machine template is a master copy of a virtual machine that can be used to create and provision new virtual machines. Typically, a template includes an installed guest operating system and a set of applications.

You create virtual machine templates in vSphere Client. You can create a virtual machine template from a previously configured virtual machine, or you can convert a previously configured virtual machine to a virtual machine template.

See the *vSphere Basic System Administration* guide for information on using vSphere Client to create virtual machine templates. See "Automated Pools That Contain Full Virtual Machines," on page 72 for information on creating automated pools.

NOTE You do not create a linked-clone pool from a virtual machine template.

Creating Customization Specifications

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

With customization specifications, you can customize View desktops as they are created in View Administrator. You create new customization specifications by using the Customization Specification wizard in vSphere Client. You can also use the Customization Specification wizard to import existing custom `sysprep.ini` files.

See the *vSphere Virtual Machine Administration* document for information on using the Customization Specification wizard.

Make sure that the customization specifications are accurate before you use them in View Administrator. In vSphere Client, deploy and customize a virtual machine from your template using the customization specifications. Fully test the virtual machine, including DHCP and authentication, before you create View desktops.

NOTE To apply customization specifications to desktop pools that use Windows XP, you must install Microsoft Sysprep tools on your vCenter Server machine.

You do not have to install Sysprep tools in vCenter Server for desktop pools that use Windows 7 or Vista. Sysprep tools are built into these operating systems.

When you use a Sysprep customization specification to join a Windows 7 desktop to a domain, you must use the fully qualified domain name (FQDN) of the Active Directory domain. You cannot use the NetBIOS name of the Active Directory domain.

Creating Desktop Pools

5

With View Manager, you create pools of desktops that deliver View desktop access to clients. View Manager deploys pools from desktop sources, which can be virtual machines that are managed by vCenter Server, virtual machines that run on another virtualization platform, or physical computers, terminal servers, or blade PCs.

You can create several types of desktop pools. You can also provision an individual desktop by deploying a manual pool with a single desktop source.

- Automated Pools That Contain Full Virtual Machines on page 72

  To create an automated desktop pool, View Manager dynamically provisions desktops based on settings that you apply to the pool. View Manager uses a virtual machine template as the desktop source for the pool and creates a new virtual machine in vCenter Server for each desktop.

- Linked-Clone Desktop Pools on page 75

  To create a linked-clone desktop pool, View Composer generates linked-clone virtual machines from a snapshot of a parent virtual machine. View Manager dynamically provisions the linked-clone desktops based on settings that you apply to the pool.

- Manual Desktop Pools on page 93

  To create a manual desktop pool, View Manager provisions desktops from existing desktop sources. For each desktop in the pool, you select a separate desktop source to deliver View access to clients.

- Microsoft Terminal Services Pools on page 97

  You can use Microsoft Terminal Servers to provide Terminal Services sessions as desktops to View clients. View Manager manages Terminal Services sessions in the same way that it manages other View desktops.

- Provisioning Desktop Pools on page 99

  When you create a desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

- Setting Power Policies for Desktop Pools on page 110

  You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server.

Automated Pools That Contain Full Virtual Machines

To create an automated desktop pool, View Manager dynamically provisions desktops based on settings that you apply to the pool. View Manager uses a virtual machine template as the desktop source for the pool and creates a new virtual machine in vCenter Server for each desktop.

Worksheet for Creating an Automated Pool That Contains Full Virtual Machines

When you create an automated desktop pool, the View Administrator Add Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Pool wizard.

To create a linked-clone pool, see "Linked-Clone Desktop Pools," on page 75.

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a desktop. Users receive the same desktop each time they log in. ■ In a floating-assignment pool, users receive different desktops each time they log in. For details, see "User Assignment in Desktop Pools," on page 100.	
Enable automatic assignment	In a dedicated-assignment pool, a desktop is assigned to a user when the user first logs in to the pool. You can also explicitly assign desktops to users. If you do not enable automatic assignment, you must explicitly assign a desktop to each user.	
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
Pool ID	The unique name that identifies the pool in View Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID. A View Connection Server configuration can be a standalone View Connection Server instance or a group of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in with View Client. If you do not specify a display name, the pool ID is displayed to users.	
View Folder	Select a View Folder in which to place the pool or leave the pool in the default root folder. If you use a View Folder, you can delegate managing the pool to an administrator with a specific role. For details, see "Using Folders to Delegate Administration," on page 26. NOTE View folders are different than vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Delete desktop after logoff	If you select floating user assignment, choose whether to delete desktops after users log off. NOTE You set this option on the Pool Settings page.	
Pool Settings	Settings that determine the desktop state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For descriptions, see "Desktop and Pool Settings," on page 106. For a list of the settings that apply to automated pools, see "Desktop Settings for Automated Pools That Contain Full Virtual Machines," on page 75. For more information about power policies and automated pools, see "Setting Power Policies for Desktop Pools," on page 110.	
Virtual machine naming	Choose whether to provision desktops by manually specifying a list of desktop names or by providing a naming pattern and the total number of desktops. For details, see "Naming Desktops Manually or Providing a Naming Pattern," on page 100.	
List of desktop names	If you specify names manually, prepare a text file that lists desktop names and, optionally, the associated user names.	
Naming pattern	If you use this naming method, provide the pattern. View Manager uses your pattern as a prefix in all the desktop names and appends a unique number to identify each desktop. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	
Maximum number of desktops	If you use a naming pattern, specify the total number of desktops in the pool. You can also specify a minimum number of desktops to provision when you first create the pool.	
Number of spare (powered on) desktops	If you specify names manually or use a naming pattern, specify a number of desktops that View Manager keeps available and powered on for new users. For details, see "Naming Desktops Manually or Providing a Naming Pattern," on page 100. When you specify names manually, this option is called # **Unassigned desktops kept powered on**.	
Minimum number of desktops	If you use a naming pattern and provision desktops on demand, specify a minimum number of desktops in the pool. If you provision desktops on demand, View Manager creates desktops as users connect to the pool for the first time. View Manager creates the minimum number of desktops when you create the pool.	

Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

Option	Description	Fill In Your Value Here
Template	Select the virtual machine template that View Manager uses to create the pool.	
vCenter Server folder	Select the folder in vCenter Server in which the desktop pool resides.	
Host or cluster	Select the ESX host or cluster on which the desktop virtual machines run.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
Datastores	Select one or more datastores on which to store the desktop pool. For clusters, you can use shared or local datastores.	
Guest customization	Select a customization specification (SYSPREP) from the list to let View Manager configure licensing, domain attachment, DHCP settings, and other properties on the desktops. Alternatively, you can customize the desktops manually after View Manager creates them.	

Create an Automated Pool That Contains Full Virtual Machines

You can create an automated desktop pool based on a virtual machine template that you select. View Manager dynamically deploys the desktops, creating a new virtual machine in vCenter Server for each desktop.

To create a linked-clone pool, see "Linked-Clone Desktop Pools," on page 75.

Prerequisites

- Prepare a virtual machine template that View Manager will use to create the desktops. View Agent must be installed on the template. See Chapter 4, "Creating and Preparing Virtual Machines," on page 45.
- If you intend to use a customization specification, make sure that the specifications are accurate. In vSphere Client, deploy and customize a virtual machine from your template using the customization specification. Fully test the resulting virtual machine, including DHCP and authentication.
- Verify that you have a sufficient number of ports on the ESX virtual switch that is used for desktop virtual machines. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESX host must equal or exceed the number of desktop virtual machines multiplied by the number of virtual NICs per virtual machine.
- Gather the configuration information you must provide to create the pool. See "Worksheet for Creating an Automated Pool That Contains Full Virtual Machines," on page 72.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop and Pool Settings," on page 106.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Click **Add**.

3 Select **Automated Pool**.

4 On the vCenter Server page, choose **Full virtual machines**.

5 Follow the prompts in the wizard to create the pool.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the desktops as they are added to the pool by clicking **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Add Entitlements to Desktop Pools," on page 115.

Desktop Settings for Automated Pools That Contain Full Virtual Machines

You must specify desktop and pool settings when you configure automated pools that contain full virtual machines. Different settings apply to pools with dedicated user assignments and floating user assignments.

Table 5-2 lists the settings that apply to automated pools with dedicated assignments and floating assignments.

For descriptions of each desktop setting, see "Desktop and Pool Settings," on page 106.

Table 5-2. Settings for Automated Pools That Contain Full Virtual Machines

Setting	Automated Pool, Dedicated Assignment	Automated Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote desktop power policy	Yes	Yes
Automatic logoff after disconnect	Yes	Yes
Allow users to reset their desktops	Yes	Yes
Allow multiple sessions per user		Yes
Delete desktop after logoff		Yes
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
Windows 7 3D Rendering	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Adobe Flash quality	Yes	Yes
Adobe Flash throttling	Yes	Yes

Linked-Clone Desktop Pools

To create a linked-clone desktop pool, View Composer generates linked-clone virtual machines from a snapshot of a parent virtual machine. View Manager dynamically provisions the linked-clone desktops based on settings that you apply to the pool.

Because linked-clone desktops share a base system-disk image, they use less storage than full virtual machines.

Worksheet for Creating a Linked-Clone Desktop Pool

When you create a linked-clone desktop pool, the View Administrator Add Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Pool wizard.

Before you create a linked-clone pool, you must use vCenter Server to take a snapshot of the parent virtual machine that you prepare for the pool. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

NOTE You cannot create a linked-clone pool from a virtual machine template.

Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a desktop. Users receive the same desktop each time they log in. ■ In a floating-assignment pool, users receive different desktops each time they log in. For details, see "User Assignment in Desktop Pools," on page 100.	
Enable automatic assignment	In a dedicated-assignment pool, a desktop is assigned to a user when the user first logs in to the pool. You can also explicitly assign desktops to users. If you do not enable automatic assignment, you must explicitly assign a desktop to each user.	
vCenter Server	Select the vCenter Server that manages the virtual machines in the pool.	
Pool ID	The unique name that identifies the pool in View Administrator. If multiple View Connection Server configurations are running in your environment, make sure that another View Connection Server configuration is not using the same pool ID. A View Connection Server configuration can be a standalone View Connection Server instance or a group of replicated instances that share a common View LDAP configuration.	
Display name	The pool name that users see when they log in with View Client. If you do not specify a display name, the pool ID is displayed to users.	
View Folder	Select a View Folder in which to place the pool or leave the pool in the default root folder. If you use a View Folder, you can delegate managing the pool to an administrator with a specific role. For details, see "Using Folders to Delegate Administration," on page 26. NOTE View folders are different than vCenter Server folders that store desktop virtual machines. You select a vCenter Server folder later in the wizard with other vCenter Server settings.	
Delete or refresh desktop on logoff	If you select floating user assignment, choose whether to refresh desktops, delete desktops, or do nothing after users log off. NOTE You set this option on the Pool Settings page.	

Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Pool Settings	Settings that determine the desktop state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For descriptions, see "Desktop and Pool Settings," on page 106. For a list of the settings that apply to linked-clone pools, see "Desktop Settings for Linked-Clone Desktop Pools," on page 82. For more information about power policies and automated pools, see "Setting Power Policies for Desktop Pools," on page 110.	
Redirect Windows profile to persistent disks	If you select dedicated user assignments, choose whether to store Windows user-profile data on a separate View Composer persistent disk or the same disk as the OS data. Separate persistent disks let you preserve user data and settings. View Composer refresh, recompose, and rebalance operations do not affect persistent disks. You can detach a persistent disk from a linked clone and attach it to another desktop. If you store the Windows profile in the OS disk, user data and settings are removed during refresh, recompose, and rebalance operations.	
Disk size and drive letter for persistent disk	If you store user profile data on a separate View Composer persistent disk, provide the disk size in megabytes and the drive letter. NOTE Do not select a drive letter that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.	
Disposable File Redirection	Choose whether to redirect the guest OS's paging and temp files to a separate, nonpersistent disk. If you do, provide the disk size in megabytes. With this configuration, when a linked clone is powered off, View Manager replaces the disposable-file disk with a copy of the original disk that was created with the linked-clone pool. Linked clones can increase in size as users interact with their desktops. Disposable file redirection can save storage space by slowing the growth of linked clones. The disk size should be larger than page-file size of the guest OS. To determine the page-file size, see "Keep a Record of the Parent Virtual Machine's Paging-File Size," on page 68. When you configure the disposable-file disk size, consider that the actual size of a formatted disk partition is slightly smaller than the value you provide in View Administrator.	
Virtual machine naming	Choose whether to provision desktops by manually specifying a list of desktop names or by providing a naming pattern and the total number of desktops. For details, see "Naming Desktops Manually or Providing a Naming Pattern," on page 100.	

Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
List of desktop names	If you specify names manually, prepare a text file that lists desktop names and, optionally, the associated user names.	
Naming pattern	If you use this naming method, provide the pattern. View Manager uses your pattern as a prefix in all the desktop names and appends a unique number to identify each desktop. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	
Maximum number of desktops	If you use a naming pattern, specify the total number of desktops in the pool. You can also specify a minimum number of desktops to provision when you first create the pool.	
Number of spare (powered on) desktops	If you specify names manually or use a naming pattern, specify a number of desktops that View Manager keeps available and powered on for new users. For details, see "Naming Desktops Manually or Providing a Naming Pattern," on page 100. When you specify names manually, this option is called # **Unassigned desktops kept powered on**.	
Minimum number of desktops	If you use a naming pattern and provision desktops on demand, specify a minimum number of desktops in the pool. If you provision desktops on demand, View Manager creates desktops as users connect to the pool for the first time. View Manager creates the minimum number of desktops when you create the pool.	
Parent virtual machine	Select the parent virtual machine for the pool. To use features that are supported in View Manager 4.5 or later, such as redirecting disposable data to a separate disk and customizing the linked clones with Sysprep, you must select a parent virtual machine on which View Agent 4.5 or later is installed. NOTE You cannot use View Composer to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1.	
Default image (snapshot)	Select the snapshot of the parent virtual machine to use as the base image for the pool. Do not delete the snapshot and parent virtual machine from vCenter Server, unless no more linked clones will be created from this default image. View Manager requires the parent virtual machine and snapshot to provision new linked clones in the pool, according to pool policies.	
Publish base image to the Transfer Server repository.	Select this option if you use the pool to provision local desktops. When a local desktop is provisioned, View Transfer Server downloads the base image from the Transfer Server repository to the client. You can also publish the base image after you create the pool.	

Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
vCenter Server folder	Select the folder in vCenter Server in which the desktop pool resides.	
Host or cluster	Select the ESX host or cluster on which the desktop virtual machines run.	
Resource pool	Select the vCenter Server resource pool in which the desktop pool resides.	
Select Datastores	Select one or more datastores on which to store the desktop pool. A table on the **Select Datastores** page of the Add Pool wizard provides high-level guidelines for estimating the pool's storage requirements. These guidelines can help you determine which datastores are large enough to store the linked-clone disks. For details, see "Storage Sizing for Linked-Clone Desktop Pools," on page 86. ■ If you store user data and OS data on separate disks, you can store the persistent disks and OS disks on separate datastores. ■ You can store the replica (master) virtual machine on a high-performance datastore and the linked clones on separate datastores. For clusters, you can use shared datastores. For an indidivual ESXi host, you can use shared or local datastores. For more information about the disks that are created for linked clones, see "Linked-Clone Desktop Data Disks," on page 92.	
Storage Overcommit	Determine the storage-overcommit level at which View Manager creates linked-clone desktops on each datastore. As the level increases, more linked clones fit on the datastore and less space is reserved to let individual clones grow. A high storage-overcommit level lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore. For details, see "Set the Storage Overcommit Level for Linked-Clone Desktops," on page 90.	
Active Directory domain	Select the Active Directory domain and user name. View Composer requires certain user privileges to create a linked-clone pool. The domain and user account are used by QuickPrep or Sysprep to customize the linked-clone desktops. For details, see "Create a User Account for View Composer," on page 14. You specify this user when you configure View Composer settings for vCenter Server. For details, see "Configure View Composer Settings for vCenter Server," on page 15. You can specify multiple domains and users when you configure View Composer settings. When you use the Add Pool wizard to create a pool, you must select one domain and user from the list.	

Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

Option	Description	Fill In Your Value Here
Active Directory container	Provide the Active Directory container relative distinguished name. For example: **CN=Computers** When you run the Add Pool wizard, you can browse your Active Directory tree for the container.	
Use QuickPrep or a customization specification (Sysprep)	Choose whether to use QuickPrep or select a customization specification (Sysprep) to let View Manager configure licensing, domain attachment, DHCP settings, and other properties on the desktops. Sysprep is supported for linked clones only on vSphere 4.1 or later software. You cannot use Sysprep to customize linked-clone desktops on vSphere 4.0 software. After you use QuickPrep or Sysprep when you create a pool, you cannot switch to the other customization method later on, when you create or recompose desktops in the pool. For details, see "Choosing QuickPrep or Sysprep to Customize Linked-Clone Desktops," on page 83.	
Power-off script	QuickPrep can run a customization script on linked-clone desktops before they are powered off. Provide the path to the script on the parent virtual machine.	
Post synchronization script	QuickPrep can run a customization script on linked-clone desktops after they are created, recomposed, and refreshed. Provide the path to the script on the parent virtual machine.	

Create a Linked-Clone Desktop Pool

You can create an automated, linked-clone desktop pool based on a parent virtual machine that you select. The View Composer service dynamically creates a new linked-clone virtual machine in vCenter Server for each desktop.

To create an automated pool that contains full virtual machines, see "Automated Pools That Contain Full Virtual Machines," on page 72.

Prerequisites

- Verify that the View Composer service is installed in vCenter Server and a View Composer database is configured. See the *VMware View Installation* document.
- Verify that View Composer settings for vCenter Server are configured in View Administrator. See "Configure View Composer Settings for vCenter Server," on page 15.
- Verify that you have a sufficient number of ports on the ESX virtual switch that is used for desktop virtual machines. The default value might not be sufficient if you create large desktop pools. The number of virtual switch ports on the ESX host must equal or exceed the number of desktop virtual machines multiplied by the number of virtual NICs per virtual machine.
- Verify that you prepared a parent virtual machine. View Agent must be installed on the parent virtual machine. See Chapter 4, "Creating and Preparing Virtual Machines," on page 45.

- Take a snapshot of the parent virtual machine in vCenter Server. You must shut down the parent virtual machine before you take the snapshot. View Composer uses the snapshot as the base image from which the clones are created.

  NOTE You cannot create a linked-clone pool from a virtual machine template.

- Gather the configuration information you must provide to create the pool. See "Worksheet for Creating a Linked-Clone Desktop Pool," on page 75.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop and Pool Settings," on page 106.

IMPORTANT While a linked-clone pool is created, do not modify the parent virtual machine in vCenter Server. For example, do not convert the parent virtual machine to a template. The View Composer service requires that the parent virtual machine remain in a static, unaltered state during pool creation.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Click **Add**.

3 Select **Automated Pool**.

4 On the vCenter Server page, choose **View Composer linked clones**.

5 Follow the prompts in the wizard to create the pool.

  Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page you completed by clicking the page name in the navigation panel.

  On the **vCenter Settings** page, you must click **Browse** and select the vCenter Server settings in sequence. You cannot skip a vCenter Server setting:

  a Default image

  b Virtual machine folder

  c Host or cluster

  d Resource pool

  e Datastores

In View Administrator, you can view the desktops as they are added to the pool by clicking **Inventory > Desktops**.

The linked clones might restart one or more times while they are provisioned.

View Composer also creates a replica virtual machine that serves as the master image for provisioning the linked clones. To reduce space consumption, the replica is created as a thin disk. If all the desktops are recomposed or deleted, and no clones are linked to the replica, the replica virtual machine is deleted from vCenter Server.

If you do not store the replica on a separate datastore, View Composer creates a replica on each datastore on which linked clones are created.

If you store the replica on a separate datastore, one replica is created for the entire pool, even when linked clones are created on multiple datastores.

What to do next

Entitle users to access the pool. See "Add Entitlements to Desktop Pools," on page 115.

Desktop Settings for Linked-Clone Desktop Pools

You must specify desktop and pool settings when you configure automated pools that contain linked-clone desktops created by View Composer. Different settings apply to pools with dedicated user assignments and floating user assignments.

Table 5-4 lists the settings that apply to linked-clone pools with dedicated assignments and floating assignments.

For descriptions of each desktop setting, see "Desktop and Pool Settings," on page 106.

Table 5-4. Settings for Automated, Linked-Clone Desktop Pools

Setting	Linked-Clone Pool, Dedicated Assignment	Linked-Clone Pool, Floating Assignment
State	Yes	Yes
Connection Server restrictions	Yes	Yes
Remote desktop power policy	Yes	Yes
Automatic logoff after disconnect	Yes	Yes
Allow users to reset their desktops	Yes	Yes
Allow multiple sessions per user		Yes
Delete or refresh desktop on logoff		Yes
Refresh OS disk after logoff	Yes	
Default display protocol	Yes	Yes
Allow users to choose protocol	Yes	Yes
Windows 7 3D Rendering	Yes	Yes
Max number of monitors	Yes	Yes
Max resolution of any one monitor	Yes	Yes
Adobe Flash quality	Yes	Yes
Adobe Flash throttling	Yes	Yes

View Composer Support for Linked-Clone SIDs and Third-Party Applications

View Composer can generate and preserve local computer security identifiers (SIDs) for linked-clone virtual machines in some situations. View Composer can preserve globally unique identifiers (GUIDs) of third-party applications, depending on the way that the applications generate GUIDs.

To understand how View Composer operations affect SIDs and application GUIDs, you should understand how linked-clone desktops are created and provisioned:

1 View Composer creates a linked clone by taking these actions:

   a Creates the replica by cloning the parent virtual-machine snapshot.

   b Creates the linked clone to refer to the replica as its parent disk.

2 View Composer and View Manager customize the linked clone with QuickPrep or a Sysprep customization specification, depending on which customization tool you select when you create the pool.

   - If you use Sysprep, a unique SID is generated for each clone.
   - If you use QuickPrep, no new SID is generated. The parent virtual machine's SID is replicated on all provisioned linked-clone desktops in the pool.
   - Some applications generate a GUID during customization.

3 View Manager creates a snapshot of the linked clone.

The snapshot contains the unique SID generated with Sysprep or common SID generated with QuickPrep.

4 View Manager powers on the desktop according to the settings you select when you create the pool.

Some applications generate a GUID the first time the desktop is powered on.

For a comparison of QuickPrep and Sysprep customization, see "Choosing QuickPrep or Sysprep to Customize Linked-Clone Desktops," on page 83.

When you refresh the linked clone, View Composer uses the snapshot to restore the clone to its initial state. Its SID is preserved.

If you use QuickPrep, when you recompose the linked clone, the parent virtual machine's SID is preserved on the linked clone as long as you select the same parent virtual machine for the recompose operation. If you select a different parent virtual machine for the recomposition, the new parent's SID is replicated on the clone.

If you use Sysprep, a new SID is always generated on the clone. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 86.

Table 5-5 shows the effect of View Composer operations on linked-clone SIDs and third-party application GUIDs.

Table 5-5. View Composer Operations, Linked-Clone SIDs, and Application GUIDs

Support for SIDs or GUIDs	Clone Creation	Refresh	Recompose
Sysprep: Unique SIDs for linked clones	With Sysprep customization, unique SIDs are generated for linked clones.	Unique SIDs are preserved.	Unique SIDS are not preserved.
QuickPrep: Common SIDs for linked clones	With QuickPrep customization, a common SID is generated for all clones in a pool.	Common SID is preserved.	Common SID is preserved.
Third-party application GUIDs	Each application behaves differently. NOTE Sysprep and QuickPrep have the same effect on GUID preservation.	The GUID is preserved if an application generates the GUID before the initial snapshot is taken. The GUID is not preserved if an application generates the GUID after the initial snapshot is taken.	Recompose operations do not preserve an application GUID unless the application writes the GUID on the drive specified as a View Composer persistent disk.

Choosing QuickPrep or Sysprep to Customize Linked-Clone Desktops

QuickPrep and Microsoft Sysprep provide different approaches to customizing linked-clone desktops. QuickPrep is designed to work efficiently with View Composer. Microsoft Sysprep offers standard customization tools.

When you create linked-clone desktops, you must modify each virtual machine so that it can function as a unique computer on the network. View Manager and View Composer provide two methods for personalizing linked-clone desktops.

Table 5-6 compares QuickPrep with customization specifications that are created with Microsoft Sysprep.

Sysprep is supported for linked clones only on vSphere 4.1 or later software. You cannot use Sysprep to customize linked-clone deskstops on vSphere 4.0 software.

Table 5-6. Comparing QuickPrep and Microsoft Sysprep

QuickPrep	Customization Specification (Sysprep)
Designed to work with View Composer. For details, see "Customizing Linked-Clone Desktops with QuickPrep," on page 84.	Can be created with the standard Microsoft Sysprep tools.
Uses the same local computer security identifier (SID) for all linked clones in the pool.	Generates a unique local computer SID for each linked clone in the pool.
Can run additional customization scripts before linked clones are powered off and after linked clones are created, refreshed, or recomposed.	Can run an additional script when the user first logs in.
Joins the linked clone computer to the Active Directory domain.	Joins the linked-clone computer to the Active Directory domain. The domain and administrator information in the Sysprep customization specification is not used. The virtual machine is joined to the domain using the guest customization information that you enter in View Administrator when you create the pool.
For each linked clone, adds a unique ID to the Active Directory domain account.	For each linked clone, adds a unique ID to the Active Directory domain account.
Does not generate a new SID after linked clones are refreshed. The common SID is preserved.	Generates a new SID when each linked clone is customized. Preserves the unique SIDs during a refresh operation, but not during a recompose or rebalance operation.
Does not generate a new SID after linked clones are recomposed. The common SID is preserved.	Runs again after linked clones are recomposed, generating new SIDs for the virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 86.
Runs faster than Sysprep.	Can take longer than QuickPrep.

After you customize a linked-clone pool with QuickPrep or Sysprep, you cannot switch to the other customization method when you create or recompose desktops in the pool.

Customizing Linked-Clone Desktops with QuickPrep

You can personalize the linked-clone desktops that are created from a parent virtual machine by using the QuickPrep system tool. View Composer executes QuickPrep when a linked-clone desktop is created or recomposed.

QuickPrep customizes a linked-clone desktop in several ways:

- Gives the computer a name that you specify when you create the linked-clone pool.
- Creates a computer account in Active Directory, joining the computer to the appropriate domain.
- Mounts the View Composer persistent disk. The Windows user profile is redirected to this disk.
- Redirects temp and paging files to a separate disk.

These steps might require the linked clones to restart one or more times.

QuickPrep uses KMS volume license keys to activate Windows 7 and Windows Vista linked-clone desktops. For details, see "Activating Windows 7 and Windows Vista on Linked-Clone Desktops," on page 66.

You can create your own scripts to further customize the linked clones. QuickPrep can run two types of scripts at predefined times:

- After linked clones are created or recomposed
- Immediately before linked clones are powered off

For guidelines and rules for using QuickPrep customization scripts, see "Running QuickPrep Customization Scripts," on page 85.

NOTE View Composer requires domain user credentials to join linked-clone desktops to an Active Directory domain. For details, see "Create a User Account for View Composer," on page 14.

Running QuickPrep Customization Scripts

With the QuickPrep tool, you can create scripts to customize the linked-clone desktops in a pool. You can configure QuickPrep to run customization scripts at two predefined times.

When QuickPrep Scripts Run

The post-synchronization script runs after linked clones are created, recomposed, or rebalanced, and the clones' status is **Ready**. The power-off script runs before linked clones are powered off. The scripts run in the guest operating systems of the linked clones.

How QuickPrep Executes Scripts

The QuickPrep process uses the Windows `CreateProcess` API call to execute scripts. Your script can invoke any process that can be created with the `CreateProcess` API. For example, `cmd`, `vbscript`, `exe`, and batch-file processes work with the API.

In particular, QuickPrep passes the path that is specified for the script as the second parameter to the `CreateProcess` API and sets the first parameter to `NULL`.

For example, if the script path is `c:\myscript.cmd`, the path appears as the second parameter in the function in the View Composer log file: `CreateProcess(NULL,c:\myscript.cmd,...)`.

Providing Paths to QuickPrep Scripts

You provide paths to the QuickPrep customization scripts when you create a linked-clone desktop pool or when you edit a pool's guest customization settings. The scripts must reside on the parent virtual machine. You cannot use a UNC path to a network share.

If you use a scripting language that needs an interpreter to execute the script, the script path must start with the interpreter binary.

For example, if you specify the path `C:\script\myvb.vbs` as a QuickPrep customization script, View Composer Agent cannot execute the script. You must specify a path that starts with the interpreter binary path:

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

QuickPrep Script Timeout Limit

View Composer terminates a post-synchronization or power-off script that takes longer than 20 seconds. If your script takes longer than 20 seconds, you can increase the timeout limit. For details, see "Increase the Timeout Limit of QuickPrep Customization Scripts," on page 69.

Alternatively, you can use your script to launch another script or process that performs the long-running task.

QuickPrep Script Account

QuickPrep runs the scripts under the account under which the VMware View Composer Guest Agent Server service is configured to run. By default, this account is `Local System`.

Do not change this log on account. If you do, the linked clones do not start.

QuickPrep Script Logs

View Composer logs contain information about QuickPrep script execution. The log records the start and end of execution and logs output or error messages. The log is located in the Windows `temp` directory:

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

Recomposing Linked Clones Customized with Sysprep

If you recompose a linked-clone desktop that was customized with Sysprep, View Manager runs the Sysprep customization specification again after the OS disk is recomposed. This operation generates a new SID for the linked-clone virtual machine.

If a new SID is generated, the recomposed linked clone functions as a new computer on the network. Some software programs such as system-management tools depend on the SID to identify the computers under their management. These programs might not be able to identify or locate the linked-clone virtual machine.

Also, if third-party software is installed on the system disk, the customization specification might regenerate the GUIDs for that software after the recomposition.

A recomposition restores the linked clone to its original state, before the customization specification was run the first time. In this state, the linked clone does not have a local computer SID or the GUID of any third-party software installed in the system drive. View Manager must run the Sysprep customization specification after the linked clone is recomposed.

Storage Sizing for Linked-Clone Desktop Pools

View Manager provides high-level guidelines that can help you determine how much storage a linked-clone desktop pool requires. A table in the Add Pool wizard shows a general estimate of the linked-clone disks' storage requirements when the pool is created and as the linked clones grow over time.

The storage-sizing table also displays the free space on the datastores that you select for storing OS disks, View Composer persistent disks, and replicas. You can decide which datastores to use by comparing the actual free space with the estimated requirements for the linked-clone disks.

The formulas that View Manager uses can only provide a general estimate of storage use. Your linked clones' actual storage growth depends on many factors:

- Amount of memory assigned to the parent virtual machine
- Frequency of refresh operations
- Size of the guest operating system's paging file
- Whether you redirect paging and temp files to a separate disk
- Whether you configure separate View Composer persistent disks
- Workload on the linked-clone desktops, determined primarily by the types of applications that users run in the guest operating system

---

NOTE In a deployment that includes hundreds or thousands of linked clones, configure your linked-clone pools so that particular sets of datastores are dedicated to particular ESX clusters. Do not configure pools randomly across all the datastores so that most or all ESX hosts must access most or all LUNs.

When too many ESX hosts attempt to write to linked-clone OS disks on a particular LUN, contention problems can occur, degrading performance and interfering with scalability. For more information about datastore planning in large deployments, see the *VMware View Architecture Planning* document.

Sizing Guidelines for Linked-Clone Pools

When you create or edit a linked-clone desktop pool, the **Select Datastores** page displays a table that provides storage-sizing guidelines. The table can help you to decide which datastores to select for the linked-clone disks.

Sizing Table for Linked-Clone Disks

Table 5-7 shows an example of storage-sizing recommendations that might be displayed for a pool of 10 virtual machines if the parent virtual machine has 1GB of memory and a 10GB replica. In this example, different datastores are selected for OS disks and View Composer persistent disks.

Table 5-7. Example Sizing Table for Linked-Clone Disks

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	40.00	80.00	130.00
Persistent disks	28.56	4.00	10.00	20.00

The **Selected Free Space** column shows the total available space on all of the datastores that you selected for a disk type such as OS disks.

The **Min Recommended** column shows the minimum amount of recommended storage for a pool.

The **50% Utilization** column shows the recommended storage when the linked-clone disks grow to 50% of the parent virtual machine.

The **Max Recommended** column shows the recommended storage when the linked-clone disks approach the full size of the parent virtual machine.

If you store OS disks and persistent disks on the same datastore, View Manager calculates the storage requirements of both disk types. The **Data Type** is shown as **Linked clones** instead of a particular disk type.

If you store View Composer replicas on a separate datastore, the table also shows storage recommendations for the replicas and adjusts the recommendations for OS disks.

Sizing Guidelines

The table provides general guidelines. Your storage calculations must account for additional factors that can affect actual storage growth in the linked-clone pool.

For OS disks, your sizing estimates depend on how frequently you refresh and recompose the pool.

If you refresh your linked-clone pool between once a day and once a week, make sure that the **Selected Free Space** can accommodate storage use between the **Min Recommended** and **50% Utilization** estimates.

If you rarely refresh or recompose the pool, the linked-clone disks continue to grow. Make sure that the **Selected Free Space** can accommodate storage use between the **50 % Utilization** and **Max Recommended** estimates.

For persistent disks, your sizing estimates depend on the amount of Windows profile data that users generate on their desktops. Refresh and recompose operations do not affect persistent disks.

How View Manager Calculates the Minimum Sizing Recommendations

To arrive at a minimum recommendation for OS disks, View Manager estimates that each clone consumes twice its memory size when it is first created and started up. If no memory is reserved for a clone, an ESX swap file is created for a clone as soon as it is powered on. The size of the guest operating system's paging file also affects the growth of a clone's OS disk.

In the minimum recommendation for OS disks, View Manager also includes space for two replicas on each datastore. View Composer creates one replica when a pool is created. When the pool is recomposed for the first time, View Composer creates a second replica on the datastore, anchors the linked clones to the new replica, and deletes the first replica if no other clones are using original snapshot. The datastore must have the capacity to store two replicas during the recompose operation.

By default, replicas use vSphere thin provisioning, but to keep the guidelines simple, View Manager accounts for two replicas that use the same space as the parent virtual machine.

To arrive at a minimum recommendation for persistent disks, View Manager calculates 20% of the disk size that you specify on the **View Composer Disks** page of the Add Pool wizard.

NOTE The calculations for persistent disks are based on static threshold values, in gigabytes. For example, if you specify a persistent disk size of any value between 1024MB and 2047MB, View Manager calculates the persistent disk size as 1GB. If you specify a disk size of 2048MB, View manager calculates the disk size as 2GB.

To arrive at a recommendation for storing replicas on a separate datastore, View Manager allows space for two replicas on the datastore. The same value is calculated for minimum and maximum usage.

For details, see "Sizing Formulas for Linked-Clone Pools," on page 88.

Sizing Guidelines and Storage Overcommit

After you estimate storage requirements, select datastores, and deploy the pool, View Manager provisions linked-clone virtual machines on different datastores based on the free space and the existing clones on each datastore.

Based on the storage-overcommit option that you select on the **Select Datastores** page in the Add Pool wizard, View Manager stops provisioning new clones and reserves free space for the existing clones. This behavior ensures that a growth buffer exists for each desktop on the datastore.

If you select an aggressive storage-overcommit level, the estimated storage requirements might exceed the capacity shown in the **Selected Free Space** column. The storage-overcommit level affects how many virtual machines that View Manager actually creates on a datastore.

For details, see "Set the Storage Overcommit Level for Linked-Clone Desktops," on page 90.

Sizing Formulas for Linked-Clone Pools

Storage-sizing formulas can help you estimate the size of linked-clone disks relative to the free space on the datastores that you select for OS disks, View Composer persistent disks, and replicas.

Storage Sizing Formulas

Table 5-8 shows the formulas that calculate the estimated sizes of linked-clone disks when you create a pool and as the linked-clone desktops grow over time. These formulas include the space for replica disks that are stored with the clones on the datastore.

If you edit an existing pool or store replicas on a separate datastore, View Manager uses a different sizing formula. See "Sizing Formulas for Creating Linked Clones When You Edit a Pool or Store Replicas on a Separate Datastore," on page 89.

Table 5-8. Storage Sizing Formulas for Linked-Clone Disks on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of VMs * (2 * memory of VM) + (2 * replica disk)	Number of VMs * (50% of replica disk + memory of VM) + (2 * replica disk)	Number of VMs * (100% of replica disk + memory of VM) + (2 * replica disk)
Persistent disks	Free space on the selected datastores	Number of VMs * 20% of persistent disk	Number of VMs * 50% of persistent disk	Number of VMs * 100% of persistent disk

Example of a Storage Sizing Estimate

In this example, the parent virtual machine is configured with 1GB of memory. The parent virtual machine's disk size is 10GB. A linked-clone pool is created with 10 desktops. Persistent disks are configured as 2048MB in size.

The OS disks are configured on a datastore that currently has 184.23GB of available space. The persistent disks are configured on a different datastore with 28.56GB of available space.

Table 5-9 shows how the sizing formulas calculate estimated storage requirements for the sample linked-clone pool.

Table 5-9. Example of a Sizing Estimate for Linked-Clone Disks Deployed on Selected Datastores

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) + (2*10GB) = 40.00	10 * (50% of 10GB + 1GB) + (2*10GB) = 80.00	10 * (100% of 10GB + 1GB) + (2*10GB) = 130.00
Persistent disks	28.56	10 * (20% of 2GB) = 4.00	10 * (50% of 2GB) = 10.00	10 * (100% of 2GB) = 20.00

Sizing Formulas for Creating Linked Clones When You Edit a Pool or Store Replicas on a Separate Datastore

View Manager calculates different sizing formulas when you edit an existing linked-clone pool, or store replicas on a separate datastore, than when you first create a pool.

If you edit an existing pool and select datastores for the pool, View Composer creates new clones on the selected datastores. The new clones are anchored to the existing snapshot and use the existing replica disk. No new replicas are created.

If you store replicas on a separate datastore, the other selected datastores are dedicated to linked-clone disks.

In these cases, View Manager does not include space for replicas when it calculates storage recommendations for linked-clone disks.

Table 5-10 shows the formulas that calculate the estimated sizes of linked-clone disks when you edit a pool or store replicas on a separate datastore.

Table 5-10. Storage Sizing Formulas for Linked-Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	Free space on the selected datastores	Number of VMs * (2 * memory of VM)	Number of VMs * (50% of replica disk + memory of VM)	Number of VMs * (100% of replica disk + memory of VM)
Persistent disks	Free space on the selected datastores	Number of VMs * 20% of persistent disk	Number of VMs * 50% of persistent disk	Number of VMs * 100% of persistent disk

Example of a Storage Sizing Estimate When You Edit a Pool or Store Replicas on a Separate Datastore

In this example, the parent virtual machine is configured with 1GB of memory. The parent virtual machine's disk size is 10GB. A linked-clone pool is created with 10 desktops. Persistent disks are configured as 2048MB in size.

The OS disks are configured on a datastore that currently has 184.23GB of available space. The persistent disks are configured on a different datastore with 28.56GB of available space.

Table 5-11 shows how the sizing formulas calculate estimated storage requirements for the sample linked-clone pool.

Table 5-11. Example of a Sizing Estimate for Linked-Clone Disks When You Edit a Pool or Store Replicas on a Separate Datastore

Data Type	Selected Free Space (GB)	Min Recommended (GB)	50% Utilization (GB)	Max Recommended (GB)
OS disks	184.23	10 * (2*1GB) = 20.00	10 * (50% of 10GB + 1GB) = 60.00	10 * (100% of 10GB + 1GB) = 110.00
Persistent disks	28.56	10 * (20% of 2GB) = 4.00	10 * (50% of 2GB) = 10.00	10 * (100% of 2GB) = 20.00

Set the Storage Overcommit Level for Linked-Clone Desktops

You can control how aggressively View Manager creates linked-clone desktops on a datastore by using the storage overcommit feature. This feature lets you create linked clones that have a total logical size larger than the physical storage limit of the datastore.

This feature works only with linked-clone pools.

The storage overcommit level calculates the amount of storage greater than the physical size of the datastore that the clones would use if each clone were a full virtual machine. For details, see "Storage Overcommit for Linked-Clone Desktops," on page 91.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 When you create a new desktop pool or edit an existing pool, navigate to the Select Datastores page.

Option	Action
New desktop pool	a Click **Add**. b Proceed through the Add Pool wizard until the Select Datastores page is displayed.
Existing desktop pool	a Select the linked-clone pool and click **Edit**. b Click the **vCenter Settings** tab.

3 On the Select Datastores page, select the storage overcommit level.

Option	Description
None	Storage is not overcommitted.
Conservative	4 times the size of the datastore. This is the default level.
Moderate	7 times the size of the datastore.
Aggressive	15 times the size of the datastore.

4 Click **Done**.

5 Click **Finish**.

Storage Overcommit for Linked-Clone Desktops

With the storage overcommit feature, you can reduce storage costs by placing more linked-clone desktops on a datastore than is possible with full virtual-machine desktops. The linked clones can use a logical storage space several times greater than the physical capacity of the datastore.

This feature helps you choose a storage level that lets you overcommit the datastore's capacity and sets a limit on the number of linked clones that View Manager creates. You can avoid either wasting storage by provisioning too conservatively or risking that the linked clones will run out of disk space and cause their desktop applications to fail.

For example, you can create at most ten full virtual machines on a 100GB datastore, if each virtual machine is 10GB. When you create linked clones from a 10GB parent virtual machine, each clone is a fraction of that size.

If you set a conservative overcommit level, View Manager allows the clones to use four times the physical size of the datastore, measuring each clone as if it were the size of the parent virtual machine. On a 100GB datastore, with a 10GB parent, View Manager provisions approximately 40 linked clones. View Manager does not provision more clones, even if the datastore has free space. This limit keeps a growth buffer for the existing clones.

Table 5-12 shows the storage overcommit levels you can set.

Table 5-12. Storage Overcommit Levels

Option	Storage Overcommit Level
None	Storage is not overcommitted.
Conservative	4 times the size of the datastore. This is the default level.
Moderate	7 times the size of the datastore.
Aggressive	15 times the size of the datastore.

Storage overcommit levels provide a high-level guide for determining storage capacity. To determine the best level, monitor the growth of linked clones in your environment.

Set an aggressive level if your OS disks will never grow to their maximum possible size. An aggressive overcommit level demands attention. To make sure that the linked clones do not run out of disk space, you can periodically refresh or rebalance the desktop pool and reduce the linked clones' OS data to its original size.

For example, it would make sense to set an aggressive overcommit level for a floating-assignment desktop pool in which the desktops are set to delete or refresh after logoff.

You can vary storage overcommit levels among different types of datastores to address the different levels of throughput in each datastore. For example, a NAS datastore can have a different setting than a SAN datastore.

Storing View Composer Replicas and Linked Clones on Separate Datastores

You can place View Composer replicas and linked clones on separate datastores with different performance characteristics. This flexible configuration can speed up intensive operations such as provisioning many linked clones at once or running antivirus scans.

For example, you can store the replica virtual machines on a solid-state disk-backed datastore. Solid-state disks have low storage capacity and high read performance, typically supporting 20,000 I/Os per second (IOPS). View Composer creates only one replica for each View Composer base-image snapshot on each ESX cluster, so replicas do not require much storage space. A solid-state disk can improve the speed at which ESX reads a replica's OS disk when a task is performed concurrently on many linked clones.

You can store linked clones on traditional, spinning media-backed datastores. These disks provide lower performance, typically supporting 200 IOPS. They are cheap and provide high storage capacity, which makes them suited for storing the many linked clones in a large pool. ESX does not need to perform intensive, simultaneous read operations on a linked clone.

Configuring replicas and linked clones in this way can reduce the impact of I/O storms that occur when many linked clones are created at once. For example, if you deploy a floating-assignment pool with a delete-desktop-on-logoff policy, and your users start work at the same time, View Manager must concurrently provision new desktops for them.

IMPORTANT This feature is designed for specific storage configurations provided by vendors who offer high-performance disk solutions. Do not store replicas on a separate datastore if your storage hardware does not support high-read performance.

You must follow certain requirements when you store the replica and linked clones in a pool on separate datastores:

- You can specify only one separate replica datastore for a pool.
- If a replica datastore is shared, it must be accessible from all ESX hosts in the cluster.
- If the linked-clone datastores are shared, the replica datastore must be shared. Replicas can reside on a local datastore only if you configure all linked clones on local datastores on the same ESX host.

Availability Considerations for Storing Replicas on a Separate Datastore or Shared Datastores

You can store View Composer replicas on a separate datastore or on the same datastores as linked-clone virtual machines. These configurations affect the availability of the pool in different ways.

When you store replicas on the same datastores as linked clones, to enhance availability, View Composer creates a separate replica on each datastore. If a datastore becomes unavailable, only the linked clones on that datastore are affected. Linked clones on other datastores continue to run.

When you store replicas on a separate datastore, all linked clones in the pool are anchored to the replicas on that datastore. If the datastore becomes unavailable, the entire pool is unavailable.

To enhance the availability of the linked-clone desktops, you can configure a high-availability solution for the datastore on which you store the replicas.

Linked-Clone Desktop Data Disks

View Composer creates more than one data disk to store the components of a linked-clone desktop.

OS Disk

View Composer creates an OS disk for each linked clone. This disk stores the system data that the clone needs to remain linked to the base image and to function as a unique desktop.

QuickPrep Configuration-Data Disk

View Composer creates a second disk with the OS disk. The second disk stores QuickPrep configuration data and other OS-related data that must be preserved during refresh and recompose operations. This disk is small, typically about 20MB. This disk is created whether you use QuickPrep or Sysprep to customize the desktop.

If you configure separate View Composer persistent disks to store user profiles, three disks are associated with each linked clone: the OS disk, the second desktop disk, and the View Composer persistent disk.

The second desktop disk is stored on the same datastore as the OS disk. You cannot configure this disk.

View Composer Persistent Disk

In a dedicated-assignment pool, you can configure separate View Composer persistent disks to store Windows user-profile data. This disk is optional.

Separate persistent disks let you preserve user data and settings. View Composer refresh, recompose, and rebalance operations do not affect persistent disks. You can detach a persistent disk from a linked clone and attach it to another linked clone.

If you do not configure separate persistent disks, the Windows profile is stored in the OS disk. User data and settings are removed during refresh, recompose, and rebalance operations.

You can store persistent disks on the same datastore as the OS disk or on a different datastore.

Disposable-Data Disk

When you create a linked-clone pool, you can configure a separate, nonpersistent disk to store the guest OS's paging and temp files that are generated during user sessions. You must specify the disk size in megabytes.

This disk is optional.

When the linked clone is powered off, View Manager replaces the disposable-data disk with a copy of the original disk that View Composer created with the linked-clone pool. Linked clones can increase in size as users interact with their desktops. Using disposable-data disks can save storage space by slowing the growth of linked clones.

The disposable-data disk is stored on the same datastore as the OS disk.

Manual Desktop Pools

To create a manual desktop pool, View Manager provisions desktops from existing desktop sources. For each desktop in the pool, you select a separate desktop source to deliver View access to clients.

View Manager can use several types of desktop sources in manual pools:

- Virtual machines that are managed by vCenter Server
- Virtual machines that run on VMware Server or another virtualization platform
- Physical computers
- HP Blade PCs

Worksheet for Creating a Manual Desktop Pool

When you create a manual desktop pool, the View Administrator Add Pool wizard prompts you to configure certain options. Use this worksheet to prepare your configuration options before you create the pool.

You can print this worksheet and write down the values you want to specify when you run the Add Pool wizard.

NOTE In a manual pool, you must prepare each desktop source to deliver View desktop access. View Agent must be installed and running on each desktop source.

Table 5-13. Worksheet: Configuration Options for Creating a Manual Desktop Pool

Option	Description	Fill In Your Value Here
User assignment	Choose the type of user assignment: ■ In a dedicated-assignment pool, each user is assigned to a desktop. Users receive the same desktop each time they log in. ■ In a floating-assignment pool, users receive different desktops each time they log in. For details, see "User Assignment in Desktop Pools," on page 100.	
Desktop Sources	The virtual machines or physical computers that you want to use as View desktops in the pool. 1 Decide which type of desktop source you want to use. You can use either virtual machines that are managed by vCenter Server or unmanaged virtual machines, physical computers, and blade PCs. 2 Prepare a list of the vCenter Server virtual machines or unmanaged virtual machines, physical computers, and blade PCs that you want to include in the pool. To use PCoIP with desktop sources that are unmanaged virtual machines, physical computers, or blade PCs, you must use Teradici hardware.	
vCenter Server	The vCenter Server that manages the desktops. This option appears only if the desktop sources are virtual machines that are managed by vCenter Server.	
Pool ID	The pool name that users see when they log in and that identifies the pool in View Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.	
Pool Settings	Settings that determine the desktop state, power status when a virtual machine is not in use, display protocol, Adobe Flash quality, and so on. For details, see "Desktop and Pool Settings," on page 106. For a list of the settings that apply to manual pools, see "Desktop Settings for Manual Pools," on page 96.	

Create a Manual Desktop Pool

You can create a manual desktop pool that provisions desktops from existing virtual machines, physical computers, and HP Blade PCs. You must select the desktop sources that make up View desktops in the pool.

For manual pools with desktops that are managed by vCenter Server, View Manager ensures that a spare desktop is powered so that users can connect to it. The spare desktop is powered on no matter which power policy is in effect.

Prerequisites

- Prepare the desktop sources to deliver View desktop access. In a manual pool, you must prepare each desktop source individually. View Agent must be installed and running on each desktop source.

To prepare virtual machines managed by vCenter Server, see Chapter 4, "Creating and Preparing Virtual Machines," on page 45.

To prepare unmanaged virtual machines, physical computers, and Blade PCs, see Chapter 3, "Preparing Unmanaged Desktop Sources," on page 41.

- Gather the configuration information that you must provide to create the pool. See "Worksheet for Creating a Manual Desktop Pool," on page 93.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop and Pool Settings," on page 106.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Click **Add**.

3 Select **Manual Pool**.

4 Follow the prompts in the wizard to create the pool.

Use the configuration information that you gathered in the worksheet. You can go directly back to any wizard page that you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the desktops as they are added to the pool by clicking **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Add Entitlements to Desktop Pools," on page 115.

Create a Manual Pool That Contains One Desktop

You can create a pool that contains a single desktop when a user requires a unique, dedicated desktop, or when, at different times, multiple users must access a costly application with a single-host license.

You can provision an individual View desktop in its own pool by creating a manual desktop pool and selecting a single desktop source.

To mimic a physical computer that can be shared by multiple users, specify a floating assignment for the users entitled to access the pool.

Whether you configure the single-desktop pool with dedicated or floating assignment, power operations are initiated by session management. The virtual machine is powered on when a user requests the desktop and powered off or suspended when the user logs off.

If you configure the **Ensure desktops are always powered on** policy, the virtual machine remains powered on. If the user shuts down the virtual machine, it immediately restarts.

Prerequisites

- Prepare the desktop source to deliver View desktop access. View Agent must be installed and running on the desktop source.

  To prepare a virtual machine managed by vCenter Server, see Chapter 4, "Creating and Preparing Virtual Machines," on page 45.

  To prepare an unmanaged virtual machine, physical computer, or Blade PC, see Chapter 3, "Preparing Unmanaged Desktop Sources," on page 41.

- Gather the configuration information you must provide to create the manual pool. See "Worksheet for Creating a Manual Desktop Pool," on page 93.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See "Desktop and Pool Settings," on page 106.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Click **Add**.

3 Select **Manual Pool**.

4 Select the type of user assignment.

Option	Description
Dedicated Assignment	The desktop is assigned to one user. Only that user can log in to the desktop.
Floating Assignment	The desktop is shared by all users who are entitled to the pool. Any entitled user can log in to the desktop as long as another user is not logged in.

5 On the Add vCenter Virtual Machines or Add Machines page, select the desktop source for your desktop.

6 Follow the prompts in the wizard to create the pool.

Use the configuration information you gathered in the worksheet. You can go directly back to any wizard page you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the desktop as it is created by clicking **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Add Entitlements to Desktop Pools," on page 115.

Desktop Settings for Manual Pools

You must specify desktop and pool settings when you configure manual pools. Not all settings apply to all types of manual pools.

Table 5-14 lists the settings that apply to manual desktop pools that are configured with these properties:

- Dedicated user assignments
- Floating user assignments
- Managed desktop sources (vCenter Server virtual machines)
- Unmanaged desktop sources

These settings also apply to a manual pool that contains a single desktop.

For descriptions of each desktop setting, see "Desktop and Pool Settings," on page 106.

Table 5-14. Settings for Manual Desktop Pools

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
State	Yes	Yes	Yes	Yes
Connection Server restrictions	Yes	Yes	Yes	Yes
Remote desktop power policy	Yes	Yes		

Table 5-14. Settings for Manual Desktop Pools (Continued)

Setting	Manual Managed Pool, Dedicated Assignment	Manual Managed Pool, Floating Assignment	Manual Unmanaged Pool, Dedicated Assignment	Manual Unmanaged Pool, Floating Assignment
Automatic logoff after disconnect	Yes	Yes	Yes	Yes
Allow users to reset their desktop	Yes	Yes		
Allow multiple sessions per user		Yes		Yes
Default display protocol	Yes	Yes	Yes To use PCoIP with a desktop source that is not managed by vCenter Server, you must install Teradici hardware on the desktop source.	Yes To use PCoIP with a desktop source that is not managed by vCenter Server, you must install Teradici hardware on the desktop source.
Allow users to choose protocol	Yes	Yes	Yes	Yes
Windows 7 3D Rendering	Yes	Yes		
Max number of monitors	Yes	Yes		
Max resolution of any one monitor	Yes	Yes		
Adobe Flash quality	Yes	Yes	Yes	Yes
Adobe Flash throttling	Yes	Yes	Yes	Yes

Microsoft Terminal Services Pools

You can use Microsoft Terminal Servers to provide Terminal Services sessions as desktops to View clients. View Manager manages Terminal Services sessions in the same way that it manages other View desktops.

A Terminal Services pools can contain multiple desktop sources served by one or more terminal servers. A terminal server desktop source can deliver multiple View desktops.

View Manager provides load balancing for the terminal servers in a pool by directing connection requests to the terminal server that has the least number of active sessions.

You entitle a whole Terminal Services pool to users or user groups.

You should deploy a roaming profile solution to propagate user settings and data to the desktop that the user is currently accessing.

NOTE Terminal Services pools support the RDP display protocol only.

Create a Microsoft Terminal Services Pool

You can create a Microsoft Terminal Services pool that provisions desktops from terminal server desktop sources. You must select the desktop sources that make up View desktops in the pool.

Prerequisites

- Prepare the terminal server desktop sources to deliver View desktop access. View Agent must be installed and running on each desktop source. See Chapter 3, "Preparing Unmanaged Desktop Sources," on page 41.
- Make a list of the terminal server desktop sources that you want to include in the pool.
- Decide how to configure desktop settings. See "Desktop Settings for Microsoft Terminal Services Pools," on page 98. For descriptions of each desktop setting, see "Desktop and Pool Settings," on page 106.
- Provide a pool ID that users see when they log in and that identifies the pool in View Administrator. If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Click **Add**.

3 Select **Microsoft Terminal Services Desktop Pool**.

4 Follow the prompts in the wizard to create the pool.

Use the configuration information you gathered in the worksheet. you can go directly back to any wizard page you completed by clicking the page name in the navigation panel.

In View Administrator, you can view the desktops as they are added to the pool by clicking **Inventory > Desktops**.

What to do next

Entitle users to access the pool. See "Add Entitlements to Desktop Pools," on page 115.

Desktop Settings for Microsoft Terminal Services Pools

You must specify desktop and pool settings when you configure Microsoft Terminal Services pools. Not all settings apply to all types of Terminal Services pools.

Table 5-15 lists the settings that apply to Terminal Services pools.

For descriptions of each desktop setting, see "Desktop and Pool Settings," on page 106.

Table 5-15. Settings for Terminal Services Pools

Setting	Microsoft Terminal Services Pool
State	Yes
Connection Server restrictions	Yes
Automatic logoff after disconnect	Yes
Default display protocol	RDP is the only supported display protocol for Terminal Services pools.
Adobe Flash quality	Yes
Adobe Flash throttling	Yes

Configure Adobe Flash Throttling with Internet Explorer in Terminal Services Sessions

To ensure that Adobe Flash throttling works with Internet Explorer in Terminal Services sessions, users must enable third-party browser extensions.

Procedure

1 Start View Client and log in to a user's desktop.

2 In Internet Explorer, click **Tools > Internet Options**.

3 Click the **Advanced** tab, select **Enable third-party browser extensions**, and click **OK**.

4 Restart Internet Explorer.

Provisioning Desktop Pools

When you create a desktop pool, you select configuration options that determine how the pool is managed and how users interact with the desktops.

- User Assignment in Desktop Pools on page 100

  You can configure a desktop pool so that users have dedicated assignments or floating assignments to the desktops in the pool. You must choose a user assignment for automated pools that contain full virtual machines, automated linked-clone pools, and manual pools.

- Naming Desktops Manually or Providing a Naming Pattern on page 100

  You can provision the desktops in an automated pool by manually specifying a list of desktop names or by providing a naming pattern and the number of desktops you want in the pool. These two approaches offer different advantages.

- Manually Customizing Desktops on page 104

  After you create an automated pool, you can customize particular desktops without reassigning ownership. By starting the desktops in maintenance mode, you can modify and test the desktops before you release them to their assigned users or make them available to all entitled users in the pool.

- Desktop and Pool Settings on page 106

  You must specify desktop and pool settings when you configure automated pools that contain full virtual machines, linked-clone desktop pools, manual desktop pools, and Microsoft Terminal Services pools. Not all settings apply to all types of desktop pools.

- Configuring 3D Rendering on Windows 7 Desktops on page 109

  When you create or edit a Windows 7 desktop pool, you can configure 3D graphics rendering for your desktops. When you select this desktop setting, users can take advantage of graphics enhancements that are provided by applications such as AERO, Microsoft Office 2010, and Google Earth.

- Prevent Access to View Desktops Through RDP on page 110

  In certain View environments, it is a priority to prohibit access to View desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access View desktops by configuring pool settings and a group policy setting.

User Assignment in Desktop Pools

You can configure a desktop pool so that users have dedicated assignments or floating assignments to the desktops in the pool. You must choose a user assignment for automated pools that contain full virtual machines, automated linked-clone pools, and manual pools.

With a dedicated assignment, View Manager assigns each entitled user to one desktop in the pool. When a user connects to the pool, the user always logs in to the same desktop. The user's settings and data are saved between sessions. No other user in the pool can access the desktop.

With a floating assignment, View Manager dynamically assigns desktops in the pool to entitled users. Users connect to a different desktop each time they log in. When a user logs off, the desktop is returned to the pool.

You can configure floating-assignment desktops to be deleted when users log off. Automatic deletion lets you keep only as many virtual machines as you need at one time. You can use automatic deletion only in automated pools that you provision with a desktop-naming pattern and a total number of desktops.

Floating-assignment desktops let you reduce software licensing costs.

Naming Desktops Manually or Providing a Naming Pattern

You can provision the desktops in an automated pool by manually specifying a list of desktop names or by providing a naming pattern and the number of desktops you want in the pool. These two approaches offer different advantages.

If you name desktops by specifying a list, you can use your company's naming scheme, and you can associate each desktop name with a user.

If you provide a naming pattern, View Manager can dynamically create and assign desktops as users need them.

You must use one of these naming methods to provision automated pools that contain full virtual machines or linked clones.

Table 5-16 compares the two naming methods, showing how each method affects the way you create and administer a desktop pool.

Table 5-16. Naming Desktops Manually or Providing a Desktop-Naming Pattern

Feature	Providing a Desktop-Naming Pattern	Naming Desktops Manually
Desktop names	View Manager generates desktop names. You provide a naming pattern. View Manager adds a unique number to identify each desktop. For details, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.	You specify a list of desktop names. In a dedicated-assignment pool, you can pair users with desktops by listing user names with the desktop names. For details, see "Specify a List of Desktop Names," on page 101.
Pool size	You specify a maximum number of desktops.	Your list of desktop names determines the number of desktops.
To add desktops to the pool	You can increase the maximum pool size.	You can add desktop names to the list. For details, see "Add Desktops to an Automated Pool Provisioned by a List of Names," on page 207.
On-demand provisioning	Available. View Manager can create and provision a desktop for a user when the user first logs in. View Manager can also create and provision all the desktops when you create the pool.	Not available. View Manager creates and provisions all the desktops that you specify in your list when the pool is created.

Table 5-16. Naming Desktops Manually or Providing a Desktop-Naming Pattern (Continued)

Feature	Providing a Desktop-Naming Pattern	Naming Desktops Manually
Initial customization	Available. When a desktop is provisioned, View Manager can run a customization specification that you select.	Available. When a desktop is provisioned, View Manager can run a customization specification that you select.
Manual customization of dedicated desktops	To customize desktops and return desktop access to your users, you must remove and reassign the ownership of each desktop. Depending on whether you assign desktops on first log in, you might have to perform these steps twice. You cannot start desktops in maintenance mode. After the pool is created, you can manually put the desktops into maintenance mode.	You can customize and test desktops without having to reassign ownership. When you create the pool, you can start all desktops in maintenance mode to prevent users from accessing them. You can customize the desktops and exit maintenance mode to return access to your users. For details, see "Manually Customizing Desktops," on page 104.
Dynamic or fixed pool size	Dynamic. If you remove a user assignment from a desktop in a dedicated-assignment pool, the desktop is returned to the pool of available desktops. If you choose to delete desktops on logoff in a floating-assignment pool, the pool size can grow or shrink depending on the number of active user sessions.	Fixed. The pool contains the number of desktops you provide in the list of desktop names. You cannot select the **Delete desktop on logoff** setting if you name desktops manually.
Spare desktops	You can specify a number of spare desktops that View Manager keeps powered on for new users. View Manager creates new desktops to maintain the specified number. View Manager stops creating spare desktops when it reaches the maximum pool size. View Manager keeps the spare desktops powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy.	You can specify a number of spare desktops that View Manager keeps powered on for new users. View Manager does not create new spare desktops to maintain the specified number. View Manager keeps the spare desktops powered on even when the pool power policy is **Power off** or **Suspend**, or when you do not set a power policy.
User assignment	You can use a naming pattern for dedicated-assignment and floating-assignment pools.	You can specify desktop names for dedicated-assignment and floating-assignment pools. NOTE In a floating-assignment pool, you cannot associate user names with desktop names. The desktops are not dedicated to the associated users. In a floating-assignment pool, all desktops that are not currently in use remain accessible to any user who logs in.

Specify a List of Desktop Names

You can provision an automated desktop pool by manually specifying a list of desktop names. This naming method lets you use your company's naming conventions to identify the desktops in a pool.

When you explicitly specify desktop names, users can see familiar names based on their company's organization when they log in to their desktops.

Follow these guidelines for manually specifying desktop names:

- Type each desktop name on a separate line.
- A desktop name can have up to 15 alphanumeric characters.

- You can add a user name to each desktop entry. Use a comma to separate the user name from the desktop name.

In this example, two desktops are specified. The second desktop is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

NOTE In a floating-assignment pool, you cannot associate user names with desktop names. The desktops are not dedicated to the associated users. In a floating-assignment pool, all desktops that are not currently in use remain accessible to any user who logs in.

Prerequisites

Make sure that each desktop name is unique. You cannot use the names of existing virtual machines in vCenter Server.

Procedure

1 Create a text file that contains the list of desktop names.

   If you intend to create a pool with only a few desktops, you can type the desktop names directly in the Add Pool wizard. You do not have to create a separate text file.

2 In View Administrator start the Add Pool wizard to begin creating an automated desktop pool.

3 On the Provisioning Settings page, select **Specify names manually** and click **Enter names**.

4 Copy your list of desktop names in the Enter Desktop Names page and click **Next**.

   The Enter Desktop Names wizard displays the desktop list and indicates validation errors with a red **X**.

5 Correct invalid desktop names.

   a Place your cursor over an invalid name to display the related error message at the bottom of the page.

   b Click **Back**.

   c Edit the incorrect names and click **Next**.

6 Click **Finish**.

7 (Optional) Select **Start desktops in maintenance mode**.

   This option lets you customize the desktops before users can log in and use them.

8 Follow the prompts in the wizard to finish creating the desktop pool.

View Manager creates a desktop for each name in the list. When an entry includes a desktop and user name, View Manager assigns the desktop to that user.

After the pool is created, you can add desktops by importing another list file that contains additional desktop names and users.

Using a Naming Pattern for Automated Desktop Pools

You can provision the desktops in a pool by providing a naming pattern and the total number of desktops you want in the pool. By default, View Manager uses your pattern as a prefix in all the desktop names and appends a unique number to identify each desktop.

Length of the Naming Pattern in a Desktop Name

Desktop names have a 15-character limit, including your naming pattern and the automatically generated number.

Table 5-17. Maximum Length of the Naming Pattern in a Desktop Name

If You Set This Number of Desktops in the Pool	This Is the Maximum Prefix Length
1-99	13 characters
100-999	12 characters
1,000 or more	11 characters

Names that contain fixed-length tokens have different length limits. See "Length of the Naming Pattern When You Use a Fixed-Length Token," on page 103.

Using a Token in a Desktop Name

You can place the automatically generated number anywhere else in the name by using a token. When you type the pool name, type **n** surrounded by curly brackets to designate the token.

For example: **amber-{n}-desktop**

When View Manager creates a desktop, View Manager replaces **{n}** with a unique number.

You can generate a fixed-length token by typing **{n:fixed=*number of digits*}**.

View Manager replaces the token with numbers containing the specified number of digits.

For example, if you type **amber-{n:fixed=3}**, View Manager replaces **{n:fixed=3}** with a three-digit number and creates these desktop names: **amber-001**, **amber-002**, **amber-003**, and so on.

Length of the Naming Pattern When You Use a Fixed-Length Token

Names that contain fixed-length tokens have a 15-character limit, including your naming pattern and the number of digits in the token.

Table 5-18. Maximum Length of the Naming Pattern When You Use a Fixed-Length Token

Fixed-Length Token	Maximum Length of the Naming Pattern
{n:fixed=1}	14 characters
{n:fixed=2}	13 characters
{n:fixed=3}	12 characters

Desktop-Naming Example

This example shows how to create two automated desktop pools that use the same desktop names, but different sets of numbers. The strategies that are used in this example achieve a specific user objective and show the flexibility of the desktop-naming methods.

The objective is to create two pools with the same naming convention such as VDIABC-*XX*, where *XX* represents a number. Each pool has a different set of sequential numbers. For example, the first pool might contain desktops VDIABC-01 through VDIABC-10. The second pool contains desktops VDIABC-11 through VDIABC-20.

You can use either desktop-naming method to satisfy this objective.

- To create fixed sets of desktops at one time, specify desktop names manually.
- To create desktops dynamically when users log in for the first time, provide a naming pattern and use a token to designate the sequential numbers.

Specifying the Names Manually

1 Prepare a text file for the first pool that contains a list of desktop names from VDIABC-01 through VDIABC-10.

2 In View Administrator, create the pool and specify desktop names manually.

3 Click **Enter Names** and copy your list into the **Enter Desktop Names** list box.

4 Repeat these steps for the second pool, using the names VDIABC-11 through VDIABC-20.

For detailed instructions, see "Specify a List of Desktop Names," on page 101.

You can add desktops to each pool after it is created. For example, you can add desktops VDIABC-21 through VDIABC-30 to the first pool, and VDIABC-31 through VDIABC-40 to the second pool. See "Add Desktops to an Automated Pool Provisioned by a List of Names," on page 207.

Providing a Naming Pattern With a Token

1 In View Administrator, create the first pool and use a naming pattern to provision the desktop names.

2 In the naming-pattern text box, type **`VDIABC-0{n}`**.

3 Limit the pool's maximum size to 9.

4 Repeat these steps for the second pool, but in the naming-pattern text box, type **`VDIABC-1{n}`**.

The first pool contains desktops VDIABC-01 through VDIABC-09. The second pool contains desktops VDIABC-11 through VDIABC-19.

Alternatively, you can configure the pools to contain up to 99 desktops each by using a fixed-length token of 2 digits:

- For the first pool, type **`VDIABC-0{n:fixed=2}`**.
- For the second pool, type **`VDIABC-1{n:fixed=2}`**.

Limit each pool's maximum size to 99. This configuration produces desktops that contain a 3-digit sequential naming pattern.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

For details about naming patterns and tokens, see "Using a Naming Pattern for Automated Desktop Pools," on page 102.

Manually Customizing Desktops

After you create an automated pool, you can customize particular desktops without reassigning ownership. By starting the desktops in maintenance mode, you can modify and test the desktops before you release them to their assigned users or make them available to all entitled users in the pool.

- Customizing Desktops in Maintenance Mode on page 105

  Maintenance mode prevents users from accessing their desktops. If you start desktops in maintenance mode, View Manager places each desktop in maintenance mode when the desktop is created.

- Customize Individual Desktops on page 105

  You can customize individual desktops after a pool is created by starting the desktops in maintenance mode.

Customizing Desktops in Maintenance Mode

Maintenance mode prevents users from accessing their desktops. If you start desktops in maintenance mode, View Manager places each desktop in maintenance mode when the desktop is created.

In a dedicated-assignment pool, you can use maintenance mode to log in to a desktop without having to reassign ownership to your own administrator account. When you finish the customization, you do not have to return ownership to the user assigned to the desktop.

In a floating-assignment pool, you can test desktops in maintenance mode before you let users log in.

To perform the same customization on all desktops in an automated pool, customize the virtual machine you prepare as a template or parent. View Manager deploys your customization to all the desktops. When you create the pool, you can also use a Sysprep customization specification to configure all the desktops with licensing, domain attachment, DHCP settings, and other computer properties.

NOTE You can start desktops in maintenance mode if you manually specify desktop names for the pool, not if you name desktops by providing a naming pattern.

Customize Individual Desktops

You can customize individual desktops after a pool is created by starting the desktops in maintenance mode.

Procedure

1 In View Administrator, begin creating an automated desktop pool by starting the Add Pool wizard.

2 On the Provisioning Settings page, select **Specify names manually**.

3 Select **Start desktops in maintenance mode**.

4 Complete the Add Pool wizard to finish creating the desktop pool.

5 In vCenter Server, log in, customize, and test the individual desktop virtual machines.

You can customize the desktops manually or by using standard Windows systems-management software such as Altiris, SMS, LanDesk, or BMC.

6 In View Administrator, select the desktop pool.

7 Click **Select all** or use the filter tool to select specific desktops to release to your users.

8 Click **More Commands > Exit Maintenance Mode**.

What to do next

Notify your users that they can log in to their desktops.

Desktop and Pool Settings

You must specify desktop and pool settings when you configure automated pools that contain full virtual machines, linked-clone desktop pools, manual desktop pools, and Microsoft Terminal Services pools. Not all settings apply to all types of desktop pools.

Table 5-19. Desktop and Pool Setting Descriptions

Setting	Options
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, and provisioning is stopped for the pool. This is an appropriate setting if you want to conduct post deployment activities such as testing or other forms of baseline maintenance.
Connection Server restrictions	■ **None**. The desktop pool can be accessed by any View Connection Server instance. ■ **With tags**. Select one or more View Connection Server tags to make the desktop pool accessible only to View Connection Server instances that have those tags. You can use the check boxes to select multiple tags.
Remote desktop power policy	Determines how a virtual machine behaves when the user logs off of the associated desktop. For descriptions of the power-policy options, see "Power Policies for Desktop Pools," on page 110. For more information about how power policies affect automated pools, see "Setting Power Policies for Desktop Pools," on page 110.
Automatically 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. Type the duration in minutes. The log off time applies to future disconnections. If a desktop session was already disconnected when you set a log off time, the log off duration for that user starts when you set the log off time, not when the session was originally disconnected. For example, if you set this value to five minutes, and a session was disconnected 10 minutes earlier, View will log off that session five minutes after you set the value.
Allow users to reset their desktops	Allow users to reset their own desktops without administrative assistance.
Allow multiple sessions per user	Allow a user to connect to multiple desktops in the pool at the same time.
Delete desktop after logoff	Select whether to delete floating-assignment, full virtual machine desktops. ■ **No**. Virtual machines remain in the desktop pool after users log off. ■ **Yes**. Virtual machines are powered off and deleted as soon as users log off.

Table 5-19. Desktop and Pool Setting Descriptions (Continued)

Setting	Options
Delete or refresh desktop on logoff	Select whether to delete, refresh, or leave alone floating-assignment, linked-clone desktops. ■ **Never**. Virtual machines remain in the pool and are not refreshed after users log off. ■ **Delete immediately**. Virtual machines are powered off and deleted as soon as users log off. When users log off, View Manager immediately puts virtual machines in a `Deleting` state. ■ **Refresh immediately**. Virtual machines are refreshed as soon as users log off. When users log off, View Manager immediately puts virtual machines in maintenance mode to prevent other users from logging in as the refresh operation begins.
Refresh OS disk after logoff	Select whether and when to refresh the OS disks for dedicated-assignment, linked-clone desktops. ■ **Never**. The OS disk is never refreshed. ■ **Always**. The OS disk is refreshed every time the user logs off. ■ **Every**. The OS disk is refreshed at regular intervals of a specified number of days. Type the number of days. The number of days is counted from the last refresh, or from the initial provisioning if no refresh has occurred yet. For example, if the specified value is **3** days, and three days have passed since the last refresh, the desktop is refreshed after the user logs off. ■ **At**. The OS disk is refreshed when its current size reaches a specified percentage of its maximum allowable size. The maximum size of a linked clone's OS disk is the size of the replica's OS disk. Type the percentage at which refresh operations occur. With the **At** option, the size of the linked clone's OS disk in the datastore is compared to its maximum allowable size. This disk-utilization percentage does not reflect disk usage that you might see inside the desktop's guest operating system. When you refresh the OS disks in a linked-clone pool with dedicated assignment, the View Composer persistent disks are not affected.
Default display protocol	Select the display protocol that you want View Connection Server to use to communicate with View clients. **PCoIP** — The default option wherever it is supported. PCoIP is supported as the display protocol for virtual-machine desktops and physical machines that have Teradici hardware. PCoIP provides an optimized PC experience for the delivery of images, audio, and video content for a wide range of users on the LAN or across the WAN. **Microsoft RDP** — Microsoft Remote Desktop Connection (RDC) uses RDP to transmit data. RDP is a multichannel protocol that allows a user to connect to a computer remotely.
Allow users to choose protocol	Allow users to override the default display protocol for their desktops by using View Client.

Table 5-19. Desktop and Pool Setting Descriptions (Continued)

Setting	Options
Windows 7 3D Rendering	You can select whether to enable 3D graphics rendering if your pool comprises Windows 7 desktops that run on vSphere 5.0 or later, PCoIP is the selected protocol, and the Allow users to choose protocol setting is set to **No**. With Windows 7 3D Rendering, users can take advantage of graphics enhancements that are provided by applications such as AERO, Microsoft Office 2010, and Google Earth. If your View deployment does not run on vSphere 5.0 or later, this setting is not available and is inactive in View Administrator. When you select this feature, you can configure the amount of VRAM that is assigned to desktops in the pool. You can select at most two monitors for your View desktops. The maximum resolution of any one monitor is set to 1920x1200 pixels. You cannot configure this value. **NOTE** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect. For more information, see "Configuring 3D Rendering on Windows 7 Desktops," on page 109.
Max number of monitors	If you use PCoIP as the display protocol, you can select the maximum number of monitors on which users can display the desktop. When the Windows 7 3D Rendering setting is not selected, the Max number of monitors setting affects the amount of VRAM that is assigned to desktops in the pool. When you increase the number of monitors, more memory is consumed on the associated ESX hosts. When the Windows 7 3D Rendering setting is selected, you can select at most two monitors. **NOTE** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.
Max resolution of any one monitor	If you use PCoIP as the display protocol and you do not select the Windows 7 3D Rendering setting, you should specify the maximum resolution of any one monitor. When the Windows 7 3D Rendering setting is not selected, the Max resolution of any one monitor setting affects the amount of VRAM that is assigned to desktops in the pool. When you increase the resolution, more memory is consumed on the associated ESX hosts. When the Windows 7 3D Rendering setting is selected, you cannot change the maximum resolution of any one monitor. The resolution is set to 1920x1200 pixels. **NOTE** You must power off and on existing virtual machines for this setting to take effect. Restarting a virtual machine does not cause the setting to take effect.

Table 5-19. Desktop and Pool Setting Descriptions (Continued)

Setting	Options
Adobe Flash quality	Determines the quality of Adobe Flash content that is displayed on Web pages. ■ **Do not control**. Quality is determined by Web page settings. ■ **Low**. This setting results in the most bandwidth savings. If no quality level is specified, the system defaults to Low. ■ **Medium**. This setting results in moderate bandwidth savings. ■ **High**. This setting results in the least bandwidth savings. For more information, see "Adobe Flash Quality and Throttling," on page 210.
Adobe Flash throttling	Determines the frame rate of Adobe Flash movies. If you enable this setting, you can reduce or increase the number of frames displayed per second by selecting an aggressiveness level. ■ **Disabled**. No throttling is performed. The timer interval is not modified. ■ **Conservative**. Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames. ■ **Moderate**. Timer interval is 500 milliseconds. ■ **Aggressive**. Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames. For more information, see "Adobe Flash Quality and Throttling," on page 210.

NOTE Properties set for local desktops do not take effect until the desktops are checked back in.

Configuring 3D Rendering on Windows 7 Desktops

When you create or edit a Windows 7 desktop pool, you can configure 3D graphics rendering for your desktops. When you select this desktop setting, users can take advantage of graphics enhancements that are provided by applications such as AERO, Microsoft Office 2010, and Google Earth.

To enable 3D graphics rendering, your pool deployment must meet the following requirements:

- The desktops must run on ESXi 5.0 or later hosts and be managed by vCenter Server 5.0 or later software
- The desktops must be Windows 7 or later
- The desktops must have virtual hardware v8 or later
- The pool must use the PCoIP as the default display protocol
- Users must not be allowed to choose their own protocol

When you enable the Windows 7 3D Rendering setting, you can configure the amount of VRAM that is assigned to the desktops in the pool by moving the slider in the Configure VRAM for 3D guests dialog box. The default VRAM size is 64MB, the minimum size. You can configure the amount of VRAM up to a maximum of 128MB.

The VRAM settings that you configure in View Administrator take precedence over the VRAM settings that can be configured for the virtual machines in vSphere Client.

When you enable the Windows 7 3D Rendering setting, you can configure the Max number of monitors setting for one or two monitors. You cannot select more than two monitors. Also, the Max resolution of any one monitor setting is set to 1920x1200 pixels. You cannot configure this value.

Prevent Access to View Desktops Through RDP

In certain View environments, it is a priority to prohibit access to View desktops through the RDP display protocol. You can prevent users and administrators from using RDP to access View desktops by configuring pool settings and a group policy setting.

NOTE Remote Desktop Services, called Terminal Services on Windows XP systems, must be started on the virtual machine that you use to create pools and on View desktops. Remote Desktop Services are required for View Agent installation, SSO, and other View session-management operations.

Prerequisites

Verify that the VMware View Agent Configuration Administrative Template file is installed in Active Directory. See "Using the View Group Policy Administrative Template Files," on page 142.

Procedure

1 Select PCoIP as the display protocol that you want View Connection Server to use to communicate with View clients.

Option	Description
Create a desktop pool	a In View Administrator, start the Add Pool wizard. b On the Desktop Settings page, select **PCoIP** as the default display protocol.
Edit an existing desktop pool	a In View Administrator, select the desktop pool and click **Edit**. b Select the Pool Settings tab and select **PCoIP** as the default display protocol.

2 For the **Allow users to choose protocol** setting, select **No**.

3 Prevent non-View clients from connecting directly to View desktops through RDP by disabling the `AllowDirectRDP` group policy setting.

   a On your Active Directory server, open the Group Policy Management Console and select **Computer Configuration > Administrative Templates > VMware View Agent Configuration**.

   b Disable the `AllowDirectRDP` setting.

Setting Power Policies for Desktop Pools

You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server.

Power policies control how a virtual machine behaves when its associated desktop is not in use. A desktop is considered not in use before a user logs in and after a user disconnects or logs off. Power policies also control how a virtual machine behaves after administrative tasks such as refresh, recompose, and rebalance are completed.

You configure power policies when you create or edit desktop pools in View Administrator. See Chapter 5, "Creating Desktop Pools," on page 71 or "Managing Desktop Pools," on page 205 for more information.

NOTE You cannot configure power policies for desktop pools that have unmanaged desktops.

Power Policies for Desktop Pools

Power policies control how a virtual machine behaves when the associated View desktop is not in use.

You set power policies when you create or edit a desktop pool. Table 5-20 describes the available power policies.

Table 5-20. Power Policies

Power Policy	Description
Take no power action	View Manager does not enforce any power policy after a user logs off. This setting has two consequences. ■ View Manager does not change the power state of the virtual machine after a user logs off. For example, if a user shuts down the virtual machine, the virtual machine remains powered off. If a user logs off without shutting down, the virtual machine remains powered on. The virtual machine restarts when a user connects to the desktop. ■ View Manager does not enforce any power state after an administrative task is completed. For example, a user might log off without shutting down. The virtual machine remains powered on. When a scheduled recomposition takes place, the virtual machine is powered off. After the recomposition is completed, View Manager does nothing to change the power state of the virtual machine. It remains powered off.
Ensure desktops are always powered on	The virtual machine remains powered on, even when it is not in use. If a user shuts down the virtual machine, it immediately restarts. The virtual machine also restarts after an administrative task such as refresh, recompose, or rebalance is completed. Select **Ensure desktops are always powered on** if you run batch processes or system management tools that must contact the virtual machines at scheduled times.
Suspend	The virtual machine enters a suspended state when a user logs off, but not when a user disconnects.
Power off	The virtual machine shuts down when a user logs off, but not when a user disconnects.

NOTE When you add a desktop to a manual pool, View Manager powers on the desktop to ensure that it is fully configured, even when you select the **Power off** or **Take no power action** power policy. After View Agent is configured, it is marked as Ready, and the normal power-management settings for the pool apply.

For manual pools with desktops that are managed by vCenter Server, View Manager ensures that a spare desktop is powered on so that users can connect to it. The spare desktop is powered on no matter which power policy is in effect.

Table 5-21 describes when View Manager applies the configured power policy.

Table 5-21. When View Manager Applies the Power Policy

Desktop Pool Type	The power policy is applied ...
Manual pool that contains one desktop (vCenter Server-managed virtual machine)	Power operations are initiated by session management. The virtual machine is powered on when a user requests the desktop and powered off or suspended when the user logs off. NOTE The **Ensure desktops are always powered on** policy always applies, whether the single-desktop pool uses floating or dedicated assignment, and whether the desktop is assigned or unassigned.
Automated pool with dedicated assignment	To unassigned desktops only. On assigned desktops, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned desktop and are powered off or suspended when the user logs off. NOTE The **Ensure desktops are always powered on** policy applies to assigned and unassigned desktops.
Automated pool with floating assignment	When a desktop is not in use and after a user logs off. When you configure the **Power off** or **Suspend** power policy for a floating-assignment desktop pool, set **Automatic logoff after disconnect** to **Immediately** to prevent discarded or orphaned sessions.
Manual pool with dedicated assignment	To unassigned desktops only. On assigned desktops, power operations are initiated by session management. Virtual machines are powered on when a user requests an assigned desktop and are powered off or suspended when the user logs off. NOTE The **Ensure desktops are always powered on** policy applies to assigned and unassigned desktops.
Manual pool with floating assignment	When a desktop is not in use and after a user logs off. When you configure the **Power off** or **Suspend** power policy for a floating-assignment desktop pool, set **Automatic logoff after disconnect** to **Immediately** to prevent discarded or orphaned sessions.

How View Manager applies the configured power policy to automated pools depends on whether a desktop is available. See "How Power Policies Affect Automated Pools," on page 112 for more information.

How Power Policies Affect Automated Pools

How View applies the configured power policy to automated pools depends on whether a View desktop is available.

A desktop in an automated pool is considered available when it meets the following criteria:

- Is active
- Does not contain a user session
- Is not assigned to a user

The View Agent service running on the desktop confirms the availability of the desktop to View Connection Server.

When you configure an automated pool, you can specify the minimum and maximum number of virtual machines that must be provisioned and the number of spare desktops that must be kept powered on and available at any given time.

Power Policy Examples for Automated Pools with Floating Assignments

When you configure an automated pool with floating assignments, you can specify that a particular number of View desktops must be available at a given time. The spare, available desktops are always powered on, no matter how the pool policy is set.

Power Policy Example 1

Table 5-22 describes the floating-assignment, automated pool in this example. The pool uses a desktop-naming pattern to provision and name the desktops.

Table 5-22. Desktop Pool Settings for Automated Pool with Floating Assignment Example 1

Desktop Pool Setting	Value
Number of desktops (minimum)	10
Number of desktops (maximum)	20
Number of spare, powered-on desktops	2
Remote desktop power policy	Suspend

When this desktop pool is provisioned, 10 desktops are created, two desktops are powered on and immediately available, and eight desktops are in a suspended state.

For each new user that connects to the pool, a desktop is powered on to maintain the number of spare, available desktops. When the number of connected users exceeds eight, additional desktops, up to the maximum of 20, are created to maintain the number of spare desktops. After the maximum number is reached, the desktops of the first two users who disconnect remain powered on to maintain the number of spare desktops. The desktop of each subsequent user is suspended according to the power policy.

Power Policy Example 2

Table 5-23 describes the floating-assignment, automated pool in this example. The pool uses a desktop-naming pattern to provision and name the desktops.

Table 5-23. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2

Desktop Pool Setting	Value
Number of desktops (minimum)	5
Number of desktops (maximum)	5
Number of spare, powered-on desktops	2
Remote desktop power policy	Suspend

When this desktop pool is provisioned, five desktops are created, two desktops are powered on and immediately available, and three desktops are in a suspended state.

If a fourth desktop in this pool is suspended, one of the existing desktops is resumed. An additional desktop is not powered on because the maximum of number of desktops has already been reached.

Power Policy Example for Automated Pools with Dedicated Assignments

Unlike a powered-on View desktop in an automated pool with floating assignments, a powered-on desktop in an automated pool with dedicated assignments is not necessarily available. It is available only if the desktop is not assigned to a user.

Table 5-24 describes the dedicated-assignment, automated pool in this example.

Table 5-24. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example

Desktop Pool Setting	Value
Number of desktops (minimum)	3
Number of desktops (maximum)	5
Number of spare, powered-on desktops	2
Remote desktop power policy	Ensure desktops are always powered on

When this desktop pool is provisioned, three desktops are created and powered on. If the desktops are powered off in vCenter Server, they are immediately powered on again, according to the power policy.

After a user connects to a desktop in the pool, the desktop becomes permanently assigned to that user. After the user disconnects from the desktop, the desktop is no longer available to any other user. However, the **Ensure desktops are always powered on** policy still applies. If the assigned desktop is powered off in vCenter Server, it is immediately powered on again.

When another user connects, a second desktop is assigned. Because the number of spare desktops falls below the limit when the second user connects, another desktop is created and powered on. An additional desktop is created and powered on each time a new user is assigned until the maximum desktop limit is reached.

Preventing View Power Policy Conflicts

When you use View Administrator to configure a power policy, you must compare the power policy to the settings in the guest operating system's Power Options control panel to prevent power policy conflicts.

A View desktop can become temporarily inaccessible if the power policy configured for the virtual machine desktop is not compatible with a power option configured for the guest operating system. If there are other desktops in the same pool, they can also be affected.

The following configuration is an example of a power policy conflict:

- In View Administrator, the power policy **Suspend** is configured for the virtual machine desktop. This policy causes the virtual machine to enter a suspended state when it is not in use.
- In the Power Options control panel in the guest operating system, the option **Put the Computer to sleep** is set to three minutes.

In this configuration, both View Connection Server and the guest operating system can suspend the virtual machine. The guest operating system power option might cause the virtual machine to be unavailable when View Connection Server expects it to be powered on.

Entitling Users and Groups

6

You configure desktop pool entitlements to control which View desktops your users can access. You can also configure the restricted entitlements feature to control desktop access based on the View Connection Server instance that users connect to when they select desktops.

This chapter includes the following topics:

Add Entitlements to Desktop Pools

Before users can access a View desktop, they must be entitled to use a desktop pool.

Prerequisites

Create a desktop pool. See Chapter 5, "Creating Desktop Pools," on page 71.

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 Select the desktop pool and click **Entitlements**.

3 Click **Add**, select one or more search criteria, and then click **Find** to find users or groups based on your search criteria.

NOTE Domain local groups are filtered out of search results for mixed-mode domains. You cannot entitle users in domain local groups if your domain is configured in mixed mode.

4 Select the users or groups you want to entitle to the desktops in the pool and click **OK**.

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

Remove Entitlements from a Desktop Pool

You can remove entitlements from a desktop pool to prevent specific users or groups from accessing a desktop.

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 Select the desktop pool and click **Entitlements**.

3 Select the user or group whose entitlement you want to remove and click **Remove**.

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

Review Desktop Pool Entitlements

You can review the desktop pools that a user or group is entitled to.

Procedure

1 In View Administrator, select **Users and Groups** and click the name of the user or group.

2 Select the **Summary** tab.

The Pool Entitlements pane lists the pools that the user or group is currently entitled to.

Restricting View Desktop Access

You can configure the restricted entitlements feature to restrict View desktop access based on the View Connection Server instance that users connect to when they select desktops.

With restricted entitlements, you assign one or more tags to a View Connection Server instance. Then, when configuring a desktop pool, you select the tags of the View Connection Server instances that you want to be able to access the desktop pool.

When users log in through a tagged View Connection Server instance, they can access only those desktop pools that have at least one matching tag or no tags.

- Restricted Entitlement Example on page 116

  This example shows a View deployment that includes two View Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

- Tag Matching on page 117

  The restricted entitlements feature uses tag matching to determine whether a View Connection Server instance can access a particular desktop pool.

- Considerations and Limitations for Restricted Entitlements on page 118

  Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- Assign a Tag to a View Connection Server Instance on page 118

  When you assign a tag to a View Connection Server instance, users who connect to that View Connection Server can access only those desktop pools that have a matching tag or no tags.

- Assign a Tag to a Desktop Pool on page 118

  When you assign a tag to a desktop pool, only users who connect to a View Connection Server instance that has a matching tag can access the desktops in that pool.

Restricted Entitlement Example

This example shows a View deployment that includes two View Connection Server instances. The first instance supports internal users. The second instance is paired with a security server and supports external users.

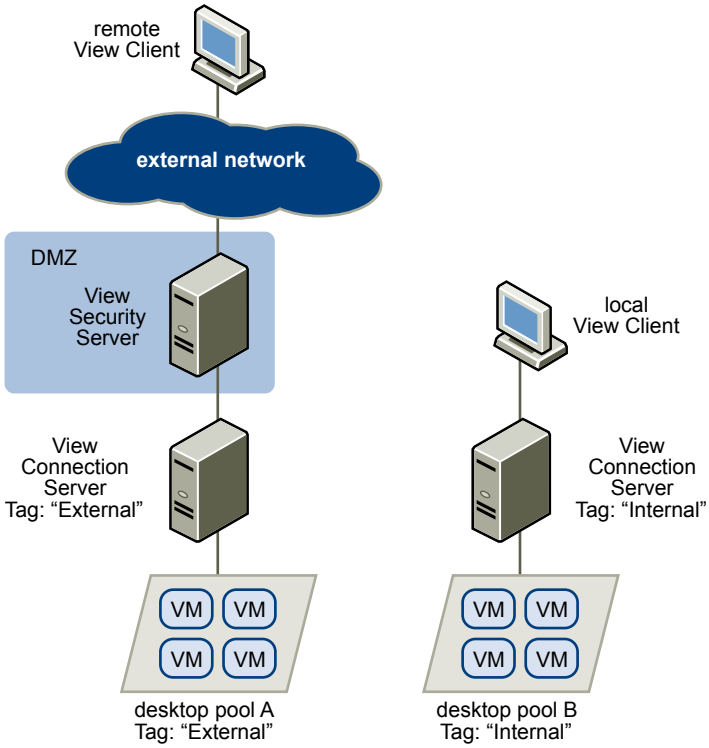
To prevent external users from accessing certain desktops, you could set up restricted entitlements as follows:

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

- Assign the "External" tag to the desktop pools that should be accessible only to external users.

External users cannot see the desktop pools tagged as Internal because they log in through the View Connection Server tagged as External, and internal users cannot see the desktop pools tagged as External because they log in through the View Connection Server tagged as Internal. Figure 6-1 illustrates this configuration.

Figure 6-1. Restricted Entitlement Configuration



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

Tag Matching

The restricted entitlements feature uses tag matching to determine whether a View Connection Server instance can access a particular desktop pool.

At the most basic level, tag matching determines that a View Connection Server instance with a specific tag can access a desktop pool that has the same tag.

The absence of tag assignments can also affect whether a View Connection Server instance can access a desktop pool. For example, View Connection Server instances that do not have any tags can only access desktop pools that also do not have any tags.

Table 6-1 shows how the restricted entitlement feature determines when a View Connection Server can access a desktop pool.

Table 6-1. Tag Matching Rules

View Connection Server	Desktop Pool	Access Permitted?
No tags	No tags	Yes
No tags	One or more tags	No

Table 6-1. Tag Matching Rules (Continued)

View Connection Server	Desktop Pool	Access Permitted?
One or more tags	No tags	Yes
One or more tags	One or more tags	Only when tags match

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

Considerations and Limitations for Restricted Entitlements

Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- A single View Connection Server instance or desktop pool can have multiple tags.
- Multiple View Connection Server instances and desktop pools can have the same tag.
- Desktop pools that do not have any tags can be accessed by any View Connection Server instance.
- View Connection Server instances that do not have any tags can only access desktop pools that also do not have any tags.
- If you use a security server, you must configure restricted entitlements on the View Connection Server instance the security server is paired with. You cannot configure restricted entitlements on a security server.
- You cannot modify or remove a tag from a View Connection Server instance if that tag is still assigned to a desktop pool and no other View Connection Server instances have a matching tag.
- Restricted entitlements take precedence over other desktop entitlements. For example, even if a user is entitled to a particular desktop, the user will not be able to access that desktop if the desktop pool's tag does not match the tag assigned to the View Connection Server instance that the user connected to.

Assign a Tag to a View Connection Server Instance

When you assign a tag to a View Connection Server instance, users who connect to that View Connection Server can access only those desktop pools that have a matching tag or no tags.

Procedure

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

2 In View Connection Servers, select the View Connection Server instance and click **Edit**.

3 Type one or more tags in the **Tags** text box.

Separate multiple tags with a comma or semicolon.

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

What to do next

Assign the tag to desktop pools.

Assign a Tag to a Desktop Pool

When you assign a tag to a desktop pool, only users who connect to a View Connection Server instance that has a matching tag can access the desktops in that pool.

You can assign a tag when you add or edit a desktop pool.

Prerequisites

Assign tags to one or more View Connection Server instances.

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 Select the pool that you want to assign a tag to.

Option	Action
Assign a tag to a new pool	Click **Add** to start the Add Pool wizard and define and identify the pool.
Assign a tag to an existing pool	Select the pool and click **Edit**.

3 Go to the Pool Settings page.

Option	Action
Pool settings for a new pool	Click **Pool Settings** in the Add Pool wizard.
Pool settings for an existing pool	Select the **Pool Settings** tab.

4 Click **Browse** next to **Connection Server restrictions** and configure the View Connection Server instances that can access the desktop pool.

Option	Action
Make the pool accessible to any View Connection Server instance	Select **No Restrictions**.
Make the pool accessible only to View Connection Server instances that have those tags	Select **Restrict to these tags** and select one or more tags. You can use the check boxes to select multiple tags.

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

Setting Up User Authentication 7

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

This chapter includes the following topics:

Using Smart Card Authentication

You can configure a View Connection Server instance or security server so that View desktop users can authenticate by using smart cards. Smart cards are sometimes referred to as Common Access Cards (CACs).

A smart card is a small plastic card that contains a computer chip. The chip, which is like a miniature computer, includes secure storage for data, including private keys and public key certificates.

With smart card authentication, a user inserts a smart card into a smart card reader attached to the client computer and enters a PIN. Smart card authentication provides two-factor authentication by verifying both what the user has (the smart card) and what the user knows (the PIN).

See the *VMware View Installation* document for information on hardware and software requirements for implementing smart card authentication. The Microsoft TechNet Web site includes detailed information on planning and implementing smart card authentication for Windows systems.

Smart card authentication is not supported by View Client for Mac or View Administrator. See the *VMware View Architecture Planning* document for complete information on smart card support.

Logging In with a Smart Card

When a user inserts a smart card into a smart card reader, the user certificates on the smart card are copied to the local certificate store on the client system. The certificates in the local certificate store are available to all of the applications running on the client computer, including the View client application.

When a user initiates a connection to a View Connection Server instance or security server that is configured for smart card authentication, the View Connection Server instance or security server sends a list of trusted certificate authorities (CAs) to the View client. The View client checks the list of trusted CAs against the available user certificates, selects a suitable certificate, and then prompts the user to enter a smart card PIN. If there are multiple valid user certificates, the View client prompts the user to select a certificate.

The View client sends the user certificate to the View Connection Server instance or security server, which verifies the certificate by checking the certificate trust and validity period. Typically, users can successfully authenticate if their user certificate is signed and valid. If certificate revocation checking is configured, users who have revoked user certificates are prevented from authenticating.

Display protocol switching is not supported with smart card authentication. To change display protocols after authenticating with a smart card, a user must log off and log in again.

Logging In to Local Desktops with Offline Smart Card Authentication

With offline smart card authentication, users can log in to a local desktop with a smart card when the desktop is not connected to View Connection Server.

To use offline smart card authentication, users must use the same authentication method that they used to authenticate to View Connection Server the last time they logged in. For example, if a user logged in with smart card A, logged in again with password authentication, and then logged in a final time with smart card B, the user must use smart card B to authenticate with offline smart card authentication.

The most recent value of the smart card removal policy is enforced during offline smart card authentication. The smart card removal policy determines whether users must reauthenticate to gain access to their desktops after removing their smart cards. If the policy is set to disconnect user sessions on smart card removal, when users remove a smart card, the guest operating system in the View desktop is locked. The View Client window remains open, and users can select **Options > Send Ctrl-Alt-Delete** to log in again. The smart card removal policy is a View Connection Server setting.

Configure Smart Card Authentication

To configure smart card authentication, you must obtain a root certificate and add it to a server truststore file, modify View Connection Server configuration properties, and configure smart card authentication settings. Depending on your particular environment, you might need to perform additional steps.

Procedure

1 Obtain the Root Certificate from the CA on page 123

You must obtain the root certificate from the CA that signed the certificates on the smart cards presented by your users.

2 Export a Root Certificate from a User Certificate on page 123

If you have a CA-signed user certificate or a smart card that contains one, you can export the root certificate if it is trusted by your system.

3 Add the Root Certificate to a Server Truststore File on page 124

You must add the root certificate for all trusted users to a server truststore file so that View Connection Server instances and security servers can authenticate smart card users and connect them to their View desktops.

4 Modify View Connection Server Configuration Properties on page 124

To enable smart card authentication, you must modify View Connection Server configuration properties on your View Connection Server or security server host.

5 Configure Smart Card Settings in View Administrator on page 125

You can use View Administrator to specify settings to accommodate different smart card authentication scenarios.

Obtain the Root Certificate from the CA

You must obtain the root certificate from the CA that signed the certificates on the smart cards presented by your users.

If you do not have the root certificate of the CA that signed the certificates on the smart cards presented by your users, you can export a root certificate from a CA-signed user certificate or a smart card that contains one. See "Export a Root Certificate from a User Certificate," on page 123.

Procedure

1 Obtain the root certificate from one of the following sources.

- A Microsoft IIS server running Microsoft Certificate Services. See the Microsoft TechNet Web site for information on installing Microsoft IIS, issuing certificates, and distributing certificates in your organization.
- The public root certificate of a trusted CA. This is the most common source of a root certificate in environments that already have a smart card infrastructure and a standardized approach to smart card distribution and authentication.

2 Select a certificate to use for smart card authentication.

The signing chain lists a series a signing authorities. The best certificate to select is usually the intermediate authority above the user certificate.

3 Verify that the authority does not sign other certificates on the card.

What to do next

Add the root certificate to a server truststore file. See "Add the Root Certificate to a Server Truststore File," on page 124.

Export a Root Certificate from a User Certificate

If you have a CA-signed user certificate or a smart card that contains one, you can export the root certificate if it is trusted by your system.

Procedure

1 If the user certificate is on a smart card, insert the smart card into the reader to add the user certificate to your personal store.

If the user certificate does not appear in your personal store, use the reader software to export the user certificate to a file.

2 In Internet Explorer, select **Tools > Internet Options**.

3 On the **Content** tab, click **Certificates**.

4 On the **Personal** tab, select the certificate you want to use and click **View**.

If the user certificate does not appear on the list, click **Import** to manually import it from a file. After the certificate is imported, you can select it from the list.

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

If the user certificate is signed as part of a trust hierarchy, the signing certificate might be signed by another higher-level certificate. Select the parent certificate (the one that actually signed the user certificate) as your root certificate.

6 On the **Details** tab, click **Copy to File**.

The Certificate Export Wizard appears.

7 Click **Next > Next** and type a name and location for the file that you want to export.

8 Click **Next** to save the file as a root certificate in the specified location.

What to do next

Add the root certificate to a server truststore file.

Add the Root Certificate to a Server Truststore File

You must add the root certificate for all trusted users to a server truststore file so that View Connection Server instances and security servers can authenticate smart card users and connect them to their View desktops.

Prerequisites

- Obtain the root certificate from the CA that signed the certificates on the smart cards presented by your users. See "Obtain the Root Certificate from the CA," on page 123.
- Verify that the `keytool` utility is added to the system path on your View Connection Server or security server host. See the *VMware View Installation* document for more information.

Procedure

1 On your View Connection Server or security server host, use the `keytool` utility to import the root certificate into the server truststore file.

For example: **`keytool -import -alias`** ***`alias`*** **`-file`** ***`root_certificate`*** **`-keystore`** ***`truststorefile.key`***

In this command, *alias* is a unique case-insensitive name for a new entry in the truststore file, *root_certificate* is the root certificate that you obtained or exported, and *truststorefile.key* is the name of the truststore file that you are adding the root certificate to. If the file does not exist, it is created in the current directory.

NOTE The `keytool` utility might prompt you to create a password for the truststore file. You will be asked to provide this password if you need to add additional certificates to the truststore file at a later time.

---

2 Copy the truststore file to the SSL gateway configuration folder on the View Connection Server or security server host.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`*`truststorefile.key`*

What to do next

Modify View Connection Server configuration properties to enable smart card authentication.

Modify View Connection Server Configuration Properties

To enable smart card authentication, you must modify View Connection Server configuration properties on your View Connection Server or security server host.

Prerequisites

Add the root certificate for all trusted users to a server truststore file.

Procedure

1 Create or edit the `locked.properties` file in SSL gateway configuration folder on the View Connection Server or security server host.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `trustKeyfile`, `trustStoretype`, and `useCertAuth` properties to the `locked.properties` file.

   a Set `trustKeyfile` to the name of your truststore file.

   b Set `trustStoretype` to **`JKS`**.

   c Set `useCertAuth` to **`true`** to enable certificate authentication.

3 Restart the View Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

The file shown specifies that the root certificate for all trusted users is located in the file `lonqa.key`, sets the trust store type to JKS, and enables certificate authentication.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
```

What to do next

If you configured smart card authentication for a View Connection Server instance, configure smart card authentication settings in View Administrator. You do not need to configure smart card authentication settings for a security server. A security server that has been configured for smart card authentication always requires users to authenticate with a smart card and PIN during login.

Configure Smart Card Settings in View Administrator

You can use View Administrator to specify settings to accommodate different smart card authentication scenarios.

These settings do not apply to security servers. A security server that has been configured for smart card authentication always requires users to authenticate with a smart card and PIN during login.

Prerequisites

- Modify View Connection Server configuration properties on your View Connection Server host.
- Verify that the **Require SSL for client connections and View Administrator** check box is selected in the Global Settings dialog box in View Administrator. You cannot configure smart card authentication options if this check box is deselected.

Procedure

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

2 Select the View Connection Server instance and click **Edit**.

3 On the **Authentication** tab, select a configuration option from the **Smart card authentication** drop-down menu.

Option	Action
Not Allowed	Smart card authentication is disabled on the View Connection Server instance.
Optional	Users can use smart card authentication or password authentication to connect to the View Connection Server instance. If smart card authentication fails, the user must provide a password.
Required	Users are required to use smart card authentication when connecting to the View Connection Server instance. When smart card authentication is required, authentication fails for users who select the **Log in as current user** check box when they connect to the View Connection Server instance. These users must reauthenticate with their smart card and PIN when they log in to View Connection Server. NOTE Smart card authentication replaces Windows password authentication only. If SecurID is enabled, users are required to authenticate by using both SecurID and smart card authentication.

4 Configure the smart card removal policy.

You cannot configure the smart card removal policy when smart card authentication is set to **Not Allowed**.

Option	Action
Disconnect users from View Connection Server when they remove their smart cards	Select the **Disconnect user sessions on smart card removal** check box.
Keep users connected to View Connection Server when they remove their smart cards and let them start new desktop sessions without reauthenticating	Deselect the **Disconnect user sessions on smart card removal** check box.

The smart card removal policy does not apply to users who connect to the View Connection Server instance with the **Log in as current user** check box selected, even if they log in to their client system with a smart card.

For users who run View desktops locally on their client systems, if the policy is set to disconnect user sessions on smart card removal, when users remove a smart card, the guest operating system in the View desktop is locked. The View Client window remains open, and users can select **Options > Send Ctrl-Alt-Delete** to reauthenticate.

5 Click **OK**.

6 Restart the View Connection Server service.

You must restart the View Connection Server service for changes to smart card settings to take effect, with one exception. You can change the **Smart card authentication** setting between **Optional** and **Required** without having to restart the View Connection Server service.

Currently logged in users are not affected by changes to smart card settings.

What to do next

Prepare Active Directory for smart card authentication, if required. See "Prepare Active Directory for Smart Card Authentication," on page 127.

Verify your smart card authentication configuration. See "Verify Your Smart Card Authentication Configuration," on page 129.

Prepare Active Directory for Smart Card Authentication

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

- Add UPNs for Smart Card Users on page 127

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

- Add the Root Certificate to the Enterprise NTAuth Store on page 128

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

- Add the Root Certificate to Trusted Root Certification Authorities on page 128

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

- Add an Intermediate Certificate to Intermediate Certification Authorities on page 128

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

Add UPNs for Smart Card Users

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

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

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

Prerequisites

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

Procedure

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

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

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

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

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

Add the Root Certificate to the Enterprise NTAuth Store

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

Procedure

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

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

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

Add the Root Certificate to Trusted Root Certification Authorities

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

Procedure

1. On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click your domain and click **Properties**.
3. On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.
4. Right-click **Default Domain Policy** and click **Edit**.
5. Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.
6. Right-click **Trusted Root Certification Authorities** and select **Import**.
7. Follow the prompts in the wizard to import the root certificate (for example, `rootCA.cer`) and click **OK**.
8. Close the Group Policy window.

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

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See "Add an Intermediate Certificate to Intermediate Certification Authorities," on page 128.

Add an Intermediate Certificate to Intermediate Certification Authorities

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

Procedure

1. On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click your domain and click **Properties**.
3. On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.
4. Right-click **Default Domain Policy**, and click **Edit**.

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

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

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

8 Close the Group Policy window.

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

Verify Your Smart Card Authentication Configuration

After you set up smart card authentication for the first time, or when smart card authentication is not working correctly, you should verify your smart card authentication configuration.

Procedure

- Verify that each client system has View Client, smart card middleware, a smart card with a valid certificate, and a smart card reader.

  See the documentation provided by your smart card vendor for information on configuring smart card software and hardware.

- On each client system, select **Start > Settings > Control Panel > Internet Options > Content > Certificates > Personal** to verify that certificates are available for smart card authentication.

  When a user inserts a smart card into the smart card reader, Windows copies certificates from the smart card to the user's computer so that View Client can use them.

- In the `locked.properties` file on the View Connection Server or security server host, verify that the `useCertAuth` property is set to **`true`** and is spelled correctly.

  The `locked.properties` file is located in *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`. The `useCertAuth` property is commonly misspelled as `userCertAuth`.

- If you configured smart card authentication on a View Connection Server instance, check the smart card authentication setting in View Administrator.

  a Select **View Configuration > Servers**, select the View Connection Server instance, and click **Edit**.

  b On the **Authentication** tab, verify that **Smart card authentication** is set to either **Optional** or **Required**.

  You must restart the View Connection Server service for changes to smart card settings to take effect.

- If the domain a smart card user resides in is different from the domain your root certificate was issued from, verify that the user's UPN is set to the SAN contained in the root certificate of the trusted CA.

  a Find the SAN contained in the root certificate of the trusted CA by viewing the certificate properties.

  b On your Active Directory server, select **Start > Administrative Tools > Active Directory Users and Computers**.

  c Right-click the user in the **Users** folder and select **Properties**.

  The UPN appears in the **User logon name** text boxes on the **Account** tab.

- If smart card users use the PCoIP display protocol to connect to View desktops, verify that the View Agent PCoIP Smartcard subfeature is installed on desktop sources. The PCoIP Smartcard subfeature lets users authenticate with smart cards when they use the PCoIP display protocol.

  NOTE The PCoIP Smartcard subfeature is not supported on Windows Vista.

- Check the log files in *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs on the View Connection Server or security server host for messages stating that smart card authentication is enabled.

Using Smart Card Certificate Revocation Checking

You can prevent users who have revoked user certificates from authenticating with smart cards by configuring certificate revocation checking. Certificates are often revoked when a user leaves an organization, loses a smart card, or moves from one department to another.

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

You can configure certificate revocation checking on a View Connection Server instance or on a security server. When a View Connection Server instance is paired with a security server, you configure certificate revocation checking on the security server. The CA must be accessible from the View Connection Server or security server host.

You can configure both CRL and OCSP on the same View Connection Server instance or security server. When you configure both types of certificate revocation checking, View attempts to use OCSP first and falls back to CRL if OCSP fails. View does not fall back to OCSP if CRL fails.

- Logging in with CRL Checking on page 130

  When you configure CRL checking, View constructs and reads a CRL to determine the revocation status of a user certificate.

- Logging in with OCSP Certificate Revocation Checking on page 131

  When you configure OCSP certificate revocation checking, View sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. View uses an OCSP signing certificate to verify that the responses it receives from the OCSP Responder are genuine.

- Configure CRL Checking on page 131

  When you configure CRL checking, View reads a CRL to determine the revocation status of a smart card user certificate.

- Configure OCSP Certificate Revocation Checking on page 131

  When you configure OCSP certificate revocation checking, View sends a verification request to an OCSP Responder to determine the revocation status of a smart card user certificate.

- Smart Card Certificate Revocation Checking Properties on page 132

  You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

Logging in with CRL Checking

When you configure CRL checking, View constructs and reads a CRL to determine the revocation status of a user certificate.

If a certificate is revoked and smart card authentication is optional, the Enter your user name and password dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate. The same events occur if View cannot read the CRL.

Logging in with OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, View sends a request to an OCSP Responder to determine the revocation status of a specific user certificate. View uses an OCSP signing certificate to verify that the responses it receives from the OCSP Responder are genuine.

If the user certificate is revoked and smart card authentication is optional, the Enter your user name and password dialog box appears and the user must provide a password to authenticate. If smart card authentication is required, the user receives an error message and is not allowed to authenticate.

View falls back to CRL checking if it does not receive a response from the OCSP Responder or if the response is invalid.

Configure CRL Checking

When you configure CRL checking, View reads a CRL to determine the revocation status of a smart card user certificate.

Prerequisites

Familiarize yourself with the `locked.properties` file properties for CRL checking. See "Smart Card Certificate Revocation Checking Properties," on page 132.

Procedure

1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `enableRevocationChecking` and `crlLocation` properties to the `locked.properties` file.

a Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.

b Set `crlLocation` to the location of the CRL. The value can be a URL or a file path.

3 Restart the View Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures CRL checking, and specifies a URL for the CRL location.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Configure OCSP Certificate Revocation Checking

When you configure OCSP certificate revocation checking, View sends a verification request to an OCSP Responder to determine the revocation status of a smart card user certificate.

Prerequisites

Familiarize yourself with the `locked.properties` file properties for OCSP certificate revocation checking. See "Smart Card Certificate Revocation Checking Properties," on page 132.

Procedure

1 Create or edit the `locked.properties` file in the SSL gateway configuration folder on the View Connection Server or security server host.

For example: *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

2 Add the `enableRevocationChecking`, `enableOCSP`, `ocspURL`, and `ocspSigningCert` properties to the `locked.properties` file.

a Set `enableRevocationChecking` to **`true`** to enable smart card certificate revocation checking.

b Set `enableOCSP` to **`true`** to enable OCSP certificate revocation checking.

c Set `ocspURL` to the URL of the OCSP Responder.

d Set `ocspSigningCert` to the location of the file that contains the OCSP Responder's signing certificate.

3 Restart the View Connection Server service or security server service to make your changes take effect.

Example: locked.properties File

The file shown enables smart card authentication and smart card certificate revocation checking, configures both CRL and OCSP certificate revocation checking, specifies the OCSP Responder location, and identifies the file that contains the OCSP signing certificate.

```
trustKeyfile=lonqa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

Smart Card Certificate Revocation Checking Properties

You set values in the `locked.properties` file to enable and configure smart card certificate revocation checking.

Table 7-1 lists the `locked.properties` file properties for certificate revocation checking.

Table 7-1. Properties for Smart Card Certificate Revocation Checking

Property	Description
`enableRevocationChecking`	Set this property to **`true`** to enable certificate revocation checking. When this property is set to **`false`**, certificate revocation checking is disabled and all other certificate revocation checking properties are ignored. The default value is **`false`**.
`crlLocation`	Specifies the location of the CRL, which can be either a URL or a file path. If you do not specify a URL, or if the specified URL is invalid, View uses the list of CRLs on the user certificate if `allowCertCRLs` is set to **`true`** or is not specified. If View cannot access a CRL, CRL checking fails.
`allowCertCRLs`	When this property is set to **`true`**, View extracts a list of CRLs from the user certificate. The default value is **`true`**.

Table 7-1. Properties for Smart Card Certificate Revocation Checking (Continued)

Property	Description
`enableOCSP`	Set this property to **`true`** to enable OCSP certificate revocation checking. The default value is **`false`**.
`ocspURL`	Specifies the URL of an OCSP Responder.
`ocspResponderCert`	Specifies the file that contains the OCSP Responder's signing certificate. View uses this certificate to verify that the OCSP Responder's responses are genuine.
`ocspSendNonce`	When this property is set to **`true`**, a nonce is sent with OCSP requests to prevent repeated responses. The default value is **`false`**.
`ocspCRLFailover`	When this property is set to **`true`**, View uses CRL checking if OCSP certificate revocation checking fails. The default value is **`true`**.

Using RSA SecurID Authentication

You can configure a View Connection Server instance so that users are required to use RSA SecurID authentication before providing their Active Directory credentials.

Because RSA SecurID authentication works with RSA Authentication Manager, an RSA Authentication Manager server is required and must be directly accessible from the View Connection Server host.

To use RSA SecurID authentication, each user must have a SecurID token that is registered with RSA Authentication Manager. An RSA SecurID token is a piece of hardware or software that generates an authentication code at fixed intervals. RSA SecurID provides two-factor authentication by requiring knowledge of both a PIN and an authentication code. The authentication code is available only on the RSA SecurID token.

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

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

- Logging in with RSA SecurID on page 133

  When a user connects to a View Connection Server instance that has RSA SecurID authentication enabled, a RSA SecurID login dialog box appears in View Client.

- Enable RSA SecurID Authentication in View Administrator on page 134

  You enable a View Connection Server instance for RSA SecurID authentication by modifying View Connection Server settings in View Administrator.

- Troubleshooting RSA SecurID Access Denial on page 134

  Access is denied when View Client connects with RSA SecurID authentication.

Logging in with RSA SecurID

When a user connects to a View Connection Server instance that has RSA SecurID authentication enabled, a RSA SecurID login dialog box appears in View Client.

Users enter their RSA SecurID username and passcode in the RSA SecurID login dialog box. An RSA SecurID passcode typically consists of a PIN followed by a token code.

If RSA Authentication Manager requires users to enter a new RSA SecurID PIN after entering their RSA SecurID username and passcode, a PIN dialog box appears. After setting a new PIN, users are prompted to wait for the next token code before logging in. If RSA Authentication Manager is configured to use system-generated PINs, a dialog box appears to confirm the PIN.

After successful validation against RSA Authentication Manager, users are prompted to enter their Active Directory credentials.

Enable RSA SecurID Authentication in View Administrator

You enable a View Connection Server instance for RSA SecurID authentication by modifying View Connection Server settings in View Administrator.

Prerequisites

- Install and configure the RSA SecurID software.
- Export the `sdconf.rec` file for the View Connection Server instance from RSA Authentication Manager. See the RSA Authentication Manager documentation for more information.

Procedure

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

2 In View Connection Servers, select the View Connection Server instance and click **Edit**.

3 On the **Authentication** tab, select **Enable** under **RSA Secure ID 2-Factor Authentication**.

4 (Optional) To force RSA SecurID user names to match user names in Active Directory, select **Enforce SecurID and Windows user name matching**.

If you select this option, users must use the same RSA SecurID user name for Active Directory authentication. If you do not select this option, the names can be different.

5 Click **Upload File**, type the location of the `sdconf.rec` file, or click **Browse** to search for the file.

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

You do not need to restart the View Connection Server service. The necessary configuration files are distributed automatically and the RSA SecurID configuration takes effect immediately.

Troubleshooting RSA SecurID Access Denial

Access is denied when View Client connects with RSA SecurID authentication.

Problem

A View Client connection with RSA SecurID displays `Access Denied` and the RSA Authentication Manager Log Monitor displays the error `Node Verification Failed`.

Cause

The RSA Agent host node secret needs to be reset.

Solution

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

2 In View Connection Servers, select the View Connection Server and click **Edit**.

3 On the **Authentication** tab, select **Clear node secret**.

4 Click **OK** to clear the node secret.

5 On the computer that is running RSA Authentication Manager, select **Start > Programs > RSA Security > RSA Authentication Manager Host Mode**.

6 Select **Agent Host > Edit Agent Host**.

7 Select **View Connection Server** from the list and deselect the **Node Secret Created** check box.

Node Secret Created is selected by default each time you edit it.

8 Click **OK**.

Using the Log In as Current User Feature

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

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

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

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

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

- If smart card authentication is set to Required on a View Connection Server instance, smart card users who select the **Log in as current user** check box must still reauthenticate with their smart card and PIN when logging in to the View desktop.
- Users cannot check out a desktop for use in local mode if they selected the **Log in as current user** check box when they logged in.
- The time on the system where the client logs in and the time on the View Connection Server host must be synchronized.
- If the default **Access this computer from the network** user-right assignments are modified on the client system, they must be modified as described in VMware Knowledge Base (KB) article 1025691.
- The client machine must be able to communicate with the corporate Active Directory server and not use cached credentials for authentication. For example, if users log in to their client machines from outside the corporate network, cached credentials are used for authentication. If the user then attempts to connect to a security server or a View Connection Server instance without first establishing a VPN connection, the user is prompted for credentials, and the Log in as Current User feature does not work.

8 Configuring Policies

You can configure policies to control the behavior of View components, desktop pools, and desktop users. You use View Administrator to set policies for client sessions and you use Active Directory group policy settings to control the behavior of View components and certain features.

This chapter includes the following topics:

Setting Policies in View Administrator

You use View Administrator to configure policies for client sessions.

You can set these policies to affect specific users, specific desktop pools, or all client sessions users. Policies that affect specific users and desktop pools are called user-level policies and desktop-level policies. Policies that affect all sessions and users are called global policies.

User-level policies inherit settings from the equivalent desktop-pool policy settings. Similarly, pool-level policies inherit settings from the equivalent global policy settings. A pool-level policy setting takes precedence over the equivalent global policy setting. A user-level policy setting takes precedence over the equivalent global and pool-level policy settings.

Lower-level policy settings can be more or less restrictive than the equivalent higher-level settings. For example, if the global policy that specifies the amount of time a desktop can be checked out is set to 10 minutes and the equivalent pool-level policy is set to 5 minutes, you can set the equivalent user-level policy to 30 minutes for any user in the pool.

- View Policies on page 139

  You can configure View policies to affect all client sessions, or you can apply them to affect specific desktops or users.

- Local Mode Policies on page 140

  You can configure local mode policies to affect all client sessions, or you can apply them to specific desktops or users.

Configure Global Policy Settings

You can configure global policies to control the behavior of all client sessions users.

Prerequisites

Familiarize yourself with the policy descriptions. See the following topics for information:

- "View Policies," on page 139
- "Local Mode Policies," on page 140

Procedure

1 In View Administrator, select **Policies > Global Policies**.

   a To configure general session policies, click **Edit policies** in the **View Policies** pane.

   b To configure local session policies, click **Edit policies** in the **Local Session Policies** pane.

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

Configure Policies for Desktop Pools

You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See the following topics for information:

- "View Policies," on page 139
- "Local Mode Policies," on page 140

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 Double-click the ID of the desktop pool and click the **Policies** tab.

   The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Pool Policy** column.

3 To configure general session policies for the pool, click **Edit policies** in the **View Policies** pane.

4 To configure local session policies for the pool, click **Edit policies** in the **Local Mode Policies** pane.

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

Configure Policies for Desktop Users

You can configure user-level policies to affect specific users. User-level policy settings always take precedence over their equivalent global and desktop-level policy settings.

Prerequisites

Familiarize yourself with the policy descriptions. See "View Policies," on page 139.

Procedure

1 In View Administrator, select **Inventory > Pools**.

2 Double-click the ID of the desktop pool and click the **Policies** tab.

The **Policies** tab shows the current policy settings. When a setting is inherited from the equivalent global policy, **Inherit** appears in the **Pool Policy** column.

3 Click **User Overrides** and then click **Add User**.

4 To find a user, click **Add**, type the name or description of the user, and then click **Find**.

5 Select one or more users from the list, click **OK**, and then click **Next**.

The Add Individual Policy dialog box appears.

6 Configure general session policies on the **General** tab.

7 Configure policies for local mode clients on the **Local** tab.

8 Click **Finish** to save your changes.

View Policies

You can configure View policies to affect all client sessions, or you can apply them to affect specific desktops or users.

Table 8-1 describes each View policy setting.

Table 8-1. View Policies

Policy	Description
Multimedia redirection (MMR)	Determines whether MMR is enabled for client systems. MMR is a Microsoft DirectShow filter that forwards multimedia data from specific codecs on View desktops directly through a TCP socket to the client system. The data is then decoded directly on the client system, where it is played. The default value is **Allow**. If client systems have insufficient resources to handle local multimedia decoding, change the setting to **Deny**. MMR does not work correctly if the client system's video display hardware does not have overlay support.
USB Access	Determines whether desktops can use USB devices connected to the client system. The default value is **Allow**. To prevent the use of external devices for security reasons, change the setting to **Deny**.

Table 8-1. View Policies (Continued)

Policy	Description
Remote mode	Determines whether users can connect to and use desktops running on vCenter Server instances. If set to **Deny**, users must check out the desktop on their local computers and run the desktop only in local mode. Restricting users to running desktops only in local mode reduces the costs associated with CPU, memory, and network bandwidth requirements of running the desktop on a back-end server. The default value is **Allow**.
PCoIP hardware acceleration	Determines whether to enable hardware acceleration of the PCoIP display protocol and specifies the acceleration priority that is assigned to the PCoIP user session. This setting has an effect only if a PCoIP hardware acceleration device is present on the physical computer that hosts the desktop. The default value is **Allow** at **Medium** priority.

Local Mode Policies

You can configure local mode policies to affect all client sessions, or you can apply them to specific desktops or users.

Table 8-2 describes each local mode policy setting.

Table 8-2. Local Mode Policies

Policy	Description
Local Mode	Determines whether users can check out desktops for local use. Also determines whether users can run local desktops while the desktops are checked out. The default value is **Allow**. If you change this value to **Deny** while a desktop is checked out, the user cannot run the desktop in local mode, and the desktop cannot be used remotely because it is still checked out.
User-initiated rollback	Determines whether users can discard a local desktop and revert to the remote version. When a user initiates the rollback process, the lock on the remote desktop is released and the local desktop is discarded. If necessary, the user can manually remove and delete the local folder that contains the local desktop data. The default value is **Allow**.
Max time without server contact	Specifies the amount of time in days that a local desktop can run without making contact with View Connection Server for policy updates. If the specified time limit is exceeded, View Client displays a warning message to the user and suspends the desktop. The default value is **7** days. On the client side, this expiration policy is stored in a file that is encrypted by a key that is built into the application. This built-in key prevents users who have access to the password from circumventing the expiration policy.

Table 8-2. Local Mode Policies (Continued)

Policy	Description
Target replication frequency	Specifies the interval in days, hours, or minutes between the start of one replication and the start of the next replication. A replication copies any changes in local desktop files to the corresponding remote desktop or View Composer persistent disk in the datacenter. The default value is the **No replication** setting. If you select **At a specified interval**, the default replication interval is 12 hours. You can prohibit scheduled replications by selecting **No replication**. The **No replication** policy does not prohibit explicit replication requests. You can initiate replications in View Administrator, and users can request replications if the **User initiated replication** policy is set to **Allow**. If a replication takes longer than the interval that is specified in the **Target replication frequency** policy, the next scheduled replication starts after the previous one is completed. The pending replication does not cancel the previous one. For example, the **Target replication frequency** policy might be set to one day. A replication might start at noon on Tuesday. If the client computer is disconnected from the network, the replication might take longer than 24 hours. At noon on Wednesday, View Client with Local Mode starts the next replication request. After the previous replication is completed, View Client with Local Mode takes a snapshot and starts the pending replication.
User deferred replication	Determines whether users can pause active replications. If you enable this policy, a user can defer a replication that is underway. The replication does not resume, and no new replications start, until the deferment period is over. The default value is **Deny**. When the value is set to **Allow**, the deferment period is two hours.
Disks replicated	Determines which desktop disks are replicated. This policy affects View Composer linked-clone desktops only. For full virtual-machine desktops, all disks are replicated. You have these disk-replication choices: ■ Persistent disks ■ OS disks ■ OS and persistent disks Changing this policy affects desktop replication after the next checkout occurs. A change does not affect desktops that are currently checked out. The default value is **Persistent disks**.
User-initiated check in	Determines whether users are allowed to check in desktops that are running in local mode. The default value is **Allow**.
User-initiated replication	Determines whether users are allowed to initiate replications from their desktops when they run in local mode. The default value is **Allow**.

Using Active Directory Group Policies

You can use Microsoft Windows Group Policy to optimize and secure View desktops, control the behavior of View components, and to configure location-based printing.

Group Policy is a feature of Microsoft Windows operating systems that provides centralized management and configuration of computers and remote users in an Active Directory environment.

Group policy settings are contained in entities called GPOs. GPOs are associated with Active Directory objects. You can apply GPOs to View components at a domain-wide level to control various areas of the View environment. After they are applied, GPO settings are stored in the local Windows Registry of the specified component.

You use the Microsoft Windows Group Policy Object Editor to manage group policy settings. The Group Policy Object Editor is a Microsoft Management Console (MMC) snap-in. The MMC is part of the Microsoft Group Policy Management Console (GPMC). See the Microsoft TechNet Web site for information on installing and using the GPMC.

Creating an OU for View Desktops

You should create an organizational unit (OU) in Active Directory specifically for your View desktops.

To prevent group policy settings from being applied to other Windows servers or workstations in the same domain as your desktops, create a GPO for your View group policies and link it to the OU that contains your View desktops.

See the Microsoft Active Directory documentation on the Microsoft TechNet Web site for information on creating OUs and GPOs.

Enabling Loopback Processing for View Desktops

By default, a user's policy settings come from the set of GPOs that are applied to the user object in Active Directory. However, in the View environment, GPOs should apply to users based on the computer they log in to.

When you enable loopback processing, a consistent set of policies applies to all users that log in to a particular computer, regardless of their location in Active Directory.

See the Microsoft Active Directory documentation for information on enabling loopback processing.

NOTE Loopback processing is only one approach to handling GPOs in View. You might need to implement a different approach.

Using the View Group Policy Administrative Template Files

View includes several component-specific Group Policy Administrative (ADM) Template files. You can optimize and secure View desktops by adding the policy settings in these ADM template files to a new or existing GPO in Active Directory.

The View ADM template files contain both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to all View desktops, regardless of who connects to the desktop.
- The User Configuration policies set policies that apply to all users, regardless of the View desktop they connect to. User Configuration policies override equivalent Computer Configuration policies.

View applies policies at View desktop startup and when users log in.

View ADM Template Files

The View ADM template files are installed in the *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles directory on your View Connection Server host.

Table 8-3. View ADM Template Files

Template Name	Template File	Description
VMware View Agent Configuration	vdm_agent.adm	Contains policy settings related to the authentication and environmental components of View Agent.
VMware View Client Configuration	vdm_client.adm	Contains policy settings related to View Client configuration. Clients that connect from outside the View Connection Server host domain are not affected by policies applied to View Client.
VMware View Server Configuration	vdm_server.adm	Contains policy settings related to View Connection Server.
VMware View Common Configuration	vdm_common.adm	Contains policy settings that are common to all View components.
VMware View PCoIP Session Variables	pcoip.adm	Contains policy settings related to the PCoIP display protocol.
VMware View Persona Management Configuration	ViewPM.adm	Contains policy settings related to View Persona Management. See "View Persona Management Group Policy Settings," on page 185.

View Agent Configuration ADM Template Settings

The View Agent Configuration ADM template file (vdm_agent.adm) contains policy settings related to the authentication and environmental components of View Agent.

Table 8-4 describes each policy setting in the View Agent Configuration ADM template file. The template contains both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting.

Table 8-4. View Agent Configuration Template Settings

Setting	Computer	User	Properties
AllowDirectRDP	X		Determines whether non-View clients can connect directly to View desktops with RDP. When this setting is disabled, View Agent permits only View-managed connections through View Client. When connecting to a virtual desktop from View Client for Mac OS X, do not disable the AllowDirectRDP setting. If this setting is disabled, the connection fails with an Access is denied error. This setting is enabled by default.
AllowSingleSignon	X		Determines whether single sign-on (SSO) is used to connect users to View desktops. When this setting is enabled, users are required to enter only their credentials when connecting with View Client. When it is disabled, users must reauthenticate when the remote connection is made. This setting is enabled by default.

Table 8-4. View Agent Configuration Template Settings (Continued)

Setting	Computer	User	Properties
CommandsToRunOnConnect	X		Specifies a list of commands or command scripts to be run when a session is connected for the first time. See "Running Commands on View Desktops," on page 145 for more information.
CommandsToRunOnReconnect	X		Specifies a list of commands or command scripts to be run when a session is reconnected after a disconnect. See "Running Commands on View Desktops," on page 145 for more information.
Connect using DNS Name	X		Determines whether View Connection Server uses the DNS name instead of the IP address of the host when connecting. This setting is typically enabled in a NAT or firewall situation when View Client or View Connection Server cannot use the desktop IP address directly. This setting is disabled by default.
ConnectionTicketTimeout	X		Specifies the amount of time in seconds that the View connection ticket is valid. View clients use a connection ticket for verification and single sign-on when connecting to View Agent. For security reasons, a connection ticket is valid for a limited amount of time. When a user connects to a View desktop, authentication must take place within the connection ticket timeout period or the session times out. If this setting is not configured, the default timeout period is 900 seconds.
CredentialFilterExceptions	X		Specifies the executable files that are not allowed to load the agent CredentialFilter. Filenames must not include a path or suffix. Use a semicolon to separate multiple filenames.
Disable Time Zone Synchronization	X	X	Determines whether the time zone of the View desktop is synchronized with the time zone of the connected client. An enabled setting applies only if the `Disable time zone forwarding` setting of the View Client Configuration policy is not set to disabled. This setting is disabled by default.
Force MMR to use software overlay	X		Determines whether the multimedia redirection (MMR) feature uses a software overlay instead of a hardware overlay. MMR uses video display hardware with overlay support for better performance. Because hardware overlays typically exist only on the primary monitor in a multi-monitor system, video is not displayed when it is dragged from the primary monitor to a secondary monitor. Enabling this setting forces MMR to use a software overlay on all monitors. This setting is disabled by default.
ShowDiskActivityIcon	X		This setting is not supported in this release.
Toggle Display Settings Control	X		Determines whether to disable the **Settings** tab in the **Display** control panel when a client session uses the PCoIP display protocol. This setting is enabled by default.

Running Commands on View Desktops

You can use the View Agent `CommandsToRunOnConnect` and `CommandsToRunOnReconnect` group policy settings to run commands and command scripts on View desktops when users connect and reconnect.

To run a command or a command script, add the command name or the file path of the script to the group policy setting's list of commands. For example:

```
date
```

```
C:\Scripts\myscript.cmd
```

To run scripts that require console access, prepend the `-C` or `-c` option followed by a space. For example:

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

Supported file types include `.CMD`, `.BAT`, and `.EXE`. `.VBS` files will not run unless they are parsed with `cscript.exe` or `wscript.exe`. For example:

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

The total length of the string, including the `-C` or `-c` option, should not exceed 260 characters.

Client System Information Sent to View Desktops

When a user connects or reconnects to a View desktop, the View client gathers information about the client system and View Connection Server sends that information to the desktop. View Agent writes the client computer information to the system registry path `HKCU\Volatile Environment` on the desktop.

You can add commands to the View Agent `CommandsToRunOnConnect` and `CommandsToRunOnReconnect` group policy settings to run commands or command scripts that read this information from the system registry when users connect and reconnect to desktops. See "Running Commands on View Desktops," on page 145 for more information.

Table 8-5 describes the registry keys that contain client system information and lists the types of client systems that support them.

Table 8-5. Client System Information

Registry Key	Description	Client Systems Supported
`ViewClient_IP_Address`	The IP address of the client system.	Windows Linux Mac
`ViewClient_MAC_Address`	The MAC address of the client system.	Windows Linux Mac
`ViewClient_Machine_Name`	The machine name of the client system.	Windows Linux Mac
`ViewClient_Machine_Domain`	The domain of the client system.	Windows Linux Mac
`ViewClient_LoggedOn_Username`	The user name that was used to log in to the client system.	Windows Linux Mac

Table 8-5. Client System Information (Continued)

Registry Key	Description	Client Systems Supported
`ViewClient_LoggedOn_Domainname`	The domain name that was used to log in to the client system.	Windows NOTE For Linux and Mac clients, see `ViewClient_Machine_Domain`. `ViewClient_LoggedOn_Domainname` is not given by the Linux or Mac client because Linux and Mac accounts are not bound to Windows domains.
`ViewClient_Type`	The thin client name or operating system type of the client system.	Windows Linux Mac
`ViewClient_Broker_DNS_Name`	The DNS name of the View Connection Server instance.	Windows Linux Mac
`ViewClient_Broker_URL`	The URL of the View Connection Server instance.	Windows Linux Mac
`ViewClient_Broker_Tunneled`	The status of the tunnel connection for the View Connection Server, which can be either `true` (enabled) or `false` (disabled).	Windows Linux Mac
`ViewClient_Broker_Tunnel_URL`	The URL of the View Connection Server tunnel connection, if the tunnel connection is enabled.	Windows Linux Mac
`ViewClient_Broker_Remote_IP_Address`	The IP address of the View Connection Server instance to which the client is connected.	Windows Linux Mac
`ViewClient_TZID`	The Olson time zone ID. To disable time zone synchronization, enable the View Agent `Disable Time Zone Synchronization` group policy setting.	Linux Mac

View Client Configuration ADM Template Settings

The View Client Configuration ADM template file (`vdm_client.adm`) contains policy settings related to the View Client configuration.

Scripting Definition Settings

Table 8-6 describes the scripting definition settings in the View Client Configuration ADM template file. The template provides a Computer Configuration and a User Configuration version of each scripting definition setting. The User Configuration setting overrides the equivalent Computer Configuration setting.

Table 8-6. View Client Configuration Template: Scripting Definitions

Setting	Description
`Connect all USB devices to the desktop on launch`	Determines whether all of the available USB devices on the client system are connected to the desktop when the desktop is launched.
`Connect all USB devices to the desktop when they are plugged in`	Determines whether USB devices are connected to the desktop when they are plugged in to the client system.

Table 8-6. View Client Configuration Template: Scripting Definitions (Continued)

Setting	Description
DesktopLayout (requires DesktopName)	Specifies the layout of the View Client window that a user sees when logging into a View desktop. The layout choices are as follows: ■ Full Screen ■ Multimonitor ■ Window – Large ■ Window – Small This setting is available only when the DesktopName to select setting is also set.
DesktopName to select	Specifies the default desktop that View Client uses during login.
Disable 3rd-party Terminal Services plugins	Determines whether View Client checks third-party Terminal Services plugins that are installed as normal RDP plugins. If you do not configure this setting, View Client checks third-party plugins by default. This setting does not affect View-specific plugins, such as USB redirection.
Logon DomainName	Specifies the NetBIOS domain that View Client uses during login.
Logon Password	Specifies the password that View Client uses during login. The password is stored in plain text by Active Directory.
Logon UserName	Specifies the username that View Client uses during login.
Server URL	Specifies the URL that View Client uses during login, for example, http://view1.example.com.
Suppress error messages (when fully scripted only)	Determines whether View Client error messages are hidden during login. This setting applies only when the login process is fully scripted, for example, when all the required login information is prepopulated through policy. If the login fails because of incorrect login information, the user is not notified and the View Client wswc.exe process is terminated.

Security Settings

Table 8-7 describes the security settings in the View Client Configuration ADM template file. This table shows whether the settings include both Computer Configuration and User Configuration settings or Computer Configuration settings only. For the security settings that include both types, the User Configuration setting overrides the equivalent Computer Configuration setting.

Table 8-7. View Client Configuration Template: Security Settings

Setting	Computer	User	Description
`Allow command line credentials`	X		Determines whether user credentials can be provided with View Client command line options. If this setting is enabled, the `smartCardPIN` and `password` options are not available when users run View Client from the command line. This setting is enabled by default.
`Brokers Trusted For Delegation`	X		Specifies the View Connection Server instances that accept the user identity and credential information that is passed when a user selects the **Log in as current user** check box. If you do not specify any View Connection Server instances, all View Connection Server instances accept this information. To add a View Connection Server instance, use one of the following formats: ■ **`domain\system$`** ■ **`system$@domain.com`** ■ The Service Principal Name (SPN) of the View Connection Server service.

Table 8-7. View Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description

`Certificate verification mode`	X		Configures the level of certificate checking that is performed by View Client. You can select one of these modes:
			■ `No Security`. View does not perform certificate checking.
			■ `Warn But Allow`. When the following server certificate issues occur, a warning is displayed, but the user can continue to connect to View Connection Server:
			  ■ A self-signed certificate is provided by View. In this case, it is acceptable if the certificate name does not match the View Connection Server name provided by the user in View Client.
			  ■ A verifiable certificate that was configured in your deployment has expired or is not yet valid.
			If any other certificate error condition occurs, View displays an error dialog and prevents the user from connecting to View Connection Server.
			`Warn But Allow` is the default value.
			■ `Full Security`. If any type of certificate error occurs, the user cannot connect to View Connection Server. View displays certificate errors to the user.
			To allow View Client to perform any type of certificate checking, you must select the **Require SSL for client connections and View Administrator** Global Setting in View Administrator.
			When this group policy setting is configured, users can view the selected certificate verification mode in View Client but cannot configure the setting. The SSL configuration dialog box informs users that the administrator has locked the setting.
			When this setting is not configured or disabled, View Client users can configure SSL and select a certificate verification mode.
			For Windows clients, if you do not want to configure this setting as a group policy, you can also enable certificate verification by adding the `CertCheckMode` value name to the following registry key on the client computer:
			`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
			Use the following values in the registry key:
			■ **`0`** implements `No Security`.
			■ **`1`** implements `Warn But Allow`.
			■ **`2`** implements `Full Security`.
			If you configure both the group policy setting and the `CertCheckMode` setting in the registry key, the group policy setting takes precedence over the registry key value.

Table 8-7. View Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
`Default value of the 'Log in as current user' checkbox`	X	X	Specifies the default value of the **Log in as current user** check box on the View Client connection dialog box. This setting overrides the default value specified during View Client installation. If a user runs View Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting. When the **Log in as current user** check box is selected, the identity and credential information that the user provided when logging in to the client system is passed to the View Connection Server instance and ultimately to the View desktop. When the check box is deselected, users must provide identity and credential information multiple times before they can access a View desktop. This setting is disabled by default.
`Display option to Log in as current user`	X	X	Determines whether the **Log in as current user** check box is visible on the View Client connection dialog box. When the check box is visible, users can select or deselect it and override its default value. When the check box is hidden, users cannot override its default value from the View Client connection dialog box. You can specify the default value for the **Log in as current user** check box by using the policy setting `Default value of the 'Log in as current user' checkbox`. This setting is enabled by default.
`Enable jump list integration`	X		Determines whether a jump list appears in the View Client icon on the taskbar of Windows 7 and later systems. The jump list lets users connect to recent View Connection Server instances and View desktops. If View Client is shared, you might not want users to see the names of recent desktops. You can disable the jump list by disabling this setting. This setting is enabled by default.
`Enable Single Sign-On for smart card authentication`	X		Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, View Client stores the encrypted smart card PIN in temporary memory before submitting it to View Connection Server. When single sign-on is disabled, View Client does not display a custom PIN dialog.
`Ignore bad SSL certificate date received from the server`	X		Determines whether errors that are associated with invalid server certificate dates are ignored. These errors occur when a server sends a certificate with a date that has passed. This setting applies to View 4.6 and earlier releases only.
`Ignore certificate revocation problems`	X		Determines whether errors that are associated with a revoked server certificate are ignored. These errors occur when the server sends a certificate that has been revoked and when the client cannot verify a certificate's revocation status. This setting is disabled by default. This setting applies to View 4.6 and earlier releases only.

Table 8-7. View Client Configuration Template: Security Settings (Continued)

Setting	Computer	User	Description
Ignore incorrect SSL certificate common name (host name field)	X		Determines whether errors that are associated with incorrect server certificate common names are ignored. These errors occur when the common name on the certificate does not match the hostname of the server that sends it. This setting applies to View 4.6 and earlier releases only.
Ignore incorrect usage problems	X		Determines whether errors that are associated with incorrect usage of a server certificate are ignored. These errors occur when the server sends a certificate that is intended for a purpose other than verifying the identity of the sender and encrypting server communications. This setting applies to View 4.6 and earlier releases only.
Ignore unknown certificate authority problems	X		Determines whether errors that are associated with an unknown Certificate Authority (CA) on the server certificate are ignored. These errors occur when the server sends a certificate that is signed by an untrusted third-party CA. This setting applies to View 4.6 and earlier releases only.

RDP Settings

Table 8-8 describes the Remote Desktop Protocol (RDP) settings in the View Client Configuration ADM template file. All RDP settings are User Configuration settings.

Table 8-8. View Client Configuration Administrative Template: RDP Settings

Setting	Description
Audio redirection	Determines whether audio information played on the View desktop is redirected. Select one of the following settings: **Disable Audio** — Audio is disabled. **Play VM (needed for VoIP USB Support)** — Audio plays within the View desktop. This setting 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 setting applies only to RDP audio. Audio that is redirected through MMR plays in the client.
Audio capture redirection	Determines whether the default audio input device is redirected from the client to the remote session. When this setting is enabled, the audio recording device on the client appears in the View desktop and can record audio input. The default setting is disabled.

Table 8-8. View Client Configuration Administrative Template: RDP Settings (Continued)

Setting	Description
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Specifies the size of the bitmap cache, in kilobytes or megabytes, to use for specific bits per pixel (bpp) bitmap color settings. Separate versions of this setting are provided for the following unit and bpp combinations: ■ KB/8bpp ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`Bitmap caching`	Determines whether remote bitmaps are cached on the local computer.
`Cache persistence active`	Determines whether persistent bitmap caching is used (active). Persistent bitmap caching can improve performance, but it requires additional disk space.
`Color depth`	Specifies the color depth of the View desktop. Select one of the available settings: ■ 8 bit ■ 15 bit ■ 16 bit ■ 24 bit ■ 32 bit For 24-bit Windows XP systems, you must enable the Limit Maximum Color Depth policy in **Computer Configuration > Administrative Templates > Windows Components > Terminal Services** and set it to 24 bits.
`Cursor shadow`	Determines whether a shadow appears under the cursor on the View desktop.
`Desktop background`	Determines whether the desktop background appears when clients connect to a View desktop.
`Desktop composition`	(Windows Vista or later) Determines whether desktop composition is enabled on the View 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, drawing is redirected to off-screen surfaces in video memory, which are then rendered into a desktop image and presented on the display.
`Enable compression`	Determines whether RDP data is compressed. This setting is enabled by default.
`Enable Credential Security Service Provider`	Specifies whether the View desktop connection uses Network Level Authentication (NLA). In Windows Vista, remote desktop connections require NLA by default. If the guest operating system requires NLA for remote desktop connections, you must enable this setting or View Client will not be able to connect to the View desktop. In addition to enabling this setting, you must also verify that the following conditions are met: ■ Both the client and guest operating systems support NLA. ■ Direct client connections are enabled for the View Connection Server instance. Tunneled connections are not supported with NLA.

Table 8-8. View Client Configuration Administrative Template: RDP Settings (Continued)

Setting	Description
`Enable RDP Auto-Reconnect`	Determines whether the RDP client component attempts to reconnect to a View desktop after an RDP protocol connection failure. This setting has no effect if the **Use secure tunnel connection to desktop** option is enabled in View Administrator. This setting is disabled by default. **NOTE** RDP auto-reconnection is supported for desktops running View Agent version 4.5 or later only. If a desktop has an earlier version of View Agent, some features will not work.
`Font smoothing`	(Windows Vista or later) Determines whether antialiasing is applied to the fonts on the View desktop.
`Menu and window animation`	Determines whether animation for menus and windows is enabled when clients connect to a View desktop.
`Redirect clipboard`	Determines whether the local clipboard information is redirected when clients connect to the View desktop.
`Redirect drives`	Determines whether local disk drives are redirected when clients connect to the View desktop. By default, local drives are redirected. Enabling this setting, or leaving it unconfigured, allows data on the redirected drive on the remote desktop to be copied to the drive on the client computer. Disable this setting if allowing data to pass from the remote desktop to users' client computers represents a potential security risk in your deployment. Another approach is to disable folder redirection in the remote desktop virtual machine by enabling the Microsoft Windows group policy setting, `Do not allow drive redirection`. The `Redirect drives` setting applies to RDP only.
`Redirect printers`	Determines whether local printers are redirected when clients connect to the View desktop.
`Redirect serial ports`	Determines whether local COM ports are redirected when clients connect to the View desktop.
`Redirect smart cards`	Determines whether local smart cards are redirected when clients connect to the View desktop. **NOTE** This setting applies to both RDP and PCoIP connections.
`Redirect supported plug-and-play devices`	Determines whether local plug-and-play and point-of-sale devices are redirected when clients connect to the View desktop. This behavior is different from the redirection that is managed by the USB Redirection component of View Agent.
`Shadow bitmaps`	Determines whether bitmaps are shadowed. This setting has no effect in full-screen mode.
`Show contents of window while dragging`	Determines whether the folder contents appear when users drag a folder to a new location.
`Themes`	Determines whether themes appear when clients connect to a View desktop.
`Windows key combination redirection`	Determines whether Windows key combinations are applied.

General Settings

Table 8-9 describes the general settings in the View Client Configuration ADM template file. General settings include both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting.

Table 8-9. View Client Configuration Template: General Settings

Setting	Computer	User	Description
`Always on top`		X	Determines whether the View Client window is always the topmost window. Enabling this setting prevents the Windows taskbar from obscuring a full-screen View Client window. This setting is enabled by default.
`Default Exit Behavior For Local Mode Desktops`		X	Controls the default exit behavior of desktops that are running in local mode. The default setting is **Shutdown**, which causes the guest operating system to shut down.
`Delay the start of replications when starting the View Client with Local Mode`	X		Specifies the number of seconds to delay the start of replication after View Client with Local Mode starts. A replication copies any changes in local desktop files to the corresponding remote desktop. The next scheduled replication begins after the delay period. Replications occur at intervals that you specify in local mode policies in View Administrator. The default delay period is 900 seconds (15 minutes).
`Determines if the VMware View Client should use proxy.pac file`	X		Determines whether View Client uses a Proxy Auto Config (PAC) file. Enabling this setting causes View Client to use a PAC file. A PAC file (commonly called `proxy.pac`) helps Web browsers and other user agents find the appropriate proxy server for a particular URL or Web site request. If you enable this setting on a multi-core machine, the WinINet application that View Client uses to find the proxy server information might crash. Disable this setting if this problem occurs on your machine. This setting is disabled by default. **NOTE** This setting applies to direct connections only. It does not affect tunnel connections. This setting applies to View 4.6 and earlier releases only.
`Disable time zone forwarding`	X		Determines whether time zone synchronization between the View desktop and the connected client is disabled.
`Disable toast notifications`			Determines whether to disable toast notifications from View Client. Enable this setting if you do not want the user to see toast notifications in the corner of the screen. **NOTE** If you enable this setting, the user does not see a 5-minute warning when the Session Timeout function is active.
`Don't check monitor alignment on spanning`		X	By default, the client desktop does not span multiple monitors if the screens do not form an exact rectangle when they are combined. Enable this setting to override the default. This setting is disabled by default.
`Enable multi-media acceleration`		X	Determines whether multimedia redirection (MMR) is enabled on the client. MMR does not work correctly if the View Client video display hardware does not have overlay support. MMR policy does not apply to local-desktop sessions.
`Enable the shade`		X	Determines whether the shade menu bar at the top of the View Client window is visible. This setting is enabled by default. **NOTE** The shade menu bar is disabled by default for kiosk mode.

Table 8-9. View Client Configuration Template: General Settings (Continued)

Setting	Computer	User	Description
Redirect smart card readers in Local Mode	X		Determines whether smart card readers are redirected to local desktops. The readers are shared with the client system. This setting is enabled by default.
Tunnel proxy bypass address list	X		Specifies a list of tunnel addresses. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries.
URL for View Client online help	X		Specifies an alternate URL from which View Client can retrieve help pages. This setting is intended for use in environments that cannot retrieve the remotely-hosted help system because they do not have internet access.
Pin the shade		X	Determines whether the pin on the shade at the top of the View Client window is enabled and autohiding of the menu bar does not occur. This setting has no effect if the shade is disabled. This setting is enabled by default.

View Server Configuration ADM Template Settings

The View Server Configuration ADM template file (`vdm_server.adm`) contains policy settings related to all View Connection Server.

Table 8-10 describes each policy setting in the View Server Configuration ADM template file. The template contains only Computer Configuration settings.

Table 8-10. View Server Configuration Template Settings

Setting	Properties
Recursive Enumeration of Trusted Domains	Determines whether every domain trusted by the domain in which the server resides is enumerated. 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 so that all trusted domains are available to the client on login. This setting is enabled by default. When it is disabled, only directly trusted domains are enumerated and connection to remote domain controllers does not take place. 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.

View Common Configuration ADM Template Settings

The View Common Configuration ADM template file (`vdm_common.adm`) contains policy settings common to all View components. This template contains only Computer Configuration settings.

Log Configuration Settings

Table 8-11 describes the log configuration policy setting in the View Common Configuration ADM template file.

Table 8-11. View Common Configuration Template: Log Configuration Settings

Setting	Properties
Number of days to keep production 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 are kept for seven days.
Maximum number of debug logs	Specifies the maximum number of debug log files to retain on the system. When a log file reaches its maximum size, no further entries are added and a new log file is created. When the number of previous log files reaches this value, the oldest log file is deleted.
Maximum debug log size in Megabytes	Specifies the maximum size in megabytes that a debug log can reach before the log file is closed and a new log file is created.
Log Directory	Specifies the full path to the directory for log files. If the location is not writeable, the default location is used. For client log files, an extra directory with the client name is created.

Performance Alarm Settings

Table 8-12 describe the performance alarm settings in the View Common Configuration ADM template file.

Table 8-12. View Common Configuration Template: Performance Alarm Settings

Setting	Properties
CPU and Memory Sampling Interval in Seconds	Specifies the CPU and memory polling interval CPU. A low sampling interval can result in an high level of output to the log.
Overall CPU usage percentage to issue log info	Specifies the threshold at which the overall CPU use of the system is logged. When multiple processors are available, this percentage represents the combined usage.
Overall memory usage percentage to issue log info	Specifies the threshold at which the overall committed system memory use is logged. Committed system memory is memory that has been allocated by processes and to which the operating system has committed physical memory or a page slot in the pagefile.
Process CPU usage percentage to issue log info	Specifies the threshold at which the CPU usage of any individual process is logged.
Process memory usage percentage to issue log info	Specifies the threshold at which the memory usage of any individual process is logged.
Process to check, comma separated name list allowing wild cards and exclusion	Specifies a comma-separated list of queries that correspond to the name of one or more processes to be examined. You can filter the list by using wildcards within each query. ■ An asterisk (*) matches zero or more characters. ■ A question mark (?) matches exactly one character. ■ An exclamation mark (!) at the beginning of a query excludes any results produced by that query. For example, the following query selects all processes starting with **ws** and excludes all processes ending with **sys**: **'!*sys,ws*'**

NOTE Performance alarm settings apply to View Connection Server and View Agent systems only. They do not apply to View Client systems.

General Settings

Table 8-13 describes the general settings in the View Common Configuration ADM template file.

Table 8-13. View Common Configuration Template: General Settings

Setting	Properties
`Disk threshold for log and events in Megabytes`	Specifies the minimum remaining disk space threshold for logs and events. If no value is specified, the default is 200. When the specified value is met, event logging stops.
`Enable extended logging`	Determines whether trace and debug events are included in the log files.

View PCoIP Session Variables ADM Template Settings

The View PCoIP Session Variables ADM template file (`pcoip.adm`) contains policy settings related to the PCoIP display protocol. You can configure settings to default values that can be overridden by an administrator, or you can configure settings to non-overridable values.

The View PCoIP Session Variables ADM template file contains two subcategories:

Overridable Administrator Defaults — Specifies PCoIP session variable default values. These settings can be overridden by an administrator. These settings write registry keys values to `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults`.

Not Overridable Administrator Settings — Contains the same settings as Overridable Administrator Defaults, but these settings cannot be overridden by an administrator. These settings write registry key values to `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin`.

The template contains Computer Configuration settings only.

Non-Policy Registry Keys

If a local machine setting needs to be applied and cannot be placed under `HKLM\Software\Policies\Teradici`, local machine settings can be placed in registry keys in `HKLM\Software\Teradici`. The same registry keys can be placed in `HKLM\Software\Teradici` as in `HKLM\Software\Policies\Teradici`. If the same registry key is present in both locations, the setting in `HKLM\Software\Policies\Teradici` overrides the local machine value.

- View PCoIP General Session Variables on page 158

  The View PCoIP Session Variables ADM template file contains group policy settings that configure general session characteristics such as PCoIP image quality, USB devices, and network ports.

- View PCoIP Session Bandwidth Variables on page 163

  The View PCoIP Session Variables ADM template file contains group policy settings that configure PCoIP session bandwidth characteristics.

- View PCoIP Session Variables for the Keyboard on page 165

  The View PCoIP Session Variables ADM template file contains group policy settings that configure PCoIP session characteristics that affect the use of the keyboard.

- View PCoIP Build-to-Lossless Feature on page 166

  The PCoIP display protocol uses an encoding approach called progressive build, which works to provide the optimal overall user experience even under constrained network conditions.

View PCoIP General Session Variables

The View PCoIP Session Variables ADM template file contains group policy settings that configure general session characteristics such as PCoIP image quality, USB devices, and network ports.

Table 8-14. View PCoIP General Session Variables

Setting	Description
`Configure clipboard redirection`	Determines the direction in which clipboard redirection is allowed. You can select one of these values: ■ **Enabled client to server only** (That is, allow copy and paste only from the client system to the View desktop.) ■ **Disabled in both directions** ■ **Enabled in both directions** ■ **Enabled server to client only** (That is, allow copy and paste only from the View desktop to the client system.) Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection does not function. This setting applies to the server only. When this setting is disabled or not configured, the default value is **Enabled client to server only**.
`Configure PCoIP client image cache size policy`	Controls the size of the PCoIP client image cache. The client uses image caching to store portions of the display that were previously transmitted. Image caching reduces the amount of data that is retransmitted. This setting applies only to Windows and Linux clients when View Client, View Agent, and View Connection Server are a View 5.0 or later release. When this setting is not configured or disabled, PCoIP uses a default client image cache size of 250MB. When you enable this setting, you can configure a client image cache size from a minimum of 50 MB to a maximum of 300 MB. The default value is 250MB.

Table 8-14. View PCoIP General Session Variables (Continued)

Setting	Description
`Configure PCoIP image quality levels`	Controls how PCoIP renders images during periods of network congestion. The **Minimum Image Quality**, **Maximum Initial Image Quality**, and **Maximum Frame Rate** values interoperate to provide fine control in network-bandwidth constrained environments. Use the **Minimum Image Quality** value to balance image quality and frame rate for limited-bandwidth scenarios. You can specify a value between 30 and 100. The default value is 50. A lower value allows higher frame-rates, but with a potentially lower quality display. A higher value provides higher image quality, but with potentially lower frame rates when network bandwidth is constrained. When network bandwidth is not constrained, PCoIP maintains maximum quality regardless of this value. Use the **Maximum Initial Image Quality** value to reduce the network bandwidth peaks required by PCoIP by limiting the initial quality of the changed regions of the display image. You can specify a value between 30 and 100. The default value is 90. A lower value reduces the image quality of content changes and decreases peak bandwidth requirements. A higher value increases the image quality of content changes and increases peak bandwidth requirements. Unchanged regions of the image progressively build to a lossless (perfect) quality regardless of this value. A value of 90 or lower best utilizes the available bandwidth. The **Minimum Image Quality** value cannot exceed the**Maximum Initial Image Quality** value. Use the **Maximum Frame Rate** value to manage the average bandwidth consumed per user by limiting the number of screen updates per second. You can specify a value between 1 and 120 frames per second. The default value is 30. A higher value can use more bandwidth but provides less jitter, which allows smoother transitions in changing images such as video. A lower value uses less bandwidth but results in more jitter. These image quality values apply to the soft host only and have no effect on a soft client. When this setting is disabled or not configured, the default values are used.
`Configure PCoIP session encryption algorithms`	Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation. Checking one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm. By default, both the Salsa20-256round12 and AES-128-GCM algorithms are available for negotiation by this endpoint. This setting applies to both server and client. The endpoints negotiate the actual session encryption algorithm that is used. If FIPS140-2 approved mode is enabled, the **Disable AES-128-GCM encryption** value is always overridden so that AES-128-GCM encryption is enabled. If this setting is disabled or not configured, both the Salsa20-256round12 and AES-128-GCM algorithms are available for negotiation by this endpoint.

Table 8-14. View PCoIP General Session Variables (Continued)

Setting	Description
`Configure PCoIP USB allowed and unallowed device rules`	Specifies the USB devices that are authorized and not authorized for PCoIP sessions that use a zero client that runs Teradici firmware. USB devices that are used in PCoIP sessions must appear in the USB authorization table. USB devices that appear in the USB unauthorization table cannot be used in PCoIP sessions. You can define a maximum of 10 USB authorization rules and a maximum of 10 USB unauthorization rules. Separate multiple rules with the vertical bar (|) character. Each rule can be a combination of a Vendor ID (VID) and a Product ID (PID), or a rule can describe a class of USB devices. A class rule can allow or disallow an entire device class, a single subclass, or a protocol within a subclass. The format of a combination VID/PID rule is **`1xxxxyyyy`**, where **`xxxx`** is the VID in hexadecimal format and **`yyyy`** is the PID in hexadecimal format. For example, the rule to authorize or block a device with VID **`0x1a2b`** and PID **`0x3c4d`** is **`11a2b3c4d`**. For class rules, use one of the following formats: **Allow all USB devices** — Format: **`23XXXXXX`**; Example: **`23XXXXXX`** **Allow USB devices with a specific class ID** — Format: **`22`*`class`*`XXXX`**; Example: **`22aaXXXX`** **Allow a specific subclass** — Format: **`21`*`class-subclass`*`XX`**; Example: **`21aabbXX`** **Allow a specific protocol** — Format: **`20`*`class-subclass-protocol`***; Example: **`20aabbcc`** For example, the USB authorization string to allow USB HID (mouse and keyboard) devices (class ID 0x03) and webcams (class ID 0x0e) is **`2203XXXX|220eXXXX`**. The USB unauthorization string to disallow USB Mass Storage devices (class ID 0x08) is **`2208XXXX`**. An empty USB authorization string means that no USB devices are authorized. An empty USB unauthorization string means that no USB devices are banned. This setting applies to the server only and only when the server is in a session with a zero client that runs Teradici firmware. Device use is negotiated between the endpoints. By default, all devices are allowed and none are disallowed.

Table 8-14. View PCoIP General Session Variables (Continued)

Setting	Description
`Configure PCoIP virtual channels`	Specifies the virtual channels that can and cannot operate over PCoIP sessions. This setting also determines whether to disable clipboard processing on the PCoIP host. Virtual channels that are used in PCoIP sessions must appear on the virtual channel authorization list. Virtual channels that appear in the unauthorized virtual channel list cannot be used in PCoIP sessions. You can specify a maximum of 15 virtual channels for use in PCoIP sessions. Separate multiple channel names with the vertical bar (|) character. For example, the virtual channel authorization string to allow the mksvchan and vdp_rdpvcbridge virtual channels is **`mksvchan|vdp_vdpvcbridge`**. If a channel name contains the vertical bar or backslash (\) character, insert a backslash character before it. For example, type the channel name awk|ward\channel as **`awk\\|ward\\channel`**. When the authorized virtual channel list is empty, all virtual channels are disallowed. When the unauthorized virtual channel list is empty, all virtual channels are allowed. The virtual channels setting applies to both server and client. Virtual channels must be enabled on both server and client for virtual channels to be used. The virtual channels setting provides a separate check box that allows you to disable remote clipboard processing on the PCoIP host. This value applies to the server only. By default, all virtual channels are enabled, including clipboard processing.
`Configure the Client PCoIP UDP port`	Specifies the UDP client port that is used by software PCoIP clients. The UDP port value specifies the base UDP port to use. The UDP port range value determines how many additional ports to try if the base port is not available. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 50002 and the port range is 64, the range spans from 50002 to 50066. This setting applies to the client only. By default, the base port is 50002 and the port range is 64.
`Configure the TCP port to which the PCoIP host binds and listens`	Specifies the TCP server port bound to by software PCoIP hosts. The TCP port value specifies the base TCP port that the server attempts to bind to. The TCP port range value determines how many additional ports to try if the base port is not available. The port range must be between 0 and 10. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182. This setting applies to the server only. By default, the base TCP port is 4172 for View 4.5 and later and 50002 for View 4.0.*x* and earlier. By default, the port range is 1.
`Configure the UDP port to which the PCoIP host binds and listens`	Specifies the UDP server port bound to by software PCoIP hosts. The UDP port value specifies the base UDP port that the server attempts to bind to. The UDP port range value determines how many additional ports to try if the base port is not available. The port range must be between 0 and 10. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 4172 and the port range is 10, the range spans from 4172 to 4182. This setting applies to the server only. By default, the base TCP port is 4172 for View 4.5 and later and 50002 for View 4.0.*x* and earlier. By default, the port range is 10.

Table 8-14. View PCoIP General Session Variables (Continued)

Setting	Description
Enable access to a PCoIP session from a vSphere console	Determines whether to allow a vSphere Client console to display an active PCoIP session and send input to the desktop. By default, when a client is attached through PCoIP, the vSphere Client console screen is blank and the console cannot send input. The default setting ensures that a malicious user cannot view the user's desktop or provide input to the host locally when a PCoIP remote session is active. This setting applies to the server only. When this setting is disabled or not configured, console access is not allowed. When this setting is enabled, the console displays the PCoIP session and console input is allowed. When this setting is enabled, the console can display a PCoIP session that is running on a Windows 7 system only when the Windows 7 virtual machine is hardware v8. Hardware v8 is available only on ESX 5.0 and later. By contrast, console input to a Windows 7 system is allowed when the virtual machine is any hardware version. On a Windows XP or Windows Vista system, the console can display a PCoIP session when the virtual machine is any hardware version.
Enable the FIPS 140-2 approved mode of operation	Determines whether to use only FIPS 140-2 approved cryptographic algorithms and protocols to establish a remote PCoIP connection. Enabling this setting overrides the disabling of AES128-GCM encryption. This setting applies to both server and client. You can configure either endpoint or both endpoints to operate in FIPS mode. Configuring a single endpoint to operate in FIPS mode limits the encryption algorithms that are available for session negotiation. FIPS mode is available for View 4.5 and later. For View 4.0.*x* and earlier, FIPS mode is not available, and configuring this setting has no effect. When this setting is disabled or not configured, FIPS mode is not used.
Enable/disable audio in the PCoIP session	Determines whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. When this setting is enabled, PCoIP audio is allowed. When it is disabled, PCoIP audio is disabled. When this setting is not configured, audio is enabled by default.
Enable/disable microphone noise and DC offset filter in PCoIP session	Determines whether to enable the microphone noise and DC offset filter for microphone input during PCoIP sessions. This setting applies to the server and Teradici audio driver only. When this setting is not configured, the Teradici audio driver uses the microphone noise and DC offset filter by default.
Turn on PCoIP user default input language synchronization	Determines whether the default input language for the user in the PCoIP session is synchronized with the default input language of the PCoIP client endpoint. When this setting is enabled, synchronization is allowed. When this setting is disabled or not configured, synchronization is disallowed. This setting applies to the server only.

View PCoIP Session Bandwidth Variables

The View PCoIP Session Variables ADM template file contains group policy settings that configure PCoIP session bandwidth characteristics.

Table 8-15. View PCoIP Session Bandwidth Variables

Setting	Description
`Configure the maximum PCoIP session bandwidth`	Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic. Set this value to the overall capacity of the link to which your endpoint is connected. For example, for a client that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value. Setting this value prevents the server from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and server to use the lower of the two values that are set on the client and server side. For example, setting a 4Mbit/s maximum bandwidth forces the server to transmit at a lower rate, even though the setting is configured on the client. When this setting is disabled or not configured on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is configured, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second. The default value when this setting is not configured is 90000 kilobits per second. This setting applies to the server and client. If the two endpoints have different settings, the lower value is used.
`Configure the PCoIP session bandwidth floor`	Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session. This setting configures the minimum expected bandwidth transmission rate for the endpoint. When you use this setting to reserve bandwidth for an endpoint, the user does not have to wait for bandwidth to become available, which improves session responsiveness. Make sure that you do not over-subscribe the total reserved bandwidth for all endpoints. Make sure that the sum of bandwidth floors for all connections in your configuration does not exceed the network capability. The default value is 0, which means that no minimum bandwidth is reserved. When this setting is disabled or not configured, no minimum bandwidth is reserved. This setting applies to the server and client, but the setting only affects the endpoint on which it is configured.
`Configure the PCoIP session MTU`	Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session. The MTU size includes IP and UDP packet headers. TCP uses the standard MTU discovery mechanism to set MTU and is not affected by this setting. The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes. Typically, you do not have to change the MTU size. Change this value if you have an unusual network setup that causes PCoIP packet fragmentation. This setting applies to the server and client. If the two endpoints have different MTU size settings, the lowest size is used. If this setting is disabled or not configured, the client uses the default value in the negotiation with the server.

Table 8-15. View PCoIP Session Bandwidth Variables (Continued)

Setting	Description
`Configure the PCoIP session audio bandwidth limit`	Specifies the maximum bandwidth that can be used for audio (sound playback) in a PCoIP session. The audio processing monitors the bandwidth used for audio. The processing selects the audio compression algorithm that provides the best audio possible, given the current bandwidth utilization. If a bandwidth limit is set, the processing reduces quality by changing the compression algorithm selection until the bandwidth limit is reached. If minimum quality audio cannot be provided within the bandwidth limit specified, audio is disabled. To allow for uncompressed high quality stereo audio, set this value to higher than 1600 kbit/s. A value of 450 kbit/s and higher allows for stereo, high-quality, compressed audio. A value between 50 kbit/s and 450 kbit/s results in audio that ranges between FM radio and phone call quality. A value below 50 kbit/s might result in no audio playback. This setting applies to the server only. You must enable audio on both endpoints before this setting has any effect. In addition, this setting has no effect on USB audio. If this setting is disabled or not configured, a default audio bandwidth limit of 500 kilobits per second is configured to constrain the audio compression algorithm selected. If the setting is configured, the value is measured in kilobits per second, with a default audio bandwidth limit of 500 kilobits per second. This setting applies to View 4.6 and later. It has no effect on earlier versions of View.
`Turn off Build-to-Lossless feature`	Specifies whether to disable the build-to-lossless feature of the PCoIP protocol, which is on by default. If you enable this setting, the build-to-lossless feature is disabled. Images and other desktop content are never built to a lossless state. In network environments with constrained bandwidth, disabling the build-to-lossless feature can provide bandwidth savings. Disabling this feature is not recommended in environments that require images and desktop content to be built to a lossless state. To enable this setting, you must click **Enabled** and check the following check box: **I accept to turn off the Build-to-Lossless feature**. This agreement indicates that you understand that images and desktop content are never built to a lossless state. For more information about the PCoIP build-to-lossless feature, see "View PCoIP Build-to-Lossless Feature," on page 166.

View PCoIP Session Variables for the Keyboard

The View PCoIP Session Variables ADM template file contains group policy settings that configure PCoIP session characteristics that affect the use of the keyboard.

Table 8-16. View PCoIP Session Variables for the Keyboard

Setting	Description
Disable sending CAD when users press Ctrl+Alt+Del	When this policy is enabled, users must press Ctrl+Alt+Insert instead of Ctrl+Alt+Del to send a Secure Attention Sequence (SAS) to the desktop during a PCoIP session. You might want to enable this setting if users become confused when they press Ctrl+Alt+Del to lock the client endpoint and an SAS is sent to both the host and the guest. This setting applies to the server only and has no effect on a client. When this policy is not configured or is disabled, users can press Ctrl+Alt +Del or Ctrl+Alt+Insert to send an SAS to the desktop.
Enable Right SHIFT behavior when a PCoIP client is connected	Determines whether to enable substitution of the Right SHIFT key with a Left SHIFT key, which allows the Right SHIFT key to function properly when using RDP through PCoIP. This setting can be useful when RDP is used within a PCoIP session. This setting applies to the server only and has no effect on a client. When this setting is disabled or not configured, the substitution is not performed. On desktops that run View Agent 4.6 and later, the Right SHIFT key functions properly when RDP is used in a PCoIP session. Use this setting only on desktops that run View Agent 4.5 and earlier. For View Agent 4.6, this setting is applied, but it is not needed. For View Agent 5.0 and later, this setting is not applied even when it is configured.

Table 8-16. View PCoIP Session Variables for the Keyboard (Continued)

Setting	Description
`Use alternate key for sending Secure Attention Sequence`	Specifies an alternate key, instead of the Insert key, for sending a Secure Attention Sequence (SAS). You can use this setting to preserve the Ctrl+Alt+Ins key sequence in virtual machines that are launched from inside a View desktop during a PCoIP session. For example, a user can launch a vSphere Client from inside a PCoIP desktop and open a console on a virtual machine in vCenter Server. If the Ctrl+Alt+Ins sequence is used inside the guest operating system on the vCenter Server virtual machine, a Ctrl+Alt+Del SAS is sent to the virtual machine. This setting allows the Ctrl+Alt+*Alternate Key* sequence to send a Ctrl+Alt+Del SAS to the PCoIP desktop. When this setting is enabled, you must select an alternate key from a drop-down menu. You cannot enable the setting and leave the value unspecified. When this setting is disabled or not configured, the Ctrl+Alt+Ins key sequence is used as the SAS. This setting applies to the server only and has no effect on a client.
`Use enhanced keyboard on Windows client if available`	Determines whether to direct keyboard sequences to be restricted to the guest operating system in PCoIP desktop sessions. When you press Ctrl+Alt+Delete, Win+L, or another keyboard sequence, the guest system only, rather than both guest and host, acts on the command. For example, pressing Ctrl+Alt+Delete does not lock the host system. This setting applies to Windows hosts only. Before the enhanced keyboard setting can take effect, the VMware keyboard filter driver, `vmkbd.sys`, must be installed and configured. The VMware keyboard filter driver is automatically installed and configured on computers that have VMware Workstation, Player, or View Client with Local Mode installed. You can use this setting only when View Client is run by a member of the administrator's group on Windows XP or is run under elevated privileges by **Run as administrator** on Windows Vista and later. This setting allows the Windows host system to process keyboard input by an alternative method. It processes raw keyboard input as soon as possible, bypassing Windows keystroke processing and any malware that is not already at a lower layer. Use enhanced virtual keyboard if the virtual machine might be used by someone with an international keyboard or a keyboard with extra keys. When this policy is not configured or disabled, the enhanced keyboard feature is not used.

View PCoIP Build-to-Lossless Feature

The PCoIP display protocol uses an encoding approach called progressive build, which works to provide the optimal overall user experience even under constrained network conditions.

Progressive build provides a highly compressed initial image, called a lossy image, that is then progressively built to a full lossless state. A lossless state means that the image appears with the full fidelity intended.

On a LAN, PCoIP always displays text using lossless compression. If available bandwidth per session drops below 1Mbs, PCoIP initially displays a lossy text image and rapidly builds the image to a lossless state. This approach allows the desktop to remain responsive and display the best possible image during varying network conditions, providing an optimal experience for users.

The build-to-lossless feature provides the following characteristics:

- Dynamically adjusts image quality
- Reduces image quality on congested networks

- Maintains responsiveness by reducing screen update latency
- Resumes maximum image quality when the network is no longer congested

The PCoIP protocol is efficient enough to provide the build-to-lossless feature in all conditions, which allows this feature to stay on by default.

You can disable the build-to-lossless feature by setting the `Turn off Build-to-Lossless feature` group policy setting. See "View PCoIP Session Bandwidth Variables," on page 163.

Setting Up Location-Based Printing

The location-based printing feature maps printers that are physically near client systems to View desktops, enabling users to print to their local and network printers from their View desktops.

The location-based printing feature is available for both Windows and non-Windows client systems. Location-based printing allows IT organizations to map View desktops to the printer that is closest to the endpoint client device. For example, as a doctor moves from room to room in a hospital, each time the doctor prints a document, the print job is sent to the nearest printer. Using this feature does require that the correct printer drivers be installed in the View desktop.

You set up location-based printing by configuring the Active Directory group policy setting `AutoConnect Map Additional Printers for VMware View`, which is located in the Microsoft Group Policy Object Editor in the **Software Settings** folder under **Computer Configuration**.

NOTE `AutoConnect Map Additional Printers for VMware View` is a computer-specific policy. Computer-specific policies apply to all View desktops, regardless of who connects to the desktop.

`AutoConnect Map Additional Printers for VMware View` is implemented as a name translation table. You use each row in the table to identify a specific printer and define a set of translation rules for that printer. The translation rules determine whether the printer is mapped to the View desktop for a particular client system.

When a user connects to a View desktop, View compares the client system to the translation rules associated with each printer in the table. If the client system meets all of the translation rules set for a printer, or if a printer has no associated translation rules, View maps the printer to the View desktop during the user's session.

You can define translation rules based on the client system's IP address, name, and MAC address, and on the user's name and group. You can specify one translation rule, or a combination of several translation rules, for a specific printer.

The information used to map the printer to the View desktop is stored in a registry entry on the View desktop in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

1 Register the Location-Based Printing Group Policy DLL File on page 167

   Before you can configure the group policy setting for location-based printing, you must register the DLL file `TPVMGPoACmap.dll`.

2 Configure the Location-Based Printing Group Policy on page 168

   To set up location-based printing, you configure the `AutoConnect Map Additional Printers for VMware View` group policy setting. The group policy setting is a name translation table that maps printers to View desktops.

Register the Location-Based Printing Group Policy DLL File

Before you can configure the group policy setting for location-based printing, you must register the DLL file `TPVMGPoACmap.dll`.

View provides 32-bit and 64-bit versions of `TPVMGPoACmap.dll` in the directory *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` on your View Connection Server host.

Procedure

1 Copy the appropriate version of `TPVMGPoACmap.dll` to your Active Directory server or to the domain computer that you use to configure group policies.

2 Use the `regsvr32` utility to register the `TPVMGPoACmap.dll` file.

For example: `regsvr32 "C:\TPVMGPoACmap.dll"`

What to do next

Configure the group policy setting for location-based printing.

Configure the Location-Based Printing Group Policy

To set up location-based printing, you configure the `AutoConnect Map Additional Printers for VMware View` group policy setting. The group policy setting is a name translation table that maps printers to View desktops.

Prerequisites

- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server or on the domain computer that you use to configure group policies.
- Register the DLL file `TPVMGPoACmap.dll` on your Active Directory server or on the domain computer that you use to configure group policies. See "Register the Location-Based Printing Group Policy DLL File," on page 167.
- Familiarize yourself with syntax of the `AutoConnect Map Additional Printers for VMware View` group policy setting. See "Location-Based Printing Group Policy Setting Syntax," on page 169.
- Create a GPO for the location-based group policy setting and link it to the OU that contains your View desktops. See "Create GPOs for View Group Policies," on page 172 for an example of how to create GPOs for View group policies.
- Because print jobs are sent directly from the View desktop to the printer, verify that the required printer drivers are installed on your desktops.

Procedure

1 On your Active Directory server or on the computer that you use to configure group policies, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

2 Right-click the OU that contains your View desktops and select **Properties**.

3 On the Group Policy tab, click **Open** to open the Group Policy Management plug-in.

4 In the right pane, right-click the GPO that you created for the location-based printing group policy setting and select **Edit**.

The Group Policy Object Editor window appears.

5 Expand **Computer Configuration**, open the **Software Settings** folder, and select **AutoConnect Map Additional Printers for VMware View**.

6 In the Policy pane, double-click **Configure AutoConnect Map Additional Printers**.

The AutoConnect Map Additional Printers for VMware View window appears.

7 Select **Enabled** to enable the group policy setting.

The translation table headings and buttons appear in the group policy window.

IMPORTANT Clicking **Disabled** deletes all table entries. As a precaution, save your configuration so that you can import it later.

---

8 Add the printers that you want to map to View desktops and define their associated translation rules.

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

Location-Based Printing Group Policy Setting Syntax

You use the `AutoConnect Map Additional Printers for VMware View` group policy setting to map printers to View desktops.

`AutoConnect Map Additional Printers for VMware View` is a name translation table that identifies printers and defines associated translation rules. Table 8-17 describes the syntax of the translation table.

Table 8-17. Translation Table Columns and Values

Column	Description
`IP Range`	A translation rule that specifies a range of IP addresses for client systems. To specify IP addresses in a specific range, use the following notation: ***ip_address-ip_address*** For example: **`10.112.116.0-10.112.119.255`** To specify all of the IP addresses in a specific subnet, use the following notation: *ip_address/subnet_mask_bits* For example: **`10.112.4.0/22`** This notation specifies the usable IPv4 addresses from 10.112.4.1 to 10.112.7.254. Type an asterisk to match any IP address.
`Client Name`	A translation rule that specifies a computer name. For example: **`Mary's Computer`** Type an asterisk to match any computer name.
`Mac Address`	A translation rule that specifies a MAC address. In the GPO editor, you must use the same format that the client system uses. For example: ■ Windows clients use hyphens: **`01-23-45-67-89-ab`** ■ Linux clients use colons: **`01:23:45:67:89:ab`** Type an asterisk to match any MAC address.
`User/Group`	A translation rule that specifies a user or group name. For example: **`jdoe`** Type an asterisk to match any user name or group.
`Printer Name`	The name of the printer when it is mapped to the View desktop. For example: **`PRINTER-2-CLR`** The mapped name does not have to match the printer name on the client system.
`Printer Driver`	The name of the driver that the printer uses. For example: **`HP Color LaserJet 4700 PS`** IMPORTANT Because print jobs are sent directly from the desktop to the printer, the printer driver must be installed on the desktop.
`IP Port/ThinPrint Port`	For network printers, the IP address of the printer prepended with **`IP_`**. For example: **`IP_10.114.24.1`**
`Default`	Indicates whether the printer is the default printer.

You use the buttons that appear above the column headings to add, delete, and move rows and save and import table entries. Each button has an equivalent keyboard shortcut. Mouse over each button to see a description of the button and its equivalent keyboard shortcut. For example, to insert a row at the end of the table, click the first table button or press Alt+A. Click the last two buttons to import and save table entries.

Table 8-18 shows an example of two translation table rows.

Table 8-18. Location-Based Printing Group Policy Setting Example

IP Range	Client Name	Mac Address	User/ Group	Printer Name	Printer Driver	IP Port/ThinPrint Port	Default
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

The network printer specified in the first row will be mapped to a View desktop for any client system because asterisks appear in all of the translation rule columns. The network printer specified in the second row will be mapped to a View desktop only if the client system has an IP address in the range 10.112.116.140 through 10.112.116.145.

Using Terminal Services Group Policies

You can use standard Microsoft Windows Terminal Services group policies to centrally control the configuration of View desktops.

In Windows Vista and later operating systems, Terminal Services are called Remote Desktop Services.

NOTE Terminal Services must be started on the virtual machine that you use to create pools and on View desktops. Terminal Services are required for View Agent installation, SSO, and other View session-management operations.

To find Terminal Services group policy settings in the Group Policy Object Editor, expand the **Computer Configuration** or **User Configuration** folder and then expand the **Administrative Templates**, **Windows Components**, and **Terminal Services** folders.

General Terminal Services Group Policy Settings

General Terminal Services group policies include settings that control log in and log off behavior, remote sessions, and desktop appearance.

Table 8-19 describes the Computer Configuration Terminal Services group policy settings that you can use to manage View desktops.

Table 8-19. General Terminal Services Policy Settings

Setting	Description
`Enforce Removal of Remote Desktop Wallpaper`	Enabling this setting enforces the removal of wallpaper during a remote session, enhancing the user experience over low-bandwidth connections.
`Limit maximum color depth`	Enabling this setting lets you specify the color depth of View desktop sessions.
`Allow users to connect remotely using Terminal Services`	Enabling this setting allows users to connect remotely to the target computer.

Table 8-19. General Terminal Services Policy Settings (Continued)

Setting	Description
`Remove Windows Security item from Start Menu`	Disabling this setting makes the Windows Security item appear in the Settings menu, ensuring that users have a logoff mechanism.
`Remove Disconnect option from Shut Down dialog`	Enabling this setting removes the Disconnect option from the Shut Down Windows dialog box, reducing the possibility of users disconnecting instead of logging off.

Terminal Services Group Policy Settings for Sessions

Terminal Services group policy settings for sessions include settings that control disconnected and idle client sessions.

Table 8-20 describes the Computer Configuration and User Configuration Terminal Services group policy settings that you can use to manage session-related properties for View desktops and users.

Table 8-20. Terminal Services Policy Settings for Sessions

Setting	Description
`Set time limit for disconnected sessions`	Enabling this setting lets you set a time limit for disconnected sessions. Disconnected sessions are logged off after the specified time limit.
`Sets a time limit for active but idle Terminal Services sessions`	Enabling this setting lets you set a time limit for idle sessions. Idle sessions are logged off after the specified time limit.

You can combine these settings with View desktop power policies to create a dynamic solution for suspending or powering off disconnected View desktops. When View desktops are suspended or powered off, resources become available to other desktops.

Active Directory Group Policy Example

One way to implement Active Directory group policies in View is to create an OU for your View desktops and link one or more GPOs to that OU. You can use these GPOs to apply group policy settings to your View desktops and to enable loopback processing.

You can configure policies on your Active Directory Server or on any computer in your domain. This example shows how to configure policies directly on your Active Directory server.

NOTE Because every View environment is different, you might need to perform different steps to meet your organization's specific needs.

Procedure

1 Create an OU for View Desktops on page 172

To apply group policies to View desktops without affecting other Windows computers in the same Active Directory domain, create an OU specifically for your View desktops.

2 Create GPOs for View Group Policies on page 172

Create GPOs to contain group policies for View components and location-based printing and link them to the OU for your View desktops.

3 Add View ADM Templates to a GPO on page 173

To apply View component group policy settings to your View desktops, add their ADM template files to GPOs.

4 Enable Loopback Processing for View Desktops on page 174

To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, enable loopback processing.

Create an OU for View Desktops

To apply group policies to View desktops without affecting other Windows computers in the same Active Directory domain, create an OU specifically for your View desktops.

Procedure

1 On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

2 Right-click the domain that contains your View desktops and select **New > Organizational Unit**.

3 Type a name for the OU and click **OK**.

The new OU appears in the left pane.

4 To add View desktops to the new OU:

a Click **Computers** in the left pane.

All the computer objects in the domain appear in the right pane.

b Right-click the name of the computer object that represents the View desktop in the right panel and select **Move**.

c Select the OU and click **OK**.

The View desktop appears in the right pane when you select the OU.

What to do next

Create GPOs for View group policies.

Create GPOs for View Group Policies

Create GPOs to contain group policies for View components and location-based printing and link them to the OU for your View desktops.

Prerequisites

- Create an OU for your View desktops.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

Procedure

1 On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

2 Right-click the OU that contains your View desktops and select **Properties**.

3 On the Group Policy tab, click **Open** to open the Group Policy Management plug-in.

4 Right-click the OU and select **Create and Link a GPO Here**.

5 Type a name for the GPO and click **OK**.

The new GPO appears under the OU in the left pane.

6 (Optional) To apply the GPO only to specific View desktops in the OU:

a Select the GPO in the left pane.

b Select **Security Filtering > Add**.

c Type the computer names of the View desktops and click **OK**.

The View desktops appear in the Security Filtering pane. The settings in the GPO apply only to these View desktops.

What to do next

Add the View ADM templates to the GPO for group policies.

Add View ADM Templates to a GPO

To apply View component group policy settings to your View desktops, add their ADM template files to GPOs.

Prerequisites

- Create GPOs for the View component group policy settings and link them to the OU that contains your View desktops.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

Procedure

1 Copy the View component ADM Template files from the *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles directory on your View Connection Server host to your Active Directory server.

2 On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

3 Right-click the OU that contains your View desktops and select **Properties**.

4 On the Group Policy tab, click **Open** to open the Group Policy Management plug-in.

5 In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

The Group Policy Object Editor window appears.

6 In the Group Policy Object Editor, right-click **Administrative Templates** under **Computer Configuration** and then select **Add/Remove Templates**.

7 Click **Add**, browse to the ADM Template file, and click **Open**.

8 Click **Close** to apply the policy settings in the ADM Template file to the GPO.

The name of the template appears in the left pane under **Administrative Templates**.

9 Configure the group policy settings.

What to do next

Enable loopback processing for your View desktops.

Enable Loopback Processing for View Desktops

To make User Configuration settings that usually apply to a computer apply to all of the users that log in to that computer, enable loopback processing.

Prerequisites

- Create GPOs for the View component group policy settings and link them to the OU that contains your View desktops.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.

Procedure

1. On your Active Directory server, select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right-click the OU that contains your View desktops and select **Properties**.
3. On the Group Policy tab, click **Open** to open the Group Policy Management plug-in.
4. In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

   The Group Policy Object Editor window appears.
5. Expand the **Computer Configuration** folder and then expand the **Administrative Templates**, **System**, and **Group Policy** folders.
6. In the right pane, right-click **User Group Policy loopback processing mode** and select **Properties**.
7. On the **Setting** tab, select **Enabled** and then select a loopback processing mode from the **Mode** drop-down menu.

Option	Action
Merge	The user policy settings applied are the combination of those included in both the computer and user GPOs. Where conflicts exist, the computer GPOs take precedence.
Replace	The user policy is defined entirely from the GPOs associated with the computer. Any GPOs associated with the user are ignored.

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

Configuring User Profiles with View Persona Management

9

With View Persona Management, you can configure user profiles that are dynamically synchronized with a remote profile repository. This feature gives users access to a personalized desktop experience whenever they log in to a desktop. View Persona Management expands the functionality and improves the performance of Windows roaming profiles.

You configure group policy settings to enable View Persona Management and control various aspects of your View Persona Management deployment.

To enable and use View Persona Management, you must have a View Premier license. See the VMware End User Licensing Agreement (EULA) at http://www.vmware.com/download/eula.

This chapter includes the following topics:

Providing User Personas in View

With the View Persona Management feature, a user's remote profile is dynamically downloaded when the user logs in to a View desktop. You can configure View to store user profiles in a secure, centralized repository. View downloads persona information as the user needs it.

View Persona Management is an alternative to Windows roaming profiles. View Persona Management expands functionality and improves performance compared to Windows roaming profiles.

You can configure and manage personas entirely within View. You do not have to configure Windows roaming profiles. If you have a Windows roaming profiles configuration, you can use your existing repository configuration with View.

A user profile is independent of the virtual desktop. When a user logs in to any desktop, the same profile appears.

For example, a user might log in to a floating-assignment, linked-clone desktop pool and change the desktop background and Microsoft Word settings. When the user starts the next session, the virtual machine is different, but the user sees the same settings.

A user profile comprises a variety of user-generated information:

- User-specific data and desktop settings
- Application data and settings

- Windows registry entries configured by user applications

Also, if you provision desktops with ThinApp applications, the ThinApp sandbox data can be stored in the user profile and roamed with the user.

View Persona Management minimizes the time it takes to log in to and log off of desktops. Login and logoff time can be a problem with Windows roaming profiles.

- During login, View downloads only the files that Windows requires, such as user registry files. Other files are copied to the local desktop when the user or an application opens them from the local profile folder.
- View copies recent changes in the local profile to the remote repository, typically once every few minutes. The default is every 10 minutes. You can specify how often to upload the local profile.
- During logoff, only files that were updated since the last replication are copied to the remote repository.

Persona Management and Windows Roaming Profiles

When Persona Management is enabled, you cannot manage View users' personas by using the Windows roaming profiles functions.

For example, if you log in to a desktop's guest operating system, navigate to the **Advanced** tab in the System Properties dialog box, and change the User Profiles settings from **Roaming profile** to **Local profile**, View Persona Management continues to synchronize the user's persona between the local desktop and the remote persona repository.

However, you can specify files and folders within users' personas that are managed by Windows roaming profiles functionality instead of View Persona Management. You use the **Windows Roaming Profiles Synchronization** policy to specify these files and folders.

Configuring a View Persona Management Deployment

To configure View Persona Management, you set up a remote repository that stores user profiles, install View Agent with the **View Persona Management** setup option on virtual machine desktops, add and configure View Persona Management group policy settings, and deploy desktop pools.

Overview of Setting Up a View Persona Management Deployment

To set up a View desktop deployment with View Persona Management, you must perform several high-level tasks.

This sequence is recommended, although you can perform these tasks in a different sequence. For example, you can configure or reconfigure group policy settings in Active Directory after you deploy desktop pools.

1 Configure a remote repository to store user profiles.

  You can configure a network share or use an existing Active Directory user profile path that you configured for Windows roaming profiles.

2 Install View Agent with the **View Persona Management** setup option on the virtual machines that you use to create desktop pools.

3 Add the View Persona Management Administrative (ADM) Template file to your Active Directory server or the Local Computer Policy configuration on the parent virtual machine.

  To configure View Persona Management for your whole View deployment, add the ADM Template file to Active Directory.

  To configure View Persona Management for one desktop pool, you can take these approaches:

  - Add the ADM Template file to the virtual machine that you use to create the pool.

- Add the ADM Template file to Active Directory and apply the group policy settings to the OU that contains the desktops in the pool.

4 Enable View Persona Management by enabling the **Manage user persona** group policy setting.

5 If you configured a network share for the remote profile repository, enable the **Persona repository location** group policy setting and specify the network share path.

6 (Optional) Configure other group policy settings in Active Directory or the Local Computer Policy configuration.

7 Create desktop pools from the virtual machines on which you installed View Agent with the **View Persona Management** setup option.

Configure a User Profile Repository

You can configure a remote repository to store the user data and settings, application-specific data, and other user-generated information in user profiles. If Windows roaming profiles are configured in your deployment, you can use an existing Active Directory user profile path instead.

NOTE You can configure View Persona Management without having to configure Windows roaming profiles.

Prerequisites

Familiarize yourself with the guidelines for creating a user profile repository. See "Creating a Network Share for View Persona Management," on page 177.

Procedure

1 Determine whether to use an existing Active Directory user profile path or configure a user profile repository on a network share.

Option	Action
Use an existing Active Directory user profile path	If you have an existing Windows roaming profiles configuration, you can use the user profile path in Active Directory that supports roaming profiles. You can skip the remaining steps in this procedure.
Configure a network share to store the user profile repository	If you do not have an existing Windows roaming profiles configuration, you must configure a network share for the user profile repository. Follow the remaining steps in this procedure.

2 Create a shared folder on a computer that your users can access from the guest operating systems on their desktops.

If `%username%` is not part of the folder path that you configure, View Persona Management appends `%username%.%userdomain%` to the path.

For example: `\\server.domain.com\VPRepository\%username%.%userdomain%`

3 Set access permissions for the shared folders that contain user profiles.

Set the permissions that you would use to configure security for Windows roaming profiles. For details, see the Microsoft TechNet topic, *Security Recommendations for Roaming User Profiles Shared Folders*. http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx

Creating a Network Share for View Persona Management

You must follow certain guidelines when you create a shared folder to use as a profile repository.

- You can create the shared folder on a server, a network-attached storage (NAS) device, or a network server.
- The shared folder does not have to be in the same domain as View Connection Server.

- The shared folder must be in the same Active Directory forest as the users who store profiles in the shared folder.
- You must use a shared drive that is large enough to store the user profile information for your users. To support a large View deployment, you can configure separate repositories for different desktop pools.

  If users are entitled to more than one pool, the pools that share users must be configured with the same profile repository. If you entitle a user to two pools with two different profile repositories, the user cannot access the same version of the profile from desktops in each pool.
- You must create the full profile path under which the user profile folders will be created. If part of the path does not exist, Windows creates the missing folders when the first user logs in and assigns the user's security restrictions to those folders. Windows assigns the same security restrictions to every folder it creates under that path.

  For example, for `user1` you might configure the View Persona Management path `\\server\VPRepository\profiles\user1`. If you create the network share `\\server\VPRepository`, and the `profiles` folder does not exist, Windows creates the path `\profiles\user1` when `user1` logs in. Windows restricts access to the `\profiles\user1` folders to the `user1` account. If another user logs in with a profile path in `\\server\VPRepository\profiles`, the second user cannot access the repository and the user's profile fails to be replicated.

Install View Agent with the View Persona Management Option

To use View Persona Management with View desktops, you must install View Agent with the **View Persona Management** setup option on the virtual machines that you use to create desktop pools.

For an automated pool, you install View Agent with the **View Persona Management** setup option on the virtual machine that you use as a parent or template. When you create a desktop pool from the virtual machine, the View Persona Management software is deployed on your View desktops.

For a manual pool, you must install View Agent with the **View Persona Management** setup option on each virtual machine that is used as a desktop source in the pool. Use Active Directory to configure View Persona Management group policies for a manual pool. The alternative is to add the ADM Template file and configure group policies on each individual desktop source.

NOTE A user cannot access the same profile if the user switches between desktops that have v1 user profiles and v2 user profiles. Windows XP uses v1 profiles. Windows Vista and Windows 7 use v2 profiles.

For example, if a user logs in to a Windows XP desktop and later logs in to a Windows 7 desktop, the Windows 7 virtual machine cannot read the v1 profile that was created during the Windows XP desktop session.

Prerequisites

- Verify that you are performing the installation on a Windows 7, Windows Vista, or Windows XP virtual machine. View Persona Management does not operate on physical computers or Microsoft Terminal Servers.
- Verify that you can log in as an administrator on the virtual machine.
- Verify that a native RTO Virtual Profiles 2.0 is not installed on the virtual machine. If a native RTO Virtual Profile 2.0 is present, uninstall it before you install View Agent with the **View Persona Management** setup option.
- On Windows XP virtual machines, download and install the Microsoft User Profile Hive Cleanup Service (UPHClean) in the guest operating system. See "Installing UPHClean on Windows XP Desktops That Use View Persona Management," on page 179.
- Familiarize yourself with installing View Agent. See "Install View Agent on a Virtual Machine," on page 49 or "Install View Agent on an Unmanaged Desktop Source," on page 41.

Procedure

- When you install View Agent on a virtual machine, select the **View Persona Management** setup option.

What to do next

Add the View Persona Management ADM Template file to your Active Directory server or the Local Computer Policy configuration on the virtual machine itself. See "Add the View Persona Management ADM Template File," on page 179.

Installing UPHClean on Windows XP Desktops That Use View Persona Management

The Microsoft User Profile Hive Cleanup Service (UPHClean) ensures that user sessions are completely terminated when a user logs off. UPHClean cleans registry key handles that might be stranded by other processes and applications. This service helps to ensure that the user's registry hive is unloaded so that it can be uploaded successfully and the local persona can be deleted.

If you configure View Persona Management on Windows XP virtual machines, download and install UPHClean in the guest operating system.

You can download the UPHClean service at the following location: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6676.

The UPHClean service is included with Windows 7 and Windows Vista operating systems. You do not have to install the service on these operating systems.

Add the View Persona Management ADM Template File

The View Persona Management Administrative (ADM) Template file contains group policy settings that allow you to configure View Persona Management. Before you can configure the policies, you must add the ADM Template file to the local virtual machines or Active Directory server.

To configure View Persona Management on a single virtual machine, you can add the group policy settings to the Local Computer Policy configuration on that local system.

To configure View Persona Management for a desktop pool, you can add the group policy settings to the Local Computer Policy configuration on the virtual machine that you use as a parent or template for deploying the desktop pool.

To configure View Persona Management at the domain-wide level and apply the configuration to many desktops or your whole deployment, you can add the group policy settings to Group Policy Objects (GPOs) on your Active Directory server. In Active Directory, you can create an OU for the desktops that use View Persona Management, create one or more GPOs, and link the GPOs to the OU. To configure separate View Persona Management policies for different types of users, you can create OUs for particular sets of desktops and apply different GPOs to the OUs.

For an example of implementing Active Directory group policies in View, see "Active Directory Group Policy Example," on page 171.

Add the Persona Management ADM Template to a Single System

To configure View Persona Management for a single desktop pool, you must add the Persona Management ADM Template file to the Local Computer Policy on the virtual machine that you use to create the pool. To configure View Persona Management on a single system, you must add the Persona Management ADM Template file to that system.

Prerequisites

- Verify that View Agent is installed with the View Persona Management setup option on the system. See "Install View Agent with the View Persona Management Option," on page 178.
- Verify that you can log in as an administrator on the system.

Procedure

1 On the local system, click **Start > Run**.

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

3 In the Local Computer Policy window, navigate to **Computer Configuration** and right-click **Administrative Templates**.

NOTE Do not select **Administrative Templates** under **User Configuration**.

4 Click **Add/Remove Templates** and click **Add**.

5 Browse to the *install_directory*\VMware\VMware View\Agent\bin directory.

The ADM Template file, ViewPM.adm, is located in this directory.

The ViewPM.adm file is also installed with the other View ADM Template files in the *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles directory on the View Connection Server host.

6 Select the ViewPM.adm file and click **Add**.

7 Close the Add/Remove Templates window.

The View Persona Management group policy settings are added to the Local Computer Policy configuration on the local system. You must use gpedit.msc to display this configuration.

What to do next

Configure the View Persona Management group policy settings on the local system. See "Configure View Persona Management Policies," on page 181.

Add the Persona Management ADM Template to Active Directory

To configure View Persona Management for your deployment, you can add the Persona Management ADM Template file to a Group Policy Object (GPO) in your Active Directory server.

Prerequisites

- Create GPOs for your View Persona Management deployment and link them to the OU that contains the View desktops that use View Persona Management. See "Active Directory Group Policy Example," on page 171.
- Verify that the Microsoft MMC and the Group Policy Object Editor snap-in are available on your Active Directory server.
- Verify that View Agent is installed with the View Persona Management setup option on a system that is accessible to your Active Directory server. See "Install View Agent with the View Persona Management Option," on page 178.

Procedure

1 Copy the View Persona Management ADM Template file, ViewPM.adm, to your Active Directory server.

The ViewPM.adm file is located in the *install_directory*\VMware\VMware View\Server\extras\GroupPolicyFiles directory on the View Connection Server host.

2 On your Active Directory server, open the Group Policy Management Console.

For example, start the Run dialog box, type **gpmc.msc**, and click **OK**.

3 In the left pane, select the domain or OU that contains your View desktops.

4 In the right pane, right-click the GPO that you created for the group policy settings and select **Edit**.

The Group Policy Object Editor window appears.

5 In the Group Policy Object Editor, right-click **Administrative Templates** under **Computer Configuration** and select **Add/Remove Templates**.

6 Click **Add**, browse to the `ViewPM.adm` file, and click **Open**.

7 Click **Close** to apply the policy settings in the ADM Template file to the GPO.

The name of the template appears in the left pane under **Administrative Templates**.

What to do next

Configure the View Persona Management group policy settings on your Active Directory server.

Configure View Persona Management Policies

To use View Persona Management, you must enable the **Manage user persona** group policy setting, which activates the View Persona Management software. To set up a user profile repository without using an Active Directory user profile path, you must configure the **Persona repository location** group policy setting.

You can configure the optional group policy settings to configure other aspects of your View Persona Management deployment.

If Windows roaming profiles are already configured in your deployment, you can use an existing Active Directory user profile path. You can leave the **Persona repository location** setting disabled or not configured.

Prerequisites

- Familiarize yourself with the **Manage user persona** and **Persona repository location** group policy settings. See "Roaming and Synchronization Group Policy Settings," on page 186.
- If you are setting group policies on a local system, familiarize yourself with opening the Group Policy window. See steps Step 1 and Step 2 in "Add the Persona Management ADM Template to a Single System," on page 179.
- If you are setting group policies on your Active Directory server, familiarize yourself with starting the Group Policy Object Editor. See steps Step 2 through Step 4 in "Add the Persona Management ADM Template to Active Directory," on page 180.

Procedure

1 Open the Group Policy window.

Option	Description
Local system	Open the Local Computer Policy window.
Active Directory server	Open the Group Policy Object Editor window.

2 Expand the **Computer Configuration** folder and navigate to the **Persona Management** folder.

Option	Description
Windows XP or Windows Server 2003	Expand the following folders: **Administrative Templates**, **VMware View Agent Configuration**, **Persona Management**
Windows Vista and later or Windows Server 2008 and later	Expand the following folders: **Administrative Templates**, **Classic Administrative Templates (ADM)**, **VMware View Agent Configuration**, **Persona Management**

3 Open the **Roaming & Synchronization** folder.

4 Double-click **Manage user persona** and click **Enabled**.

This setting activates View Persona Management. When this setting is disabled or not configured, View Persona Management does not function.

5 Type the profile upload interval, in minutes, and click **OK**.

The profile upload interval determines how often View Persona Management copies user profile changes to the remote repository. The default upload interval is 10 minutes.

6 Double-click **Persona repository location** and click **Enabled**.

If you have an existing Windows roaming profiles deployment, you can use an Active Directory user profile path for the remote profile repository. You do not have to configure a **Persona repository location**.

7 Type the UNC path to a network file server share that stores the user profiles.

For example: `\\server.domain.com\UserProfilesRepository\%username%`

The network share must be accessible to the virtual machines in your deployment.

If you intend to use an Active Directory user profile path, you do not have to specify a UNC path.

8 If an Active Directory user profile path is configured in your deployment, determine whether to use or override this path.

Option	Action
Use the network share.	Check the **Override Active Directory user profile path if it is configured** check box.
Use an Active Directory user profile path, if one exists.	Do not check the **Override Active Directory user profile path if it is configured** check box.

9 Click **OK**.

10 (Optional) Configure other View Persona Management group policy settings.

Create View Desktops That Use Persona Management

To use View Persona Management with View desktops, you must create desktop pools with a View Persona Management agent installed on each desktop.

You must deploy View Persona Management on virtual machines. You cannot use View Persona Management on physical computers or Microsoft Terminal Servers.

You cannot use View Persona Management with desktops that run in local mode.

Prerequisites

- Verify that View Agent with the **View Persona Management** setup option is installed on the virtual machine that you use to create the desktop pool. See "Install View Agent with the View Persona Management Option," on page 178.
- If you intend to configure View Persona Management policies for this pool only, verify that you added the View Persona Management ADM Template file to the virtual machine and configured group policy settings in the Local Computer Policy configuration. See "Add the Persona Management ADM Template to a Single System," on page 179 and "Configure View Persona Management Policies," on page 181.

Procedure

- Generate a snapshot or template from the virtual machine and create an automated desktop pool.

  You can configure View Persona Management with pools that contain full virtual machines or linked clones. The pools can use dedicated or floating assignments.

- (Optional) To use View Persona Management with manual desktop pools, select desktop sources on which View Agent with the **View Persona Management** option is installed.

NOTE After you deploy View Persona Management on your View desktops, if you remove the **View Persona Management** setup option on the desktops, or uninstall View Agent altogether, the local user profiles are removed from the desktops of users who are not currently logged in. For users who are currently logged in, the user profiles are downloaded from the remote profile repository during the uninstall process.

Best Practices for Configuring a View Persona Management Deployment

You should follow best practices for configuring View Persona Management to enhance your users' desktop experience, improve desktop performance, and ensure that View Persona Management operates efficiently with other View features.

Determining Whether to Remove Local User Profiles at Logoff

By default, View Persona Management does not delete user profiles from the local desktops when users log off. The **Remove local persona at log off** policy is disabled. In many cases, the default setting is a best practice because it reduces I/O operations and avoids redundant behavior.

For example, keep this policy disabled if you deploy floating-assignment pools and either refresh or delete the desktops on logoff. The local profile is deleted when the virtual machine is refreshed or deleted. In a floating-assignment, automated pool, full virtual machines can be deleted after logoff. In a floating-assignment, linked-clone pool, the clones can be refreshed or deleted on logoff.

If you deploy dedicated-assignment pools, you can keep the policy disabled because users return to the same desktops at each session. With the policy disabled, when a user logs in, View Persona Management does not have to download files that are present in the local profile. If you configure dedicated-assignment, linked-clone pools with persistent disks, keep the policy disabled to avoid deleting user data from the persistent disks.

In some cases, you might want to enable the **Remove local persona at log off** policy.

Handling Deployments That Include View Persona Management and Windows Roaming Profiles

In deployments in which Windows roaming profiles are configured, and users access View desktops with View Persona Management and standard desktops with Windows roaming profiles, the best practice is to use different profiles for the two desktop environments. If a View desktop and the client computer from which the desktop is launched are in the same domain, and you use an Active Directory GPO to configure both Windows roaming profiles and View Persona Management, enable the **Persona repository location** policy and select **Override Active Directory user profile path if it is configured**.

This approach prevents Windows roaming profiles from overwriting a View Persona Management profile when the user logs off from the client computer.

If users intend to share data between existing Windows roaming profiles and View Persona Management profiles, you can configure Windows folder redirection.

Configuring Paths for Redirected Folders

When you use the **Folder Redirection** group policy setting, configure the folder path to include `%username%`, but make sure that the last subfolder in the path uses the name of the redirected folder, such as `My Videos`. The last folder in the path is displayed as the folder name on the user's desktop.

For example, if you configure a path such as `\\myserver\videos\%username%\My Videos`, the folder name that appears on the user's desktop is `My Videos`.

If `%username%` is the last subfolder in the path, the user's name appears as the folder name. For example, instead of seeing a `My Videos` folder on the desktop, the user `JDoe` sees a folder named `JDoe` and cannot easily identify the folder.

Additional Best Practices

You can also follow these recommendations:

- By default, many antivirus products do not scan offline files. For example, when a user logs in to a desktop, these anti-virus products do not scan user profile files that are not specified in the **Files and folders to preload** or **Windows roaming profiles synchronization** group policy setting. For many deployments, the default behavior is the best practice because it reduces the I/O required to download files during on-demand scans.

  If you do want to retrieve files from the remote repository and enable scanning of offline files, see the documentation for your antivirus product.

- It is highly recommended that you use standard practices to back up network shares on which View Persona Management stores the profile repository.

  NOTE Do not use backup software such as MozyPro or Windows Volume backup services with View Persona Management to back up user profiles on View desktops.

  View Persona Management ensures that user profiles are backed up to the remote profile repository, eliminating the need for additional tools to back up user data on the desktops. In certain cases, tools such as MozyPro or Windows Volume backup services can interfere with View Persona Management and cause data loss or corruption.

- You can set View Persona Management policies to enhance performance when users start ThinApp applications. See "Configuring User Profiles to Include ThinApp Sandbox Folders," on page 184.

- If your users generate substantial persona data, and you plan to use refresh and recompose to manage dedicated-assignment, linked-clone desktops, configure your desktop pool to use separate View Composer persistent disks. Persistent disks can enhance the performance of View Persona Management. See "Configuring View Composer Persistent Disks with View Persona Management," on page 185.

Configuring User Profiles to Include ThinApp Sandbox Folders

View Persona Management maintains user settings that are associated with ThinApp applications by including ThinApp sandbox folders in user profiles. You can set View Persona Management policies to enhance performance when users start ThinApp applications.

View Persona Management preloads ThinApp sandbox folders and files in the local user profile when a user logs in. The ThinApp sandbox folders are created before a user can complete the log on. To enhance performance, View Persona Management does not download the ThinApp sandbox data during the login, although files are created on the local desktop with the same basic attributes and sizes as the ThinApp sandbox files in the user's remote profile.

As a best practice, download the actual ThinApp sandbox data in the background. Enable the **Folders to background download** group policy setting and add the ThinApp sandbox folders. See "Roaming and Synchronization Group Policy Settings," on page 186.

The actual ThinApp sandbox files can be large. With the **Folders to background download** setting, users do not have to wait for large files to download when they start an application. Also, users do not have to wait for the files to preload when they log in, as they might if you use the **Files and folders to preload** setting with large files.

Configuring View Composer Persistent Disks with View Persona Management

With View Composer persistent disks, you can preserve user data and settings while you manage linked-clone OS disks with refresh, recompose, and rebalance operations. Configuring persistent disks can enhance the performance of View Persona Management when users generate a large amount of persona information. You can configure persistent disks only with dedicated-assignment, linked-clone desktops.

View Persona Management maintains each user profile on a remote repository that is configured on a network share. After a user logs into a desktop, the persona files are dynamically downloaded as the user needs them.

If you configure persistent disks with View Persona Management, you can refresh and recompose the linked-clone OS disks and keep a local copy of the each user profile on the persistent disks.

The persistent disks can act as a cache for the user profiles. When a user requires persona files, View Persona Management does not need to download data that is the same on the local persistent disk and the remote repository. Only unsynchronized persona data needs to be downloaded.

If you configure persistent disks, do not enable the **Remove local persona at log off** policy. Enabling this policy deletes the user data from the persistent disks when users log off.

View Persona Management Group Policy Settings

The View Persona Management ADM Template file contains group policy settings that you add to the Group Policy configuration on individual systems or on an Active Directory server. You must configure the group policy settings to set up and control various aspects of View Persona Management.

The ADM Template file, `ViewPM.adm`, is installed with the other View ADM Template files in the *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles` directory on the View Connection Server host.

When you install View Agent with the **View Persona Management** setup option, the `ViewPM.adm` file is also installed on the virtual machine in the *`install_directory`*`\VMware\VMware View\Agent\bin` directory.

After you add the `ViewPM.adm` file to your Group Policy configuration, the policy settings are located in the **Persona Management** folder in the Group Policy window.

Table 9-1. Location of View Persona Management Settings in the Group Policy Window

Operating System	Location
Windows Vista and later or Windows Server 2008 and later	**Computer Configuration** > **Administrative Templates** > **Classic Administrative Templates (ADM)** > **VMware View Agent Configuration** > **Persona Management**
Windows XP or Windows Server 2003	**Computer Configuration** > **Administrative Templates** > **VMware View Agent Configuration** > **Persona Management**

The group policy settings are contained in these folders:

- Roaming & Synchronization
- Folder Redirection
- Desktop UI
- Logging

Roaming and Synchronization Group Policy Settings

The roaming and synchronization group policy settings turn View Persona Management on and off, set the location of the remote profile repository, determine which folders and files belong to the user profile, and control how to synchronize folders and files.

Group Policy Setting	Description
Manage user persona	Determines whether to manage user profiles dynamically with View Persona Management or with Windows roaming profiles. This setting turns View Persona Management on and off. When this setting is enabled, View Persona Management manages user profiles. When the setting is enabled, you can specify a profile upload interval in minutes. This value determines how often changes in the user profile are copied to the remote repository. The default value is 10 minutes. When this setting is disabled or not configured, user profiles are managed by Windows.
Persona repository location	Specifies the location of the user profile repository. This setting also determines whether to use a network share that is specified in View Persona Management or a path that is configured in Active Directory to support Windows roaming profiles. When this setting is enabled, you can use the **Share path** to determine the location of the user profile repository. In the **Share path** text box, you specify a UNC path to a network share that is accessible to View Persona Management desktops. This setting lets View Persona Management control the location of the user profile repository. For example: `\\server.domain.com\VPRepository` If `%username%` is not part of the folder path that you configure, View Persona Management appends `%username%.%userdomain%` to the path. For example: `\\server.domain.com\VPRepository\%username%.%userdomain%` If you specify a location in the **Share path**, you do not have to set up roaming profiles in Windows or configure a user profile path in Active Directory to support Windows roaming profiles. For details about configuring a UNC network share for View Persona Management, see "Configure a User Profile Repository," on page 177. By default, the Active Directory user profile path is used. Specifically, when the **Share path** is left blank, the Active Directory user profile path is used. The **Share path** is blank and inactive when this setting is disabled or not configured. You can also leave the path blank when this setting is enabled. When this setting is enabled, you can select the **Override Active Directory user profile path if it is configured** check box to make sure that View Persona Management uses the path specified in the **Share path**. By default, this check box is unchecked, and View Persona Management uses the Active Directory user profile path when both locations are configured.
Remove local persona at log off	Deletes each user's locally stored profile from the desktop system when the user logs off. You can also check a box to delete each user's local settings folders when the user profile is removed. In Windows 7 and Windows Vista, checking this box removes the `AppData\Local` folder. In Windows XP, checking the box removes the `Local Settings` folder. For guidelines for using this setting, see "Best Practices for Configuring a View Persona Management Deployment," on page 183. When this setting is disabled or not configured, the locally stored user profiles, including local settings folders, are not deleted when users log off.
Roam local settings folders	Roams the local settings folders with the rest of each user profile. For Windows 7 or Windows Vista, this policy affects the `AppData\Local` folder. For Windows XP, this policy affects the `Local Settings` folder. By default, local settings are not roamed.

Group Policy Setting	Description
Files and folders to preload	Specifies a list of files and folders that are downloaded to the local user profile when the user logs in. Changes in the files are copied to the remote repository as they occur. In some situations, you might want to preload specific files and folders into the locally stored user profile. Use this setting to specify these files and folders. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname. For example: `Application Data\Microsoft\Certificates` After the specified files and folders are preloaded, View Persona Management manages the files and folders in the same way that it manages other profile data. When a user updates preloaded files or folders, View Persona Management copies the updated data to the remote profile repository during the session, at the next profile upload interval.
Files and folders to preload (exceptions)	Prevents the specified files and folders from being preloaded. The selected folder paths must reside within the folders that you specify in the **Files and folders to preload** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Windows roaming profiles synchronization	Specifies a list of files and folders that are managed by standard Windows roaming profiles. The files and folders are retrieved from the remote repository when the user logs in. The files are not copied to the remote repository until the user logs off. For the specified files and folders, View Persona Management ignores the profile replication interval that is configured by the **Profile upload interval** in the **Manage user persona** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Windows roaming profiles synchronization (exceptions)	The selected files and folders are exceptions to the paths that are specified in the **Windows roaming profiles synchronization** setting. The selected folder paths must reside within the folders that you specify in the **Windows roaming profiles synchronization** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Files and folders excluded from roaming	Specifies a list of files and folders that are not roamed with the rest of the user profile. The specified files and folders exist only on the local system. Some situations require specific files and folders to reside only in the locally stored user profile. For example, you can exclude temporary and cached files from roaming. These files do not need to be replicated to the remote repository. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname. By default, the user profile's temp folder, ThinApp cache folder, and cache folders for Internet Explorer, Firefox, Chrome, and Opera are excluded from roaming.
Files and folders excluded from roaming (exceptions)	The selected files and folders are exceptions to the paths that are specified in the **Files and folders excluded from roaming** setting. The selected folder paths must reside within the folders that you specify in the **Files and folders excluded from roaming** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Folders to background download	The selected folders are downloaded in the background after a user logs in to the desktop. In certain cases, you can optimize View Persona Management by downloading the contents of specific folders in the background. With this setting, users do not have to wait for large files to download when they start an application. Also, users do not have to wait for the files to preload when they log in, as they might if you use the **Files and folders to preload** setting with very large files. For example, you can include VMware ThinApp sandbox folders in the **Folders to background download** setting. The background download does not affect performance when a user logs in or uses other applications on the desktop. When the user starts the ThinApp application, the required ThinApp sandbox files are likely to be downloaded from the remote repository, improving the application startup time. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.
Folders to background download (exceptions)	The selected folders are exceptions to the paths that are specified in the **Folders to background download** setting. The selected folder paths must reside within the folders that you specify in the **Folders to background download** setting. Specify paths that are relative to the root of the local profile. Do not specify a drive in a pathname.

Folder Redirection Group Policy Settings

With folder redirection group policy settings, you can redirect user profile folders to a network share. When a folder is redirected, all data is stored directly on the network share during the user session.

You can use these settings to redirect folders that must be highly available. View Persona Management copies updates from the local user profile to the remote profile as often as once a minute, depending on the value you set for the profile upload interval. However, if a network outage or failure on the local system occurs, a user's updates since the last replication might not be saved in the remote profile. In situations where users cannot afford a temporary loss of a few minutes of recent work, you can redirect those folders that store this critical data.

The following rules and guidelines apply to folder redirection:

- When you enable this setting for a folder, you must type the UNC path of the network share to which the folder is redirected.
- If `%username%` is not part of the folder path that you configure, View Persona Management appends `%username%` to the UNC path.
- As a best practice, configure the folder path to include `%username%`, but make sure that the last subfolder in the path uses the name of the redirected folder, such as `My Videos`. The last folder in the path is displayed as the folder name on the user's desktop. For details, see "Configuring Paths for Redirected Folders," on page 183.
- You configure a separate setting for each folder. You can select particular folders for redirection and leave others on the local View desktop. You can also redirect different folders to different UNC paths.
- If a folder redirection setting is disabled or not configured, the folder is stored on the local View desktop and managed according to the View Persona Management group policy settings.
- If View Persona Management and Windows roaming profiles are configured to redirect the same folder, View Persona Management's folder redirection takes precedence over Windows roaming profiles.
- Folder redirection applies only to applications that use the Windows shell APIs to redirect common folder paths. For example, if an application writes a file to `%USERPROFILE%\AppData\Roaming`, the file is written to the local profile and not redirected to the network location.

You can redirect the following folders to a network share:

- Application Data (roaming)
- Contacts
- Cookies
- Desktop
- Downloads
- Favorites
- History
- Links
- My Documents
- My Music
- My Pictures
- My Videos
- Network Neighborhood

- Printer Neighborhood
- Recent Items
- Save Games
- Searches
- Start Menu
- Startup Items
- Templates
- Temporary Internet Files

Certain folders are available only in Windows Vista and later operating systems.

Desktop UI Group Policy Settings

The desktop UI group policy settings control View Persona Management settings that users see on their desktops.

Group Policy Setting	Description
Hide local offline file icon	Determines whether to hide the offline icon when a user views locally stored files that belong to the user profile. Enabling this setting hides the offline icon in Windows Explorer and most Windows dialog boxes. By default, the offline icon is hidden.
Show progress when downloading large files	Determines whether to display a progress window on a user's desktop when the client retrieves large files from the remote repository. When this setting is enabled, you can specify the minimum file size, in megabytes, to begin displaying the progress window. The window is displayed when View Persona Management determines that the specified amount of data will be retrieved from the remote repository. This value is an aggregate of all files that are retrieved at one time. For example, if the setting value is 50MB and a 40MB file is retrieved, the window is not displayed. If a 30MB file is retrieved while the first file is still being downloaded, the aggregate download exceeds the value and the progress window is displayed. The window appears when a file starts downloading. By default, this value is 50MB. By default, this progress window is not displayed.
Show critical errors to users via tray icon alerts	Displays critical error icon alerts in the desktop tray when replication or network connectivity failures occur. By default, these icon alerts are hidden.

Logging Group Policy Settings

The logging group policy settings determine the name, location, and behavior of the View Persona Management log files.

Group Policy Setting	Description
Logging filename	Specifies the full pathname of the local View Persona Management log file. On Windows 7 computers, the default path is `ProgramData\VMware\VDM\logs\`*`filename`*. On Windows XP computers, the default path is *`All Users`*`\Application Data\VMware\VDM\logs\`*`filename`*. The default logging filename is `VMWVvp.txt`.
Logging destination	Determines whether to write all log messages to the log file, the debug port, or both destinations. By default, logging messages are sent to the log file.

Group Policy Setting	Description
Logging flags	Determines the types of messages to log. When this setting is configured, you can select any or all log message types to generate: ■ Log error messages. ■ Log information messages. ■ Log debug messages. By default, error and information log message types are generated.
Debug flags	Determines the types of debug messages to log. View Persona Management handles debug messages in the same way that it handles log messages. When this setting is enabled, you can select any or all debug message types to generate: ■ Debug error messages ■ Debug information messages ■ Debug registry messages ■ Debug IRQL messages ■ Debug port messages ■ Debug process messages By default, no debug messages are generated.

Managing Linked-Clone Desktops 10

With View Composer, you can update linked-clone desktops, reduce the size of their operating system data, and rebalance the linked-clone virtual machines among disk drives. You also can manage the View Composer persistent disks associated with linked clones.

- Reduce Linked-Clone Size with Desktop Refresh on page 191

  A desktop refresh operation restores the operating system disk of each linked clone to its original state and size, reducing storage costs.

- Update Linked-Clone Desktops on page 193

  You can update linked-clone desktops by creating a new base image on the parent virtual machine and using the recompose feature to distribute the updated image to the linked clones.

- Rebalance Linked-Clone Desktops on page 197

  A desktop rebalance operation evenly redistributes linked-clone desktops among available datastores.

- Manage View Composer Persistent Disks on page 199

  You can detach a View Composer persistent disk from a linked-clone desktop and attach it to another linked clone. This feature lets you manage user information separately from linked-clone desktops.

Reduce Linked-Clone Size with Desktop Refresh

A desktop refresh operation restores the operating system disk of each linked clone to its original state and size, reducing storage costs.

If possible, schedule refresh operations during off-peak hours.

For guidelines, see "Desktop Refresh Operations," on page 192.

Prerequisites

- Decide when to schedule the refresh operation. By default, View Composer starts the operation immediately.

  You can schedule only one refresh operation at a time for a given set of linked clones. You can schedule multiple refresh operations if they affect different linked clones.

- Decide whether to force all users to log off as soon as the operation begins or wait for each user to log off before refreshing that user's desktop.

  If you force users to log off, View Manager notifies users before they are disconnected and allows them to close their applications and log off.

- If your deployment includes replicated View Connection Server instances, verify that all instances are the same version.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select the pool to refresh by double-clicking the pool ID in the left column.

3 Choose whether to refresh the whole pool or selected desktops.

Option	Action
To refresh all desktops in the pool	On the selected pool's page, click the **Settings** tab.
To refresh selected desktops	a On the selected pool's page, click the **Inventory** tab. b Select the desktops to refresh.

4 Click **View Composer > Refresh**.

5 Follow the wizard instructions to refresh the linked-clone desktops.

The OS disks are reduced to their original size.

In vCenter Server, you can monitor the progress of the refresh operation on the linked-clone virtual machines.

In View Administrator, you can monitor the operation by clicking **Inventory > Pools**, selecting the pool ID, and clicking the **Tasks** tab. You can click **Cancel Task**, **Pause Task**, or**Resume Task** to terminate a task, suspend a task, or resume a suspended task.

Desktop Refresh Operations

As users interact with linked-clone desktops, the clones' OS disks grow. A desktop refresh operation restores the OS disks to their original state and size, reducing storage costs.

A refresh operation does not affect View Composer persistent disks.

A linked clone uses less storage space than the parent virtual machine, which contains the complete OS data. However, a clone's OS disk expands each time data is written to it from within the guest operating system.

When View Composer creates a linked clone, it takes a snapshot of the clone's OS disk. The snapshot uniquely identifies the linked-clone virtual machine. A refresh operation reverts the OS disk to the snapshot.

View Composer can refresh a linked clone in as little as half the time it takes to delete and recreate the clone.

Apply these guidelines to refresh operations:

- You can refresh a desktop pool on demand, as a scheduled event, or when the OS data reaches a specified size.

  You can schedule only one refresh operation at a time for a given set of linked clones. If you start a refresh operation immediately, the operation overwrites any previously scheduled task.

  You can schedule multiple refresh operations if they affect different linked clones.

  Before you schedule a new refresh operation, you must cancel any previously scheduled task.
- You can refresh dedicated-assignment and floating-assignment pools.
- You cannot refresh desktops that are running local sessions.
- A refresh can only occur when users are disconnected from their View desktops.
- A refresh preserves the unique computer information set up by QuickPrep or Sysprep. You do not need to rerun Sysprep after a refresh to restore the SID or the GUIDs of third-party software installed in the system drive.

- After you recompose a linked clone, View Manager takes a new snapshot of the linked clone's OS disk. Future refresh operations restore the OS data to that snapshot, not the one originally taken when the linked clone was first created.

NOTE You can slow the growth of linked clones by redirecting their paging files and system temp files to a temporary disk. When a linked clone is powered off, View Manager replaces the temporary disk with a copy of the original temporary disk that View Composer created with the linked-clone pool. This operation shrinks the temporary disk to its original size.

You can configure this option when you create a linked-clone pool.

Update Linked-Clone Desktops

You can update linked-clone desktops by creating a new base image on the parent virtual machine and using the recompose feature to distribute the updated image to the linked clones.

- Prepare a Parent Virtual Machine to Recompose Linked-Clone Desktops on page 193

  Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones.

- Recompose Linked-Clone Desktops on page 194

  Desktop recomposition simultaneously updates all the linked-clone desktops anchored to a parent virtual machine.

- Recompose Linked-Clone Desktops That Can Run in Local Mode on page 195

  You can recompose linked-clone desktops that can run in local mode. However, the desktops must be checked in or rolled back to the datacenter before the recompose operation can take place.

- Updating Linked Clones with Desktop Recomposition on page 196

  In a desktop recomposition, you can provide operating system patches, install or update applications, or modify the desktop hardware settings in all the linked clones in a desktop pool.

- Correcting an Unsuccessful Recomposition on page 197

  You can correct a recomposition that failed. You can also take action if you accidentally recompose linked clones using a different base image than the one you intended to use.

Prepare a Parent Virtual Machine to Recompose Linked-Clone Desktops

Before you recompose a linked-clone desktop pool, you must update the parent virtual machine that you used as a base image for the linked clones.

View Composer does not support recomposing linked clones that use one operating system to a parent virtual machine that uses a different operating system. For example, you cannot use a snapshot of a Windows 7 or Windows Vista parent virtual machine to recompose a Windows XP linked clone.

Procedure

1 In vCenter Server, update the parent virtual machine for the recomposition.

   - Install OS patches or service packs, new applications, application updates, or make other changes in the parent virtual machine.
   - Alternatively, prepare another virtual machine to be selected as the new parent during the recomposition.

2 In vCenter Server, power off the updated or new parent virtual machine.

3 In vCenter Server, take a snapshot of the parent virtual machine.

What to do next

Recompose the linked-clone desktop pool.

Recompose Linked-Clone Desktops

Desktop recomposition simultaneously updates all the linked-clone desktops anchored to a parent virtual machine.

If possible, schedule recompositions during off-peak hours.

Prerequisites

- Verify that you have a snapshot of the parent virtual machine. See "Prepare a Parent Virtual Machine to Recompose Linked-Clone Desktops," on page 193.
- Familiarize yourself with the recomposition guidelines. See "Updating Linked Clones with Desktop Recomposition," on page 196.
- Decide when to schedule the recomposition. By default, View Composer starts the recomposition immediately.

  You can schedule only one recomposition at a time for a given set of linked clones. You can schedule multiple recompositions if they affect different linked clones.
- Decide whether to force all users to log off as soon as the recomposition begins or wait for each user to log off before recomposing that user's desktop.

  If you force users to log off, View Manager notifies users before they are disconnected and allows them to close their applications and log off.
- Decide whether to stop provisioning at first error. If you select this option and an error occurs when View Composer provisions a linked clone, provisioning stops for all clones in the pool. You can select this option to ensure that resources such as storage are not consumed unnecessarily.

  Selecting the **Stop at first error** option does not affect customization. If a customization error occurs on a linked clone, other clones continue to be provisioned and customized.
- Verify that provisioning for the pool is enabled. When pool provisioning is disabled, View Manager stops the desktops from being customized after they are recomposed.
- If your deployment includes replicated View Connection Server instances, verify that all instances are the same version.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select the pool to recompose by double-clicking the pool ID in the left column.

3 Choose whether to recompose the whole pool or selected desktops.

Option	Action
To recompose all desktops in the pool	On the selected pool's page, click the **Settings** tab.
To recompose selected desktops	a On the selected pool's page, click the **Inventory** tab. b Select the desktops to recompose.

4 Click **View Composer > Recompose**.

5 Follow the wizard instructions to recompose the linked-clone desktops.

If you recompose the whole pool from the **Settings** tab, you can check the **Change the default image for new desktops** box. With this setting, new desktops that are created in the pool use the updated base image. This setting is checked by default.

On the Ready to Complete page, you can click **Show Details** to display the linked-clone desktops that will be recomposed.

The linked-clone desktops are refreshed and updated. The OS disks are reduced to their original size.

In a dedicated-assignment pool, unassigned linked clones are deleted and recreated. The specified number of spare desktops is maintained.

In a floating-assignment pool, all selected linked clones are recomposed.

In vCenter Server, you can monitor the progress of the recomposition on the linked-clone virtual machines.

In View Administrator, you can monitor the operation by clicking **Inventory > Pools**, selecting the pool ID, and clicking the **Tasks** tab. You can click **Cancel Task**, **Pause Task**, or**Resume Task** to terminate a task, suspend a task, or resume a suspended task.

NOTE If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 86.

Recompose Linked-Clone Desktops That Can Run in Local Mode

You can recompose linked-clone desktops that can run in local mode. However, the desktops must be checked in or rolled back to the datacenter before the recompose operation can take place.

Prerequisites

- Familiarize yourself with the recomposition guidelines. See "Updating Linked Clones with Desktop Recomposition," on page 196.
- Familiarize yourself with the procedure for updating the base image and recomposing linked-clone desktops. See "Prepare a Parent Virtual Machine to Recompose Linked-Clone Desktops," on page 193 and "Recompose Linked-Clone Desktops," on page 194.
- Familiarize yourself with the procedure for publishing base images to the Transfer Server repository. See "Publish Package Files in the Transfer Server Repository," on page 254.

Procedure

1 Check in or roll back the local, linked-clone desktops that were created from the base image.

2 Initiate the recompose operation.

The recompose operation ignores desktops that are in local mode.

3 Publish the recomposed base image to the Transfer Server repository.

The linked-clone desktops are updated with the new base image.

The next time users check out their linked-clone desktops, View Transfer Server downloads the updated base image from the Transfer Server repository to the client computers. View Transfer Server also downloads the linked-clones' OS disks and View Composer persistent disks to the client computers.

NOTE Desktops that were in local mode during the recompose operation continue to use the old base image. These desktops are not recomposed when users check them in.

Updating Linked Clones with Desktop Recomposition

In a desktop recomposition, you can provide operating system patches, install or update applications, or modify the desktop hardware settings in all the linked clones in a desktop pool.

To recompose linked-clone desktops, you update the parent virtual machine in vCenter Server or select a different virtual machine to become the new parent. Next, you take a snapshot of the new parent virtual machine configuration.

You can change the parent virtual machine without affecting the linked clones because they are linked to the replica, not directly to the parent.

You then initiate the recomposition, selecting the snapshot to be used as the new base image for the desktop pool. View Composer creates a new replica, copies the reconfigured OS disk to the linked clones, and anchors the linked clones to the new replica.

The recomposition also refreshes the linked clones, reducing the size of their OS disks.

Desktop recompositions do not affect View Composer persistent disks.

Apply these guidelines to recompositions:

- You can recompose dedicated-assignment and floating-assignment pools.
- You can recompose a desktop pool on demand or as a scheduled event.

  You can schedule only one recomposition at a time for a given set of linked clones. Before you can schedule a new recomposition, you must cancel any previously scheduled task or wait until the previous operation is completed. Before you can start a new recomposition immediately, you must cancel any previously scheduled task.

  You can schedule multiple recompositions if they affect different linked clones.
- You can recompose selected linked clones or all linked clones in a desktop pool.
- When different linked clones in a pool are derived from different snapshots of the base image or from different base images, the pool includes more than one replica.
- You cannot recompose desktops that are running in local mode. Local desktops must be checked in or rolled back to the datacenter before a recompose operation can take place.
- A recomposition can only occur when users are logged off of their View desktops.
- You cannot recompose linked clones that use one operating system to a new or updated parent virtual machine that uses a different operating system.
- You cannot recompose Windows 7 linked clones that use one OS disk controller to a new or updated parent virtual machine that uses a different OS disk controller.
- You cannot recompose linked clones to a lower hardware version than their current version. For example, you cannot recompose hardware version 8 clones to a parent virtual machine that is hardware version 7.

NOTE If you used a Sysprep customization specification to customize the linked clones when you created the desktop pool, new SIDs might be generated for the recomposed virtual machines. For details, see "Recomposing Linked Clones Customized with Sysprep," on page 86.

Correcting an Unsuccessful Recomposition

You can correct a recomposition that failed. You can also take action if you accidentally recompose linked clones using a different base image than the one you intended to use.

Problem

The desktops are in an erroneous or outdated state as a result of an unsuccessful recomposition.

Cause

A system failure or problem might have occurred on the vCenter Server host, in vCenter Server, or on a datastore during the recomposition.

Alternatively, the recomposition might have used a virtual-machine snapshot with a different operating system than the operating system of the original parent virtual machine. For example, you might have used a Windows 7 snapshot to recompose Windows XP linked clones.

Solution

1 Select the snapshot that was used in the last successful recomposition.

You can also select a new snapshot to update the linked clones to a new state.

The snapshot must use the same operating system as the original parent virtual machine's snapshot.

2 Recompose the pool again.

View Composer creates a base image from the snapshot and recreates the linked-clone OS disks.

View Composer persistent disks that contain user data and settings are preserved during the recomposition.

Depending on the conditions of the incorrect recomposition, you might refresh or rebalance the linked clones instead of or in addition to recomposing them.

NOTE If you do not configure View Composer persistent disks, all recompositions delete user-generated changes in the linked-clone desktops.

Rebalance Linked-Clone Desktops

A desktop rebalance operation evenly redistributes linked-clone desktops among available datastores.

If possible, schedule rebalance operations during off-peak hours.

For guidelines, see "Rebalancing Linked Clones Among Logical Drives," on page 198.

Prerequisites

- Familiarize yourself with the rebalance operation. See "Rebalancing Linked Clones Among Logical Drives," on page 198.
- Decide when to schedule the rebalance operation. By default, View Composer starts the operation immediately.

  You can schedule only one rebalance operation at a time for a given set of linked clones. You can schedule multiple rebalance operations if they affect different linked clones.
- Decide whether to force all users to log off as soon as the operation begins or wait for each user to log off before rebalancing that user's desktop.

  If you force users to log off, View Manager notifies users before they are disconnected and allows them to close their applications and log off.

- Verify that provisioning for the pool is enabled. When pool provisioning is disabled, View Manager stops the desktops from being customized after they are rebalanced.
- If your deployment includes replicated View Connection Server instances, verify that all instances are the same version.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select the pool to rebalance by double-clicking the pool ID in the left column.

3 Choose whether to rebalance the whole pool or selected desktops.

Option	Action
To rebalance all desktops in the pool	On the selected pool's page, click the **Settings** tab.
To rebalance selected desktops	a On the selected pool's page, click the **Inventory** tab. b Select the desktops to rebalance.

4 Click **View Composer > Rebalance**.

5 Follow the wizard instructions to rebalance the linked-clone desktops.

The linked-clone desktops are refreshed and rebalanced. The OS disks are reduced to their original size.

In View Administrator, you can monitor the operation by clicking **Inventory > Pools**, selecting the pool ID, and clicking the **Tasks** tab. You can click **Cancel Task**, **Pause Task**, or**Resume Task** to terminate a task, suspend a task, or resume a suspended task.

Rebalancing Linked Clones Among Logical Drives

A desktop rebalance operation evenly redistributes linked-clone desktops among available logical drives. It saves storage space on overloaded drives and ensures that no drives are underused.

When you create large linked-clone desktop pools and use multiple Logical Unit Numbers (LUNs), the space might not be used efficiently if the initial sizing was inaccurate. If you set an aggressive storage overcommit level, the linked clones can grow quickly and consume all the free space on the datastore.

When the virtual machines use 95% of the space on the datastore, View Manager generates a warning log entry. At 99% usage, vSphere suspends every virtual machine on the datastore.

The rebalance also refreshes the linked clones, reducing the size of their OS disks. It does not affect View Composer persistent disks.

Apply these guidelines to desktop rebalances:

- You can rebalance dedicated-assignment and floating-assignment pools.
- You can rebalance selected linked clones or all clones in a pool.
- You can rebalance a desktop pool on demand or as a scheduled event.

  You can schedule only one rebalance operation at a time for a given set of linked clones. If you start a rebalance operation immediately, the operation overwrites any previously scheduled task.

  You can schedule multiple rebalance operations if they affect different linked clones.

  Before you schedule a new rebalance operation, you must cancel any previously scheduled task.
- You can only rebalance desktops in the Available, Error, or Customizing state with no schedules or pending cancellations.
- As a best practice, do not mix linked-clone virtual machines with other types of virtual machines on the same datastore. This way View Composer can rebalance all the virtual machines on the datastore.

- If you edit a pool and change the host or cluster and the datastores on which linked clones are stored, you can only rebalance the linked clones if the newly selected host or cluster has full access to both the original and the new datastores. All hosts in the new cluster must have access to the original and new datastores.

  For example, you might create a linked-clone pool on a standalone host and select a local datastore to store the clones. If you edit the pool and select a cluster and a shared datastore, a rebalance operation will fail because the hosts in the cluster cannot access the original, local datastore.

Filenames of Linked-Clone Disks After a Rebalance Operation

When you rebalance linked-clone desktops, vCenter Server changes the filenames of View Composer persistent disks and disposable-data disks in linked clones that are moved to a new datastore.

The original filenames identify the disk type. The renamed disks do not include the identifying labels.

An original persistent disk has a filename with a `user-disk` label: *`desktop_name`*`-vdm-user-disk-D-`*`ID`*`.vmdk`.

An original disposable-data disk has a filename with a `disposable` label: *`desktop_name`*`-vdm-disposable-`*`ID`*`.vmdk`.

After a rebalance operation moves a linked clone to a new datastore, vCenter Server uses a common filename syntax for both types of disks: *`desktop_name_n`*`.vmdk`.

Manage View Composer Persistent Disks

You can detach a View Composer persistent disk from a linked-clone desktop and attach it to another linked clone. This feature lets you manage user information separately from linked-clone desktops.

View Composer Persistent Disks

With View Composer, you can configure OS data and user information on separate disks in linked-clone desktops. View Composer preserves the user information on the persistent disk when the OS data is updated, refreshed, or rebalanced.

A View Composer persistent disk contains user settings and other user-generated data. You create persistent disks when you create a linked-clone desktop pool. See "Worksheet for Creating a Linked-Clone Desktop Pool," on page 75.

You can detach a persistent disk from its linked-clone desktop and store the disk on its original datastore or another datastore. After you detach the disk, the linked-clone virtual machine is deleted. A detached persistent disk is no longer associated with any desktop.

You can use several methods to attach a detached persistent disk to another linked-clone desktop. This flexibility has several uses:

- When a linked clone is deleted, you can preserve the user data.
- When an employee leaves the company, another employee can access the departing employee's user data.
- A user who has multiple desktops can consolidate the user data on a single desktop.
- If a virtual machine becomes inaccessible in vCenter Server, but the persistent disk is intact, you can import the persistent disk and create a new linked clone using the disk.

NOTE You cannot detach a persistent disk from a Windows XP linked clone and recreate or attach the persistent disk to a Windows 7 or Windows Vista linked clone. Persistent disks must be reconnected to the operating system that was used when they were created.

View Manager can manage persistent disks from linked-clone pools that were created in View Manager 4.5 or later. Persistent disks that were created in earlier versions of View Manager cannot be managed and do not appear on the Persistent Disks page in View Administrator.

Detach a View Composer Persistent Disk

When you detach a View Composer persistent disk from a linked-clone desktop, the disk is stored and the linked clone is deleted. By detaching a persistent disk, you can store and reuse user-specific information with another desktop.

Procedure

1 In View Administrator, click **Inventory > Persistent disks**.

2 Select the persistent disk to detach.

3 Click **Detach**.

4 Choose where to store the persistent disk.

Option	Description
Use current datastore	Store the persistent disk on the datastore where it is currently located.
Move to the following datastore	Select a new datastore on which to store the persistent disk. Click **Browse**, click the down arrow, and select a new datastore from the **Choose a Datastore** menu.

The View Composer persistent disk is saved on the datastore. The linked-clone desktop is deleted and does not appear in View Administrator.

Attach a View Composer Persistent Disk to Another Linked-Clone Desktop

You can attach a detached persistent disk to another linked-clone desktop. Attaching a persistent disk makes the user settings and information in the disk available to the user of the other desktop.

You attach a detached persistent disk as a secondary disk on the selected linked-clone desktop. The new desktop user has access to the secondary disk and to the existing user information and settings on the desktop.

Prerequisites

Verify that the selected desktop uses the same operating system as the linked clone in which the persistent disk was created.

Procedure

1 In View Administrator, click **Inventory > Persistent disks**.

2 Click the **Detached** tab.

3 Select the persistent disk.

4 Click **Attach**.

5 Select a linked-clone desktop to which to attach the persistent disk.

6 Select **Attach as a secondary disk**.

7 Click **Finish**.

What to do next

Make sure that the user of the linked-clone desktop has sufficient privileges to use the attached secondary disk. For example, if the original user had certain access permissions on the persistent disk, and the persistent disk is attached as drive `D` on the new desktop, the new desktop user must have the original user's access permissions on drive `D`.

Log in to the desktop's guest operating system as an administrator and assign appropriate privileges to the new desktop user.

Edit a View Composer Persistent Disk's Pool or User

You can assign a detached View Composer persistent disk to a new pool or user if the original pool or user was deleted from View Manager.

A detached persistent disk is still associated with its original pool and user. If the pool or user is deleted from View Manager, you cannot use the persistent disk to recreate a linked-clone desktop.

By editing the pool and user, you can use the detached persistent disk to recreate a desktop in the new pool. The desktop is assigned to the new user.

You can select a new pool, a new user, or both.

Prerequisites

- Verify that the persistent disk's pool or user was deleted from View Manager.
- Verify that the new pool uses the same operating system as the pool in which persistent disk was created.

Procedure

1 In View Administrator, click **Inventory > Persistent Disks**

2 Select the persistent disk for which the user or pool has been deleted.

3 Click **Edit**.

4 (Optional) Select a linked-clone pool from the list.

5 (Optional) Select a user for the persistent disk.

You can browse your Active Directory for the domain and username.

What to do next

Recreate a linked-clone desktop with the detached persistent disk.

Recreate a Linked-Clone Desktop With a Detached Persistent Disk

When you detach a View Composer persistent disk, the linked clone is deleted. You can give the original user access to the detached user settings and information by recreating the linked-clone desktop from the detached disk.

NOTE If you recreate a linked-clone desktop in a pool that has reached its maximum size, the recreated desktop is still added to the pool. The pool grows larger than the specified maximum size.

If a persistent disk's original pool or user was deleted from View Manager, you can assign a new one to the persistent disk. See "Edit a View Composer Persistent Disk's Pool or User," on page 201.

Procedure

1 In View Administrator, click **Inventory > Persistent Disks**.

2 Click the **Detached** tab.

3 Select the persistent disk.

You can select multiple persistent disks to recreate a linked-clone desktop for each disk.

4 Click **Recreate Desktop**.

5 Click **OK**.

View Manager creates a linked-clone desktop for each persistent disk you select and adds the desktop to the original pool.

The persistent disks remain on the datastore where they were stored.

Restore a Linked-Clone Desktop by Importing a Persistent Disk from vSphere

If a linked-clone desktop becomes inaccessible in View Manager, you can restore the desktop if it was configured with a View Composer persistent disk. You can import the persistent disk from a vSphere datastore into View Manager.

You import the persistent disk file as a detached persistent disk in View Manager. You can either attach the detached disk to an existing desktop or recreate the original linked clone in View Manager.

Procedure

1 In View Administrator, click **Inventory > Persistent Disks**.

2 Click the **Detached** tab.

3 Click **Import from vCenter**.

4 Select a vCenter Server.

5 Select the datacenter where the disk file is located.

6 Select a linked-clone pool in which to create a new linked clone desktop with the persistent disk.

7 In the **Persistent Disk File** box, click **Browse**, click the down arrow, and select a datastore from the **Choose a Datastore** menu.

8 Click the datastore name to display its disk storage files and virtual-machine files.

9 Select the persistent-disk file you want to import.

10 In the **User** box, click **Browse**, select a user to assign to the desktop, and click **OK**.

The disk file is imported into View Manager as a detached persistent disk.

What to do next

To restore the linked-clone desktop, you can recreate the original desktop or attach the detached persistent disk to another desktop.

For details, see "Recreate a Linked-Clone Desktop With a Detached Persistent Disk," on page 201 and "Attach a View Composer Persistent Disk to Another Linked-Clone Desktop," on page 200.

Delete a Detached View Composer Persistent Disk

When you delete a detached persistent disk, you can remove the disk from View Manager and leave it on the datastore or delete the disk from View Manager and the datastore.

Procedure

1 In View Administrator, click **Inventory > Persistent Disks**.

2 Click the **Detached** tab.

3 Select the persistent disk.

4 Click **Delete**.

5 Choose whether to delete the disk from the datastore or let it remain on the datastore after it is removed from View Manager.

Option	Description
Delete from disk	After the deletion, the persistent disk no longer exists.
Delete from View Manager only	After the deletion, the persistent disk is no longer accessible in View Manager but remains on the datastore.

6 Click **OK**.

Managing Desktops and Desktop Pools

11

In View Administrator, you can manage desktop pools, virtual-machine desktops, and desktop sessions.

This chapter includes the following topics:

Managing Desktop Pools

You can edit, disable, and delete desktop pools in View Administrator.

Edit a Desktop Pool

You can edit an existing desktop pool to configure settings such as pool settings, number of spare desktops, datastores, and customization specifications.

Prerequisites

Familiarize yourself with the pool settings that you can and cannot change after a pool is created. See "Modifying Settings in an Existing Desktop Pool," on page 206 and "Fixed Settings in an Existing Desktop Pool," on page 206.

Procedure

1 Click **Inventory > Pools**.

2 Select a pool.

3 Click **Edit**.

4 Click a tab in the **Edit***pool_name* dialog and reconfigure pool options.

5 Click **OK**.

Modifying Settings in an Existing Desktop Pool

After you create a desktop pool, you can change certain configuration settings.

Table 11-1. Editable Settings in an Existing Desktop Pool

Configuration Tab	Description
General	Edit pool-naming options.
Pool Settings	Edit desktop settings such as the remote desktop power policy, display protocol, and Adobe Flash settings.
Provisioning Settings	Edit pool-provisioning options and add desktops to the pool. This tab is available for automated pools only.
vCenter Settings	Edit the virtual machine template or default base image. Add or change the vCenter Server instance, ESX host or cluster, datastores, and other vCenter features. The new values only affect new virtual machines that are created after the settings are changed. The new settings do not affect existing virtual machines. This tab is available for automated pools only.
Guest Customization	Select Sysprep customization specifications. If QuickPrep was used to customize a linked-clone pool, you can change the Active Directory domain and container and specify QuickPrep power-off and post-synchronization scripts This tab is available for automated pools only.

Fixed Settings in an Existing Desktop Pool

After you create a desktop pool, you cannot change certain configuration settings.

Table 11-2. Fixed Settings in an Existing Desktop Pool

Setting	Description
Pool type	After you create an automated, manual, or Terminal Services pool, you cannot change the pool type.
User assignment	You cannot switch between dedicated assignments and floating assignments.
Type of virtual machine	You cannot switch between full desktops and linked-clone desktops.
Pool ID	You cannot change the pool ID.
Desktop-naming and provisioning method	To add desktops to a pool, you must use the provisioning method that was used to create the pool. You cannot switch between specifying desktop names manually and using a naming pattern. If you specify names manually, you can add names to the list of desktop names. If you use a naming pattern, you can increase the maximum number of desktops.
vCenter settings	You cannot change vCenter settings for existing virtual machines. You can change vCenter settings in the **Edit***pool_name* dialog, but the values only affect new virtual machines that are created after the settings are changed.
View Composer persistent disks	You cannot configure persistent disks after a linked-clone pool is created without persistent disks.
View Composer customization method	After you customize a linked-clone pool with QuickPrep or Sysprep, you cannot switch to the other customization method when you create or recompose desktops in the pool.

Change the Size of an Automated Pool Provisioned by a Naming Pattern

When you provision an automated desktop pool by using a naming pattern, you can increase or decrease the size of the pool by changing the maximum number of desktops.

Prerequisites

- Verify that you provisioned the pool by using a naming pattern. If you specify desktop names manually, see "Add Desktops to an Automated Pool Provisioned by a List of Names," on page 207.
- Verify that the pool is automated.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select the pool and click **Edit**.

3 Click the **Provisioning Settings** tab.

4 In the **Max number of desktops** box, type the new number of desktops in the pool.

If you increase the pool size, new desktops can be added to the pool up to the maximum number.

If you decrease the size of a floating-assignment pool, unused desktops are deleted. If more users are logged into the pool than the new maximum, the pool size decreases after users log off.

If you decrease the size of a dedicated-assignment pool, unassigned desktops are deleted. If more users are assigned to desktops than the new maximum, the pool size decreases after you unassign users.

NOTE When you decrease the size of a pool, the actual number of desktops might be larger than **Max number of desktops** if more users are currently logged in or assigned to desktops than the maximum number.

Add Desktops to an Automated Pool Provisioned by a List of Names

To add desktops to an automated pool provisioned by manually specifying desktop names, you provide another list of new desktop names. This feature lets you expand a desktop pool and continue to use your company's naming conventions.

Follow these guidelines for manually adding desktop names:

- Type each desktop name on a separate line.
- A desktop name can have up to 15 alphanumeric characters.
- You can add a user name to each desktop entry. Use a comma to separate the user name from the desktop name.

In this example, two desktops are added. The second desktop is associated with a user:

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

NOTE In a floating-assignment pool, you cannot associate user names with desktop names. The desktops are not dedicated to the associated users. In a floating-assignment pool, all desktops that are not currently in use remain accessible to any user who logs in.

Prerequisites

Verify that you created the pool by manually specifying desktop names. You cannot add desktops by providing new desktop names if you created the pool by providing a naming pattern.

Procedure

1 Create a text file that contains the list of additional desktop names.

If you intend to add only a few desktops, you can type the desktop names directly in the Add Pool wizard. You do not have to create a separate text file.

2 In View Administrator, click **Inventory > Pools**.

3 Select the pool to be expanded.

4 Click **Edit**.

5 Click the **Provisioning Settings** tab.

6 Click **Add Desktops**.

7 Copy your list of desktop names in the Enter Desktop Names page and click **Next**.

The Enter Desktop Names wizard displays the desktop list and indicates validation errors with a red **X**.

8 Correct invalid desktop names.

a Place your cursor over an invalid name to display the related error message at the bottom of the page.

b Click **Back**.

c Edit the incorrect names and click **Next**.

9 Click **Finish**.

10 Click **OK**.

View Manager adds the new desktops to the pool.

In vCenter Server, you can monitor the creation of the new virtual machines.

In View Administrator, you can view the desktops as they are added to the pool by clicking **Inventory > Pools** or **Inventory > Desktops**.

Disable or Enable a Desktop Pool

When you disable a desktop pool, the pool is no longer presented to users and pool provisioning is stopped. Users have no access to the pool. After you disable a pool, you can enable it again.

You can disable a pool to prevent users from accessing their desktops while you prepare the desktops for use. If a pool is no longer needed, you can use the disable feature to withdraw the pool from active use without having to delete the pool definition from View Manager.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select a desktop pool and change the status of the pool.

Option	Action
Disable the pool	Click **Status > Disable Pool**.
Enable the pool	Click **Status > Enable Pool**.

3 Click **OK**.

Disable or Enable Provisioning in a Desktop Pool

When you disable provisioning in a desktop pool, View Manager stops provisioning new virtual machines for the pool. After you disable provisioning, you can enable provisioning again.

Before you change a pool's configuration, you can disable provisioning to ensure that no new desktops are created with the old configuration. You also can disable provisioning to prevent View Manager from using additional storage when a pool is close to filling up the available space.

When provisioning is disabled in a linked-clone pool, View Manager stops new desktops from being provisioned and stops desktops from being customized after they are recomposed or rebalanced.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select a desktop pool and change the status of the pool.

Option	Action
Disable provisioning	Click **Status > Disable Provisioning**.
Enable provisioning	Click **Status > Enable Provisioning**.

3 Click **OK**.

Delete a Desktop Pool from View Manager

When you delete a desktop pool from View Manager, users can no longer access the desktops in the pool.

Users in currently active sessions can continue to use full virtual-machine desktops if you keep the virtual machines in vCenter Server. After the users log off, they cannot access the deleted desktops.

With linked-clone desktops, vCenter Server always deletes the virtual machines from disk.

IMPORTANT Do not delete the virtual machines in vCenter Server before you delete a desktop pool with View Administrator. This action could put View components into an inconsistent state.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select a desktop pool and click **Delete**.

3 Choose how to delete the pool.

Option	Description
Pool that contains full virtual-machine desktops	Choose whether to keep or delete the virtual machines in vCenter Server. If you delete the virtual machines from disk, users in active sessions are disconnected from their desktops. If you keep the virtual machines in vCenter Server, choose whether to let users in active sessions stay connected to their desktops or disconnect them.
Linked-clone pool with View Composer persistent disks	Choose whether to detach or delete the persistent disks when the desktops are deleted. In both cases, vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops. If you detach a persistent disk, it can be attached to another desktop. You can store detached persistent disks in the same datastore or a different one.
Linked-clone pool without View Composer persistent disks	vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops.

The desktop pool is removed from View Connection Server. If you keep the virtual machines in vCenter Server, View Manager cannot access them.

When you delete a desktop pool from View Manager, linked-clone computer accounts are removed from Active Directory. Full virtual machine accounts remain in Active Directory. To remove these accounts, you must manually delete them from Active Directory.

When you delete a pool that contains local desktops, the datacenter copies of the desktops are removed from View Manager. The local desktops no longer function when the clients contact View Connection Server or the maximum time without server contact is exceeded. If you choose to keep full virtual machines in vCenter Server or detach and save View Composer persistent disks, changes that users made on their local desktops since the last replication or check-out are not preserved in the virtual machines or persistent disks.

Reducing Adobe Flash Bandwidth

You can reduce the amount of bandwidth used by Adobe Flash content that runs in View desktop sessions. This reduction can improve the overall browsing experience and make other applications that run in the desktop more responsive.

Configure Adobe Flash Quality and Throttling

You can set Adobe Flash quality and throttling modes to reduce the amount of bandwidth that is used by Adobe Flash content in View desktops.

Prerequisites

Familiarize yourself with Adobe Flash quality and throttling settings. See "Adobe Flash Quality and Throttling," on page 210.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select a pool and click **Edit**.

3 Click the **Pool Settings** tab.

4 Select a quality mode from the **Adobe Flash quality** menu.

5 Select a throttling mode from the **Adobe Flash throttling** menu.

6 Click **OK**.

NOTE Adobe Flash bandwidth-reduction settings do not take effect until View Client reconnects with the desktop.

Adobe Flash Quality and Throttling

You can specify a maximum allowable level of quality for Adobe Flash content that overrides Web page settings. If Adobe Flash quality for a Web page is higher than the maximum level allowed, quality is reduced to the specified maximum. Lower quality results in more bandwidth savings.

To make use of Adobe Flash bandwidth-reduction settings, Adobe Flash must not be running in full screen mode.

Table 11-3 shows the available Adobe Flash render-quality settings.

Table 11-3. Adobe Flash Quality Settings

Quality Setting	Description
Do not control	Quality is determined by Web page settings.
Low	This setting results in the most bandwidth savings.
Medium	This setting results in moderate bandwidth savings.
High	This setting results in the least bandwidth savings.

If no maximum level of quality is specified, the system defaults to a value of **Low**.

Adobe Flash uses timer services to update what is shown on the screen at a given time. A typical Adobe Flash timer interval value is between 4 and 50 milliseconds. By throttling, or prolonging, the interval, you can reduce the frame rate and thereby reduce bandwidth.

Table 11-4 shows the available Adobe Flash throttling settings.

Table 11-4. Adobe Flash Throttling Settings

Throttling Setting	Description
Disabled	No throttling is performed. The timer interval is not modified.
Conservative	Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.
Moderate	Timer interval is 500 milliseconds.
Aggressive	Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.

Audio speed remains constant regardless of which throttling setting you select.

Configure Adobe Flash Throttling with Internet Explorer in Terminal Services Sessions

To ensure that Adobe Flash throttling works with Internet Explorer in Terminal Services sessions, users must enable third-party browser extensions.

Procedure

1 Start View Client and log in to a user's desktop.

2 In Internet Explorer, click **Tools > Internet Options**.

3 Click the **Advanced** tab, select **Enable third-party browser extensions**, and click **OK**.

4 Restart Internet Explorer.

Override Bandwidth-Reduction Settings in the Desktop

By using the mouse cursor in the desktop, users can override Adobe Flash content display settings.

Procedure

1 On a View desktop, start Internet Explorer and browse to the relevant Adobe Flash content.

If necessary, start the content.

Depending on how Adobe Flash settings are configured, you might notice dropped frames or low playback quality.

2 Move the mouse cursor into the Adobe Flash content while it is playing.

Display quality is improved as long as the cursor remains inside the Adobe Flash content.

3 To retain the increase in quality, double-click inside the Adobe Flash content.

Managing Virtual-Machine Desktops

You can search for, manage, and delete virtual-machine desktops and manage desktop sessions.

View, Disconnect, or Restart Active Sessions

You can view the users actively connected to the View desktops in a pool. You can disconnect users from their desktops, force users to log off, and restart active sessions.

Procedure

1 In View Administrator, click **Inventory > Pool**.

2 Double-click a pool and click the **Sessions** tab.

3 Select a desktop.

4 Choose whether to disconnect, log off, or restart the session.

Option	Description
Disconnect Session	Disconnects the user from the desktop. The session remains active. The user can log back in to the session if **Automatically logoff after disconnect** is set to **Never**, or the specified length of time after the disconnect occurs is not exceeded. You can configure the **Automatically logoff after disconnect** setting when the pool is created or edit the setting after the pool is created.
Logoff Session	Disconnects the user from the desktop. The user is logged off.
Reset	Shuts down the desktop and restarts the session without a graceful logoff and disconnection.
Send Message	Lets you type a message that is displayed on the user's desktop.

Assign a Desktop to a User

In a dedicated-assignment pool, you can assign a user to be the owner of a desktop. Only the assigned user can log in and connect to the desktop.

View Manager assigns desktops to users in these situations.

- When you create a pool and select the **Enable automatic assignment** setting.

  NOTE If you select the **Enable automatic assignment** setting, you can still manually assign desktops to users.

- When you create an automated pool, select the **Specify desktop names manually** setting, and provide user names with the desktop names.

If you do not select either setting in a dedicated-assignment pool, users do not have access to desktops. You must manually assign a desktop to each user.

You can also use the `vdmadmin` command to assign desktops to users. See "Assigning Dedicated Desktops Using the -L Option," on page 330.

Prerequisites

- Verify that the desktop belongs to a dedicated-assignment pool. In View Administrator, the pool assignment appears in the Settings tab on the desktop pool's page.
- Verify that the desktop is not checked out for use in local mode. You cannot assign users or remove user assignments while desktops are checked out.

Procedure

1 In View Administrator, click **Inventory > Desktops**, or click **Inventory > Pools**, double-click a pool ID, and select the **Inventory** tab.

2 Select the desktop.

3 Click **More Commands > Assign User**.

4 Choose whether to find users or groups, select a domain, and type a search string in the **Name** or **Description** text box.

5 Select the user or group name and click **OK**.

Unassign a User from a Dedicated Desktop

In a dedicated-assignment pool, you can remove a desktop assignment to a user.

You can also use the `vdmadmin` command to remove a desktop assignment to a user. See "Assigning Dedicated Desktops Using the -L Option," on page 330.

Prerequisites

Verify that the desktop is not checked out for use in local mode. You cannot assign users or remove user assignments while desktops are checked out.

Procedure

1 In View Administrator, click **Inventory > Desktops** or click **Inventory > Pools**, double-click a pool ID, and select the **Inventory** tab.

2 Select the desktop.

3 Click **More Commands > Unassign User**.

4 Click **OK**.

The desktop is available and can be assigned to another user.

Customize Existing Desktops in Maintenance Mode

After a desktop pool is created, you can customize, modify, or test individual desktops by placing them in maintenance mode. When a desktop is in maintenance mode, users cannot access it.

You place existing desktops in maintenance mode one at a time. You can remove multiple desktops from maintenance mode in one operation.

When you create a pool, you can start all the desktops in the pool in maintenance mode if you specify desktop names manually. For details, see "Customizing Desktops in Maintenance Mode," on page 105.

Procedure

1 In View Administrator, click **Inventory > Desktops** or click **Inventory > Pools**, double-click a pool ID, and select the **Inventory** tab.

2 Select a desktop.

3 Click **More Commands > Enter Maintenance Mode**.

4 Customize, modify, or test the virtual-machine desktop.

5 Repeat Step 2 through Step 4 for all desktops you want to customize.

6 Select the customized desktops and click **More Commands > Exit Maintenance Mode**.

The modified desktops are available to users.

Monitor Desktop Status

You can quickly survey the status of desktops in your View deployment by using the View Administrator dashboard. For example, you can display all disconnected desktops or desktops that are in maintenance mode.

Prerequisites

Familiarize yourself with the desktop states. See "Desktop Status of Virtual Machines," on page 214.

Procedure

1 In View Administrator, click **Dashboard**.

2 In the Desktop Status pane, expand a status folder.

Option	Description
Preparing	Lists the desktop states while the virtual machine is being provisioned, deleted, or in maintenance mode.
Problem Desktops	Lists the desktop error states.
Prepared for use	Lists the desktop states when the desktop is ready for use.

3 Locate the desktop status and click the hyperlinked number next to it.

The **Desktops** page displays all desktops with the selected status.

What to do next

You can click a desktop name to see details about the desktop or click the View Administrator back arrow to return to the dashboard page.

Desktop Status of Virtual Machines

Virtual-machine desktops that are managed by vCenter Server can be in various states of operation and availability. In View Administrator, you can track the status of desktops in the right-hand column of the desktop-list page.

Table 11-5 shows the operational state of virtual-machine desktops that are displayed in View Administrator. A desktop can be in only one state at a time.

Table 11-5. Status of Virtual-Machine Desktops That Are Managed by vCenter Server

Status	Type of State	Description
Provisioning	Provisioning	The virtual machine is being provisioned.
Provisioning error	Provisioning	An error occurred during provisioning.
Customizing	Provisioning	The virtual machine in an automated pool is being customized.
Deleting	Provisioning	The virtual machine is marked for deletion. View Manager will delete the virtual machine soon.
Waiting for Agent	Agent state	View Connection Server is waiting to establish communication with View Agent on a virtual machine in a manual pool. NOTE This state is the same as the Customizing state for a virtual machine in an automated pool.
Startup	Agent state	View Agent has started on the virtual machine, but other required services such as the display protocol are still starting. For example, View Agent cannot establish an RDP connection with client computers until RDP has finished starting.
Agent unreachable	Agent state	View Connection Server cannot establish communication with View Agent on a virtual machine.

Table 11-5. Status of Virtual-Machine Desktops That Are Managed by vCenter Server (Continued)

Status	Type of State	Description
Configuration error	Agent state	The display protocol such as RDP or PCoIP is not enabled.
Provisioned	Availability	The virtual machine is powered off or suspended.
Available	Availability	The virtual machine is powered on and ready for an active connection. In a dedicated pool, the virtual machine is assigned to a user and will start when the user logs in.
Checked out	Session state	The virtual machine for a local desktop is checked out.
Connected	Session state	The virtual machine is in an active session and has an active remote connection to a View client.
Disconnected	Session state	The virtual machine is in an active session, but it is disconnected from the View client.
Unassigned user connected	Miscellaneous	A user other than the assigned user is logged in to a virtual machine in a dedicated pool. For example, this state can occur if an administrator starts vSphere Client, opens a console on the virtual machine, and logs in.
Unassigned user disconnected	Miscellaneous	A user other than the assigned user is logged in and disconnected from a virtual machine in a dedicated pool.
Unknown	Miscellaneous	The virtual machine is in an unknown state.
Maintenance mode	Miscellaneous	The virtual machine is in maintenance mode. Users cannot log in or use the virtual machine.
Error	Miscellaneous	An unknown error occurred in the virtual machine.
–	Miscellaneous	A failure occurred when the virtual machine was in any of the preceding states.

While a desktop is in a particular state, it can be subject to further conditions. View Administrator displays these conditions as suffixes to the desktop state. For example, View Administrator might display the `Customizing (missing)` state.

Table 11-6 shows these additional conditions.

Table 11-6. Desktop-Status Conditions

Condition	Description
Missing	The virtual machine is missing in vCenter Server. Typically, the virtual machine was deleted in vCenter Server, but the View LDAP configuration still has a record of the desktop.
Task halted	A View Composer operation such as refresh, recompose, or rebalance was stopped. For details about troubleshooting a recompose operation, see "Correcting an Unsuccessful Recomposition," on page 197. For details about View Composer error states, see "View Composer Provisioning Errors," on page 317. The `Task halted` condition applies to all virtual machines that were selected for the operation, but on which the operation has not yet started. Virtual machines in the pool that are not selected for the operation are not placed in the `Task halted` condition.

A desktop state can be subject to both conditions, `(missing, task halted)`, if a View Composer task was stopped and the virtual machine is missing in vCenter Server.

Delete Desktops from View Manager

When you delete desktops from View Manager, users can no longer access the desktops.

Users in currently active sessions can continue to use full virtual-machine desktops if you keep the virtual machines in vCenter Server. After the users log off, they cannot access the deleted desktops.

With linked-clone desktops, vCenter Server always deletes the virtual machines from disk.

NOTE Do not delete the virtual machines in vCenter Server before you delete desktops with View Administrator. This action could put View components into an inconsistent state.

Procedure

1 In View Administrator, click **Inventory > Desktops**.

2 Select one or more desktops and click **Remove**.

3 Choose how to delete the desktops.

Option	Description
Pool that contains full virtual-machine desktops	Choose whether to keep or delete the virtual machines in vCenter Server. If you delete the virtual machines from disk, users in active sessions are disconnected from their desktops. If you keep the virtual machines in vCenter Server, choose whether to let users in active sessions stay connected to their desktops or disconnect them.
Linked-clone pool with View Composer persistent disks	Choose whether to detach or delete the persistent disks when the desktops are deleted. In both cases, vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops. If you detach a persistent disk, it can be attached to another desktop. You can store detached persistent disks in the same datastore or a different one.
Linked-clone pool without View Composer persistent disks	vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops.

The desktops are removed from View Connection Server. If you keep the virtual machines in vCenter Server, View Manager cannot access them.

When you delete desktops from View Manager, linked-clone computer accounts are removed from Active Directory. Full virtual machine accounts remain in Active Directory. To remove these accounts, you must manually delete them from Active Directory.

When you delete local desktops, the datacenter copies of the desktops are removed from View Manager. The local desktops no longer function when the clients contact View Connection Server or the maximum time without server contact is exceeded. If you choose to keep full virtual machines in vCenter Server or detach and save View Composer persistent disks, changes that users made on their local desktops since the last replication or check-out are not preserved in the virtual machines or persistent disks.

Export View Information to External Files

In View Administrator, you can export View table information to external files. You can export the tables that list users and groups, pools, desktops, View Composer persistent disks, ThinApp applications, events, and VDI sessions. You can view and manage the information in a spreadsheet or another tool.

For example, you might collect information about desktops that are managed by more than one View Connection Server instance or group of replicated View Connection Server instances. You can export the **Desktops** table from each View Administrator interface and view it in a spreadsheet.

When you export a View Administrator table, it is saved as a comma-separated `cvs` file. This feature exports the entire table, not individual pages.

Procedure

1 In View Administrator, display the table you want to export.

For example, click **Inventory > Desktops** to display the desktops table.

2 Click the **Export** icon in the upper right corner of the table.

When you point your mouse at the icon, it displays the `Export table contents` tooltip.

3 Type a filename for the `csv` file in the Select location for download dialog.

The default filename is `global_table_data_export.csv`.

4 Browse to a location to store the file.

5 Click **Save**.

What to do next

Open a spreadsheet or another tool to view the `csv` file.

Managing Physical Computers and Terminal Servers

12

In View Administrator, you can add, remove, and unregister View desktops that are not managed by vCenter Server. Unmanaged desktop sources include virtual machines that are not managed by vCenter Server, physical computers, blade PCs, and Microsoft Terminal Services sources.

NOTE When you reconfigure a setting that affects an unmanaged desktop source, it can take up to 10 minutes for the new setting to take effect. For example, if you change the Message security mode in Global Settings or change the Automatically logoff after disconnect setting for a pool, View Manager might take up to 10 minutes to reconfigure the affected unmanaged desktop sources.

This chapter includes the following topics:

Add an Unmanaged Desktop Source to a Pool

You can increase the size of a manual desktop pool that uses unmanaged desktop sources by adding desktop sources to the pool.

Prerequisites

Verify that View Agent is installed on the unmanaged desktop source. See "Install View Agent on an Unmanaged Desktop Source," on page 41.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 In the left column of the Pools table, click the pool ID of the manual pool.

3 In the **Inventory** tab, click **Add**.

4 Select desktop sources from the Add Desktop Resources window and click **OK**.

View Manager adds the desktop source to the pool.

Remove an Unmanaged Desktop Source from a Pool

You can reduce the size of a manual desktop pool that uses unmanaged desktop sources by removing desktop sources from the pool.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Double-click a pool ID and select the **Inventory** tab.

3 Select the desktop sources to remove.

4 Click **Remove**.

5 If users are logged in to the unmanaged desktops, choose whether to terminate the sessions or let the sessions remain active.

Option	Description
Leave active	Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions.
Terminate	Active sessions end immediately.

6 Click **OK**.

View Manager removes the desktop sources from the pool.

Delete a Pool That Contains Unmanaged Desktops

When you delete a desktop pool that contains unmanaged desktop sources, the pool is removed from View Manager.

Procedure

1 In View Administrator, click **Inventory > Pools**.

2 Select an unmanaged desktop pool and click **Delete**.

3 If users are logged in to the unmanaged desktops, choose whether to terminate the sessions or let the sessions remain active.

Option	Description
Leave active	Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions.
Terminate	Active sessions end immediately.

4 Click **OK**.

The unmanaged desktop pool is removed from View Manager. View Manager does not delete the registration information for the unmanaged desktop sources that belong to the pool.

To remove the unmanaged desktop sources from View Manager, you must unregister them. See "Unregister an Unmanaged Desktop Source," on page 221.

Unregister an Unmanaged Desktop Source

All desktop sources that vCenter Server manages are registered when you install View Agent. You can unregister only unmanaged desktop sources.

Unmanaged desktop sources include virtual machines that are not managed by vCenter Server, physical computers, blade PCs, and Terminal Services sources.

When you unregister a desktop source, it becomes unavailable in View Manager. To make a source available again, reinstall View Agent in the desktop source.

Prerequisites

Verify that the desktop sources that you want to unregister are not being used in any desktop pools.

Procedure

1 Click **View Configuration > Registered desktop sources**.

2 Select the type of unmanaged desktop source and click **Details**.

3 Select the desktop source to unregister and click **Unregister**.

You can select only desktop sources that are not being used by a desktop pool.

4 Click **OK** to confirm that you want to unregister the desktop source.

The desktop source is unregistered and no longer available.

Desktop Status of Physical Computers and Terminal Servers

Desktop sources that are physical computers, terminal servers, or virtual machines that are not managed by vCenter Server can be in various states of operation and availability. In View Administrator, you can track the status of desktops in the right-hand column of the desktop-list page.

Table 12-1 shows the operational state of physical-computer and terminal-server desktops that are displayed in View Administrator. A desktop can be in only one state at a time.

Table 12-1. Status of Desktops That Are Physical Computers or Terminal Servers

Status	Type of State	Description
Waiting for Agent	Agent state	View Connection Server is waiting to receive the first request from View Agent on a physical-computer or terminal-server desktop.
Agent not reachable	Agent state	View Connection Server cannot establish communication with View Agent on the desktop. The desktop-source computer might be powered off.
Configuration error	Agent state	The display protocol such as RDP is not enabled, a terminal server is not enabled, or another protocol is not enabled.
Available	Availability	The desktop-source computer is powered on and the desktop is ready for an active connection. In a dedicated pool, the desktop is assigned to a user. The desktop starts when the user logs in.
Connected	Session state	The desktop is in an active session and has an active remote connection to a View client.
Disconnected	Session state	The desktop is in an active session, but it is disconnected from the View client.
–	Miscellaneous	A failure occurred when the desktop was in any of the preceding states.

Managing ThinApp Applications in View Administrator

13

You can use View Administrator to distribute and manage applications packaged with VMware ThinApp™. Managing ThinApp applications in View Administrator involves capturing and storing application packages, adding ThinApp applications to View Administrator, and assigning ThinApp applications to desktops and pools.

You must have a license to use the ThinApp management feature in View Administrator.

This chapter includes the following topics:

View Requirements for ThinApp Applications

When capturing and storing ThinApp applications that will be distributed to View desktops in View Administrator, you must meet certain requirements.

- You must package your applications as Microsoft Installation (MSI) packages.
- You must use ThinApp version 4.6 or later to create or repackage the MSI packages.
- You must store the MSI packages on a Windows network share that resides in an Active Directory domain that it accessible to your View Connection Server host and View desktops. The file server must support authentication and file permissions that are based on computer accounts.
- You must configure the file and sharing permissions on the network share that hosts the MSI packages to give Read access to the built-in Active Directory group Domain Computers. If you plan to distribute ThinApp applications to domain controllers, you must also give Read access to the built-in Active Directory group Domain Controllers.
- To allow users access to streaming ThinApp application packages, you must set the NTFS permission of the network share that hosts the ThinApp packages to `Read&Execute` for users.
- Make sure that a disjoint namespace does not prevent domain member computers from accessing the network share that hosts the MSI packages. A disjoint namespace occurs when an Active Directory domain name is different from the DNS namespace that is used by machines in that domain. See VMware Knowledge Base (KB) article 1023309 for more information.

- To run streamed ThinApp applications on View desktops, users must have access to the network share that hosts the MSI packages.

Capturing and Storing Application Packages

ThinApp provides application virtualization by decoupling an application from the underlying operating system and its libraries and framework and bundling the application into a single executable file called an application package.

To manage ThinApp applications in View Administrator, you must use the ThinApp Setup Capture wizard to capture and package your applications in MSI format and store the MSI packages in an application repository.

An application repository is a Windows network share. You use View Administrator to register the network share as an application repository. You can register multiple application repositories.

NOTE If you have multiple application repositories, you can use third-party solutions to manage load balancing and availability. View does not include load balancing or availability solutions.

See the *Introduction to VMware ThinApp* and the *ThinApp User's Guide* for complete information on ThinApp features and how to use the ThinApp Setup Capture wizard.

1 Package Your Applications on page 224

You use the ThinApp Setup Capture wizard to capture and package your applications.

2 Create a Windows Network Share on page 225

You must create a Windows network share to host the MSI packages that are distributed to View desktops and pools in View Administrator.

3 Register an Application Repository on page 225

You must register the Windows network share that hosts your MSI packages as an application repository in View Administrator.

4 Add ThinApp Applications to View Administrator on page 226

You add ThinApp applications to View Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to View Administrator, you can assign it to desktops and pools.

5 Create a ThinApp Template on page 226

You can create a template in View Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

Package Your Applications

You use the ThinApp Setup Capture wizard to capture and package your applications.

Prerequisites

- Download the ThinApp software from http://www.vmware.com/products/thinapp and install it on a clean computer. View supports ThinApp version 4.6 and later.
- Familiarize yourself with the ThinApp software requirements and application packaging instructions in the *ThinApp User's Guide*.

Procedure

1 Start the ThinApp Setup Capture wizard and follow the prompts in the wizard.

2 When the ThinApp Setup Capture wizard prompts you for a project location, select **Build MSI package**.

3 If you plan to stream the application to View desktops, set the MSIStreaming property to 1 in the `package.ini` file.

```
MSIStreaming=1
```

The ThinApp Setup Capture wizard encapsulates the application, all of the necessary components to run the application, and the application itself into an MSI package.

What to do next

Create a Windows network share to store the MSI packages.

Create a Windows Network Share

You must create a Windows network share to host the MSI packages that are distributed to View desktops and pools in View Administrator.

Prerequisites

- Use the ThinApp Setup Capture wizard to package the applications.
- Verify that the network share meets View requirements for storing ThinApp applications. See "View Requirements for ThinApp Applications," on page 223 for more information.

Procedure

1 Create a shared folder on a computer in an Active Directory domain that it accessible to both your View Connection Server host and View desktops.

2 Configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.

3 If you plan to assign ThinApp applications to domain controllers, give Read access to the built-in Active Directory group Domain Controllers.

4 If you plan to use streaming ThinApp application packages, set the NTFS permission of the network share that hosts the ThinApp packages to `Read&Execute` for users.

5 Copy your MSI packages to the shared folder.

What to do next

Register the Windows network share as an application repository in View Administrator.

Register an Application Repository

You must register the Windows network share that hosts your MSI packages as an application repository in View Administrator.

You can register multiple application repositories.

Prerequisites

Create a Windows network share.

Procedure

1 In View Administrator, select **View Configuration > ThinApp Configuration** and click **Add Repository**.

2 Type a display name for the application repository in the **Display name** text box.

3 Type the path to the Windows network share that hosts your application packages in the **Share path** text box.

The network share path must be in the form `\\ServerComputerName\ShareName` where *ServerComputerName* is the DNS name of the server computer. Do not specify an IP address.

For example: `\\server.domain.com\MSIPackages`

4 Click **Save** to register the application repository with View Administrator.

Add ThinApp Applications to View Administrator

You add ThinApp applications to View Administrator by scanning an application repository and selecting ThinApp applications. After you add a ThinApp application to View Administrator, you can assign it to desktops and pools.

Prerequisites

Register an application repository with View Administrator.

Procedure

1 In View Administrator, select **Inventory > ThinApps**.

2 On the **Summary** tab, click **Scan New ThinApps**.

3 Select an application repository and a folder to scan and click **Next**.

If the application repository contains subfolders, you can expand the root folder and select a subfolder.

4 Select the ThinApp applications that you want to add to View Administrator.

You can press Ctrl+click or Shift+click to select multiple ThinApp applications.

5 Click **Scan** to begin scanning the MSI packages that you selected.

You can click **Stop Scan** if you need to stop the scan.

View Administrator reports the status of each scanning operation and the number of ThinApp applications that were added to View Administrator. If you select an application that is already in View Administrator, it is not added again.

6 Click **Finish**.

The new ThinApp applications appear on the **Summary** tab.

What to do next

(Optional) Create ThinApp templates.

Create a ThinApp Template

You can create a template in View Administrator to specify a group of ThinApp applications. You can use templates to group applications together by function, vendor, or any other logical grouping that makes sense in your organization.

With ThinApp templates, you can streamline the distribution of multiple applications. When you assign a ThinApp template to a desktop or pool, View Administrator installs all of the applications that are currently in the template.

Creating ThinApp templates is optional.

NOTE If you add an application to a ThinApp template after assigning the template to a desktop or pool, View Administrator does not automatically assign the new application to the desktop or pool. If you remove an application from a ThinApp template that was previously assigned to a desktop or pool, the application remains assigned to the desktop or pool.

Prerequisites

Add selected ThinApp applications to View Administrator.

Procedure

1 In View Administrator, select **Inventory > ThinApps** and click **New Template**.

2 Type a name for the template and click **Add**.

All of the available ThinApp applications appear in the table.

3 To find a particular ThinApp application, type the name of the application in the **Find** text box and click **Find**.

4 Select the ThinApp applications that you want to include in the template and click **Add**.

You can press Ctrl+click or Shift+click to select multiple applications.

5 Click **OK** to save the template.

Assigning ThinApp Applications to Desktops and Pools

To install a ThinApp application on a View desktop, you use View Administrator to assign the ThinApp application to a desktop or pool.

When you assign a ThinApp application to a desktop, View Administrator begins installing the application on the desktop a few minutes later. When you assign a ThinApp application to a pool, View Administrator begins installing the application the first time a user logs in to a desktop in the pool.

Streaming	View Administrator installs a shortcut to the ThinApp application on the desktop. The shortcut points to the ThinApp application on the network share that hosts the repository. Users must have access to the network share to run streamed ThinApp applications.
Full	View Administrator installs the full ThinApp application on the local file system.

The amount of time it takes to install a ThinApp application depends on the size of the application.

IMPORTANT You can assign ThinApp applications to desktops and pools that have virtual machine sources only. You cannot assign ThinApp applications to Terminal Servers, Blade PCs, or traditional PCs.

- Best Practices for Assigning ThinApp Applications on page 228
  Follow best practices when you assign ThinApp applications to desktops and pools.
- Assign a ThinApp Application to Multiple Desktops on page 228
  You can assign a particular ThinApp to one or more desktops.
- Assign Multiple ThinApp Applications to a Desktop on page 229
  You can assign one or more ThinApp applications to a particular desktop.
- Assign a ThinApp Application to Multiple Pools on page 230
  You can assign a particular ThinApp application to one or more pools.

- Assign Multiple ThinApp Applications to a Pool on page 231

  You can assign one more ThinApp applications to a particular pool.

- Assign a ThinApp Template to a Desktop or Pool on page 231

  You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a desktop or pool.

- Review ThinApp Application Assignments on page 232

  You can review all of the desktops and pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular desktop or pool.

- Display MSI Package Information on page 233

  After you add a ThinApp application to View Administrator, you can display information about its MSI package.

Best Practices for Assigning ThinApp Applications

Follow best practices when you assign ThinApp applications to desktops and pools.

- To install a ThinApp application on a particular desktop, assign the application to the desktop. If you use a common naming convention for your desktops, you can use desktop assignments to quickly distribute applications to all of the desktops that use that naming convention.
- To install a ThinApp application on all of the desktops in a pool, assign the application to the pool. If you organize your pools by department or user type, you can use pool assignments to quickly distribute applications to specific departments or users. For example, if you have a pool for your accounting department users, you can distribute the same application to all of the users in your accounting department by assigning the application to the accounting pool.
- To streamline the distribution of multiple ThinApp applications, include the applications in a ThinApp template. When you assign a ThinApp template to a desktop or pool, View Administrator installs all of the applications currently in the template.
- Do not assign a ThinApp template to a desktop or pool if the template contains a ThinApp application that is already assigned to that desktop or pool. Also, do not assign a ThinApp template to the same desktop or pool more than once with a different installation type. View Administrator will return ThinApp assignment errors in both of these situations.
- Although assigning ThinApp applications to local desktops is not supported, View Administrator does not prevent you from doing so. If you want to experiment with assigning ThinApp applications to local desktops, you must meet certain requirements. If you plan to stream a ThinApp application, verify that View Agent in the local mode desktop can access the network share that hosts the ThinApp repository. Streamed ThinApp applications work only when the client system is connected to the network.

  Assigning ThinApp applications and removing them from a desktop work only if both View Connection Server and View Agent in the local mode desktop can access the network share that hosts the ThinApp repository.

CAUTION Rolling back a desktop might cause View Connection Server to have incorrect information about the ThinApps on the rolled-back desktop.

Assign a ThinApp Application to Multiple Desktops

You can assign a particular ThinApp to one or more desktops.

Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See "Add ThinApp Applications to View Administrator," on page 226.

Procedure

1 Select **Inventory > ThinApps** and select the ThinApp application.

2 From the **Add Assignment** drop-down menu, select **Desktops**.

The desktops that the ThinApp application is not already assigned to appear in the table.

Option	Action
Find a specific desktop	Type the name of the desktop in the **Find** text box and click **Find**.
Find all of the desktops that follow the same naming convention	Type a partial desktop name in the **Find** text box and click **Find**.

3 Select the desktops that you want to assign the ThinApp application to and click **Add**.

You can press Ctrl+click or Shift+click to select multiple desktops.

4 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp application a few minutes later. After the installation is finished, the application is available to all of the users of the desktops.

Assign Multiple ThinApp Applications to a Desktop

You can assign one or more ThinApp applications to a particular desktop.

Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See "Add ThinApp Applications to View Administrator," on page 226.

Procedure

1 Select **Inventory > Desktops** and double-click the name of the desktop in the Desktop column.

2 On the **Summary** tab, click **Add Assignment** in the ThinApps pane.

The ThinApp applications that are not already assigned to the desktop appear in the table.

3 To find a particular application, type the name of the application in the **Find** text box and click **Find**.

4 Select a ThinApp application to assign to the desktop and click **Add**.

Repeat this step to add multiple applications.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp applications a few minutes later. After the installation is finished, the applications are available to all of the users of the desktop.

Assign a ThinApp Application to Multiple Pools

You can assign a particular ThinApp application to one or more pools.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, View Administrator reinstalls the application for you. You do not have to manually reinstall the application.

Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See "Add ThinApp Applications to View Administrator," on page 226.

Procedure

1 Select **Inventory > ThinApps** and select the ThinApp application.

2 From the **Add Assignment** drop-down menu, select **Pools**.

The pools that the ThinApp application is not already assigned to appear in the table.

Option	Action
Find a specific pool	Type the name of the pool in the **Find** text box and click **Find**.
Find all of the pools that follow the same naming convention	Type a partial pool name in the **Find** text box and click **Find**.

3 Select the pools that you want to assign the ThinApp application to and click **Add**.

You can press Ctrl+click or Shift+click to select multiple pools.

4 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp application the first time a user logs in to a desktop in the pool. After the installation is finished, the application is available to all of the users of the desktop.

Assign Multiple ThinApp Applications to a Pool

You can assign one more ThinApp applications to a particular pool.

If you assign a ThinApp application to a linked-clone pool and later refresh, recompose, or rebalance the pool, View Administrator reinstalls the application for you. You do not have to manually reinstall the application.

Prerequisites

Scan an application repository and add selected ThinApp applications to View Administrator. See "Add ThinApp Applications to View Administrator," on page 226.

Procedure

1 Select **Inventory > Pools** and double-click the pool ID.

2 On the **Inventory** tab, click **ThinApps** and then click **Add Assignment**.

The ThinApp applications that are not already assigned to the pool appear in the table.

3 To find a particular application, type the name of the ThinApp application in the **Find** text box and click **Find**.

4 Select a ThinApp application to assign to the pool and click **Add**.

Repeat this step to select multiple applications.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

View Administrator begins installing the ThinApp applications the first time a user logs in to a desktop in the pool. After the installation is finished, the applications are available to all of the users of the desktop.

Assign a ThinApp Template to a Desktop or Pool

You can streamline the distribution of multiple ThinApp applications by assigning a ThinApp template to a desktop or pool.

When you assign a ThinApp template to a desktop or pool, View Administrator installs the ThinApp applications currently in the template.

Prerequisites

Create a ThinApp template. See "Create a ThinApp Template," on page 226.

Procedure

1 In View Administrator, select **Inventory > ThinApps**.

2 Select the ThinApp template.

3 From the **Add Assignment** drop-down menu, select **Desktops** or **Pools**.

All desktops or pools appear in the table.

Option	Action
Find a specific desktop or pool	Type the name of the desktop or pool in the **Find** text box and click **Find**.
Find all of the desktops or pools that follow the same naming convention	Type a partial desktop or pool name in the **Find** text box and click **Find**.

4 Select the desktops or pools that you want to assign the ThinApp template to and click **Add**.

Repeat this step to select multiple desktops or pools.

5 Select an installation type and click **OK**.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

Some ThinApp applications do not support both installation types. How the application package was created determines which installation types are available.

When you assign a ThinApp template to a desktop, View Administrator begins installing the applications in the template a few minutes later. When you assign a ThinApp template to a pool, View Administrator begins installing the applications in the template the first time a user logs in to a desktop in the pool. After the installation is finished, the applications are available to all of the users of the desktop or pool.

View Administrator returns an application assignment error if a ThinApp template contains an application that is already assigned to the desktop or pool.

Review ThinApp Application Assignments

You can review all of the desktops and pools that a particular ThinApp application is currently assigned to. You can also review all of the ThinApp applications that are assigned to a particular desktop or pool.

Prerequisites

Familiarize yourself with the ThinApp installation status values in "ThinApp Application Installation Status Values," on page 233.

Procedure

- Select the ThinApp application assignments that you want to review.

Option	Action
Review all of the desktops and pools that a particular ThinApp application is assigned to	Select **Inventory > ThinApps** and double-click the name of the ThinApp application. The **Assignments** tab shows the desktops and pools that the application is currently assigned to, including the installation type. The **Desktops** tab shows the desktops that are currently associated with the application, including installation status information. **NOTE** When you assign a ThinApp application to a pool, desktops in the pool appear on the **Desktops** tab only after the application is installed.
Review all of the ThinApp applications that are assigned to a particular desktop	Select **Inventory > Desktops** and double-click the name of the desktop in Desktop column. The ThinApps pane on **Summary** tab shows each application that is currently assigned to the desktop, including the installation status.
Review all of the ThinApp applications that are assigned to a particular pool	Select **Inventory > Pools**, double-click the pool ID, select the **Inventory** tab, and click **ThinApps**. The ThinApp Assignments pane shows each application that is currently assigned to the pool.

ThinApp Application Installation Status Values

After you assign a ThinApp application to a desktop or pool, View Administrator indicates the status of the installation.

Table 13-1 describes each status value.

Table 13-1. ThinApp Application Installation Status

Status	Description
Assigned	The ThinApp application is assigned to the desktop.
Install Error	An error occurred when View Administrator attempted to install the ThinApp application.
Uninstall Error	An error occurred when View Administrator attempted to uninstall the ThinApp application.
Installed	The ThinApp application is installed.
Pending Install	View Administrator is attempting to install the ThinApp application. You cannot unassign an application that has this status. **NOTE** This value does not appear for desktops in pools.
Pending Uninstall	View Administrator is attempting to uninstall the ThinApp application.

Display MSI Package Information

After you add a ThinApp application to View Administrator, you can display information about its MSI package.

Procedure

1. In View Administrator, select **Inventory > ThinApps**.

   The **Summary** tab lists the applications that are currently available and shows the number of full and streaming assignments.

2. Double-click the name of the application in the ThinApp column.

3. Select the **Summary** tab to see general information about the MSI package.

4 Click **Package Info** to see detailed information about the MSI package.

Maintaining ThinApp Applications in View Administrator

Maintaining ThinApp applications in View Administrator involves tasks such as removing ThinApp application assignments, removing ThinApp applications and application repositories, and modifying and deleting ThinApp templates.

NOTE To upgrade a ThinApp application, you must unassign and remove the older version of the application and add and assign the newer version.

- Remove a ThinApp Application Assignment from Multiple Desktops on page 234
  You can remove an assignment to a particular ThinApp application from one or more desktops.
- Remove Multiple ThinApp Application Assignments from a Desktop on page 235
  You can remove assignments to one or more ThinApp applications from a particular desktop.
- Remove a ThinApp Application Assignment from Multiple Pools on page 235
  You can remove an assignment to a particular ThinApp application from one or more pools.
- Remove Multiple ThinApp Application Assignments from a Pool on page 235
  You can remove one or more ThinApp application assignments from a particular pool.
- Remove a ThinApp Application from View Administrator on page 236
  When you remove a ThinApp application from View Administrator, you can no longer assign the application to desktops and pools.
- Modify or Delete a ThinApp Template on page 236
  You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.
- Remove an Application Repository on page 236
  You can remove an application repository from View Administrator.

Remove a ThinApp Application Assignment from Multiple Desktops

You can remove an assignment to a particular ThinApp application from one or more desktops.

Prerequisites

Notify the users of the desktops that you intend to remove the application.

Procedure

1 Select **Inventory > ThinApps** and double-click the name of the ThinApp application.

2 On the **Assignments** tab, select a desktop and click **Remove Assignment**.

You can press Ctrl+click or Shift+click to select multiple desktops.

View Administrator uninstalls the ThinApp application a few minutes later.

IMPORTANT If an end user is using the ThinApp application at the time when View Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the View desktop and then click **Force Clear Assignment** in View Administrator.

Remove Multiple ThinApp Application Assignments from a Desktop

You can remove assignments to one or more ThinApp applications from a particular desktop.

Prerequisites

Notify the users of the desktop that you intend to remove the applications.

Procedure

1 Select **Inventory > Desktops** and double-click the name of the desktop in the Desktop column.

2 On the **Summary** tab, select the ThinApp application and click **Remove Assignment** in the ThinApps pane.

Repeat this step to remove another application assignment.

View Administrator uninstalls the ThinApp application a few minutes later.

IMPORTANT If an end user is using the ThinApp application at the time when View Administrator attempts to uninstall the application, the uninstallation fails and the application status changes to Uninstall Error. When this error occurs, you must first manually uninstall the ThinApp application files from the View desktop and then click **Force Clear Assignment** in View Administrator.

Remove a ThinApp Application Assignment from Multiple Pools

You can remove an assignment to a particular ThinApp application from one or more pools.

Prerequisites

Notify the users of the desktops in the pools that you intend to remove the application.

Procedure

1 Select **Inventory > ThinApps** and double-click the name of the ThinApp application.

2 On the **Assignments** tab, select a pool and click **Remove Assignment**.

You can press Ctrl+click or Shift+click to select multiple pools.

View Administrator uninstalls the ThinApp application the first time a user logs in to a desktop in the pool.

Remove Multiple ThinApp Application Assignments from a Pool

You can remove one or more ThinApp application assignments from a particular pool.

Prerequisites

Notify the users of the desktops in the pool that you intend to remove the applications.

Procedure

1 Select **Inventory > Pools** and double-click the pool ID.

2 On the **Inventory** tab, click **ThinApps**, select the ThinApp application, and click **Remove Assignment**.

Repeat this step to remove multiple applications.

View Administrator uninstalls the ThinApp applications the first time a user logs in to a desktop in the pool.

Remove a ThinApp Application from View Administrator

When you remove a ThinApp application from View Administrator, you can no longer assign the application to desktops and pools.

You might need to remove a ThinApp application if your organization decides to replace it with a different vendor's application.

NOTE You cannot remove a ThinApp application if it is already assigned to a desktop or pool or if it is in the Pending Uninstall state.

Prerequisites

If a ThinApp application is currently assigned to a desktop or pool, remove the assignment from the desktop or pool.

Procedure

1 In View Administrator, select **Inventory > ThinApps** and select the ThinApp application.

2 Click **Remove ThinApp**.

3 Click **OK**.

Modify or Delete a ThinApp Template

You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.

If you add an application to a ThinApp template after assigning the template to a desktop or pool, View Administrator does not automatically assign the new application to the desktop or pool. If you remove an application from a ThinApp template that was previously assigned to a desktop or pool, the application remains assigned to the desktop or pool.

Procedure

◆ In View Administrator, select **Inventory > ThinApps** and select the ThinApp template.

Option	Action
Add or remove ThinApp applications from the template	Click **Edit Template**.
Delete the template	Click **Delete Template**.

Remove an Application Repository

You can remove an application repository from View Administrator.

You might need to remove an application repository if you no longer need the MSI packages that it contains, or if you need to move the MSI packages to a different network share. You cannot edit the share path of an application repository in View Administrator.

Procedure

1 In View Administrator, select **View Configuration > ThinApp Configuration** and select the application repository.

2 Click **Remove Repository**.

Monitoring and Troubleshooting ThinApp Applications in View Administrator

View Administrator logs events that are related to ThinApp application management to the Events and Reporting database. You can view these events on the **Events** tab in View Administrator.

An event appears on the **Events** tab when the following situations occur.

- A ThinApp application is assigned or an application assignment is removed
- A ThinApp application is installed or uninstalled on a desktop
- A ThinApp application cannot be installed or uninstalled
- A ThinApp application repository is registered, modified, or removed from View Administrator
- A ThinApp application is added to View Administrator

Troubleshooting tips are available for common ThinApp application management problems.

Cannot Register an Application Repository

You cannot register an application repository in View Administrator.

Problem

You receive an error message when you attempt to register an application repository in View Administrator.

Cause

The View Connection Server host cannot access the network share that hosts the application repository. The network share path that you typed in the **Share path** text box might be incorrect, the network share that hosts the application repository is in a domain that is not accessible from the View Connection Server host, or the network share permissions have not been set up properly.

Solution

- If the network share path is incorrect, type the correct network share path. Network share paths that contain IP addresses are not supported.
- If the network share is not in an accessible domain, copy your application packages to a network share in a domain that is accessible from the View Connection Server host.
- Verify that the file and sharing permissions on the shared folder give Read access to the built-in Active Directory group Domain Computers. If you plan to assign ThinApps to domain controllers, verify that the file and sharing permissions also give Read access to the built-in Active Directory group Domain Controllers. After you set or change permissions, it can take up to 20 minutes for the network share to become accessible.

Cannot Add ThinApp Applications to View Administrator

View Administrator cannot add ThinApp applications to View Administrator.

Problem

No MSI packages are available when you click **Scan New ThinApps** in View Administrator.

Cause

Either the application packages are not in MSI format or the View Connection Server host cannot access the directories in the network share.

Solution

- Verify that the application packages in the application repository are in MSI format.
- Verify that the network share meets View requirements for ThinApp applications. See "View Requirements for ThinApp Applications," on page 223 for more information.
- Verify that the directories in the network share have the proper permissions. See "Cannot Register an Application Repository," on page 237 for more information.

Messages appear in the View Connection Server debug log file when an application repository is scanned. View Connection Server log files are located on the View Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

Cannot Assign a ThinApp Template

You cannot assign a ThinApp template to a desktop or pool.

Problem

View Administrator returns an assignment error when you attempt to assign a ThinApp template to a desktop or pool.

Cause

Either the ThinApp template contains an application that is already assigned to the desktop or pool, or the ThinApp template was previously assigned to the desktop or pool with a different installation type.

Solution

If the template contains a ThinApp application that is already assigned to the desktop or pool, create a new template that does not contain the application or edit the existing template and remove the application. Assign the new or modified template to the desktop or pool.

To change the installation type of a ThinApp application, you must remove the existing application assignment from the desktop or pool. After the ThinApp application is uninstalled, you can assign it to the desktop or pool with a different installation type.

ThinApp Application Is Not Installed

View Administrator cannot install a ThinApp application.

Problem

The ThinApp application installation status shows either Pending Install or Install Error.

Cause

Common causes for this problem include the following:

- There was not enough disk space on the desktop to install the ThinApp application.
- Network connectivity was lost between the View Connection Server host and the desktop or between the View Connection Server host and the application repository.
- The ThinApp application was not accessible in the network share.
- The ThinApp application was previously installed or the directory or file already exists on the desktop.

You can see the View Agent and View Connection Server log files for more information about the cause of the problem.

View Agent log files are located on the desktop in *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs for Windows XP systems and *drive*:\ProgramData\VMware\VDM\logs for Windows 7 systems.

View Connection Server log files are located on the View Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

Solution

1 In View Administrator, select **Inventory > ThinApps**.

2 Click the name of the ThinApp application.

3 On the **Desktops** tab, select the desktop and click **Retry Install** to reinstall the ThinApp application.

ThinApp Application Is Not Uninstalled

View Administrator cannot uninstall a ThinApp application.

Problem

The ThinApp application installation status shows Uninstall Error.

Cause

Common causes for this error include the following:

- The ThinApp application was busy when View Administrator tried to uninstall it.
- Network connectivity was lost between the View Connection Server host and the desktop.

You can see the View Agent and View Connection Server log files for more information about the cause of the problem.

View Agent log files are located on the desktop in *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs for Windows XP systems and *drive*:\ProgramData\VMware\VDM\logs for Windows 7 systems.

View Connection Server log files are located on the View Connection Server host in the *drive*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs directory.

Solution

1 In View Administrator, select **Inventory > ThinApps**.

2 Click the name of the ThinApp application.

3 Click the **Desktops** tab, select the desktop, and click **Retry Uninstall** to retry the uninstall operation.

4 If the uninstall operation still fails, manually remove the ThinApp application from the desktop and then click **Force Clear Assignment**.

   This command clears the ThinApp application assignment in View Administrator. It does not remove any files or settings in the desktop.

   Important Use this command only after manually removing the ThinApp application from the desktop.

MSI Package Is Invalid

View Administrator reports an invalid MSI package in an application repository.

Problem

View Administrator reports that an MSI package is invalid during a scanning operation.

Cause

Common causes of this problem include the following:

- The MSI file is corrupted.

- The MSI file was not created with ThinApp.
- The MSI file was created or repackaged with an unsupported version of ThinApp. You must use ThinApp version 4.6 or later.

Solution

See the *ThinApp User's Guide* for information on troubleshooting problems with MSI packages.

ThinApp Configuration Example

The ThinApp configuration example takes you step-by-step through a typical ThinApp configuration, beginning with capturing and packaging applications and ending with checking the status of an installation.

Prerequisites

See these topics for complete information about how to perform the steps in this example.

- "Capturing and Storing Application Packages," on page 224
- "Assigning ThinApp Applications to Desktops and Pools," on page 227

Procedure

1 Download the ThinApp software from http://www.vmware.com/products/thinapp and install it on a clean computer.

View supports ThinApp version 4.6 and later.

2 Use the ThinApp Setup Capture wizard to capture and package your applications in MSI format.

3 Create a shared folder on a computer in an Active Directory domain that it accessible to both your View Connection Server host and your View desktops and configure the file and sharing permissions on the shared folder to give Read access to the built-in Active Directory group Domain Computers.

If you plan to assign ThinApp applications to domain controllers, also give Read access to the built-in Active Directory group Domain Controllers.

4 Copy your MSI packages to the shared folder.

5 Register the shared folder as an application repository in View Administrator.

6 In View Administrator, scan the MSI packages in the application repository and add selected ThinApp applications to View Administrator.

7 Decide whether to assign the ThinApp applications to desktops or pools.

If you use a common naming convention for your desktops, you can use desktop assignments to quickly distribute applications to all of the desktops that use that naming convention. If you organize your pools by department or user type, you can use pool assignments to quickly distribute applications to specific departments or users.

8 In View Administrator, select the ThinApp applications to assign to your desktops or pools and specify the installation method.

Option	Action
Streaming	Installs a shortcut to the application on the desktop. The shortcut points to the application on the network share that hosts the repository. Users must have access to the network share to run the application.
Full	Installs the full application on the local file system.

9 In View Administrator, check the installation status of the ThinApp applications.

14 Managing Local Desktops

To manage desktops that are used in local mode, you must set up the environment so that data is transferred when users check View desktops out to their local systems. You must also manage other tasks where data transfer occurs, such as desktop check-in, rollback, and backup, and set policies for which of these actions users can initiate.

This chapter includes the following topics:

Benefits of Using View Desktops in Local Mode

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

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

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

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

Local resource utilization

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

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

Conserving datacenter resources by requiring local mode

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

Check-outs

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

Backups

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

Rollbacks

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

Check-ins

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

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

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

- You must have a View license that includes the Local Mode component.
- End users cannot access their local desktop while rollbacks and check-ins are taking place.
- This feature is available only for virtual machines that are managed by vCenter Server.
- Checking out a View desktop that uses virtual hardware version 8 is not supported. If you use vSphere 5 to create virtual machines that will be sources for local mode desktops, be sure to create virtual machines that use virtual hardware version 7.
- You cannot use View Persona Management with desktops that run in local mode.
- Assigning application packages created with VMware ThinApp is not supported for View desktops that are downloaded and used in local mode. Rolling back a desktop might cause View Connection Server to have incorrect information about the ThinApps on the rolled-back desktop.
- For security reasons, you cannot access the host CD-ROM from within the View desktop.
- Also for security reasons, you cannot copy and paste text or system objects such as files and folders between the local system and the View desktop.

Overview of Setting Up a Local Desktop Deployment

To create and deploy View desktops in local mode, you must have the required license, set up a View Transfer Server, use a desktop source managed by vCenter Server, and apply settings and policies specific to local mode.

When you create desktops that can be checked out for use on end users' local systems, in addition to the usual setup tasks, you must complete several tasks for local mode.

1. Verify that you have a license for the VMware View with Local Mode component.

   In View Administrator, go to **View Configuration > Product licensing and usage**.

2. Verify that the user account used to access vCenter Server from View Connection Server has the required administrator privileges.

   To see which user account is being used, in View Administrator, go to **View Configuration > Servers**, select the vCenter Server, and click **Edit.**

   The list of privileges required for vCenter Server operations is provided in the *VMware View Installation* document, in the section about configuring user accounts for vCenter Server.

3. Install View Transfer Server in a virtual machine and add this server to a View Connection Server configuration.

   In View Administrator, go to **View Configuration > Servers**.

4. If you plan to use View Composer linked-clone desktops, configure a Transfer Server repository.

   In View Administrator, go to **View Configuration > Transfer Server Repository**.

5. If you plan to create a manual pool, verify that the desktop source is a virtual machine managed by vCenter Server.

6. Create a virtual machine in vCenter Server to use as the desktop source.

If you create a virtual machine that has more virtual memory and processors than are available on a local client system, the local version of the desktop will not power on, and an error message will appear.

7 If you plan to use linked-clone desktops, publish the desktops' View Composer base image as a package in the Transfer Server repository.

You can publish the base image when you create a pool or after the pool is created.

8 Verify that the **Local Mode** policy is set to **Allow** for the desktop pool.

In View Administrator, go to the **Policies** tab for that pool.

9 If you want desktops to run only in local mode so that users must always check out the desktop, set the **Remote Mode** policy to **Deny**.

In View Administrator, go to the **Policies** tab for that pool.

10 Direct end users to install View Client with Local Mode on their local systems.

IMPORTANT In addition, take the following considerations into account when planning to deploy local desktops:

- When creating automated pools, use dedicated assignment and create the pool only for desktops that are intended to be used in local mode. Virtual machines that are intended for use in local mode can be placed on datastores with lower IOPS than storage intended to support large numbers of remote View desktops. Also, because assigning ThinApp packages to local desktops is not supported, a best practice is to assign ThinApp packages to pools that do not contain any local desktops.
- As a standard best practice for desktops, make sure that a unique password is created for the local Administrator account on each View desktop that you plan to use in local mode.
- If you configure the desktop to use RSA authentication, end users are prompted for the RSA token when they have a network connection to View Connection Server, but are not prompted when they do not have a network connection.

Set a Desktop to Run Only in Local Mode

You can reduce datacenter costs associated with bandwidth, memory, and CPU resources by requiring that View desktops be downloaded and used only in local mode.

When a View desktop is configured to run only in local mode, end users see that a download and check out are required when they select the desktop in View Client. The options of connecting to the desktop and checking it in are not available to end users.

Prerequisites

- Verify that the View desktop meets all the requirements for running in local mode.

  See "Overview of Setting Up a Local Desktop Deployment," on page 243.

- Familiarize yourself with the policies and settings specific to local mode.

  See "Managing Data Transfers," on page 257.

Procedure

1 In View Administrator, view the policy for the appropriate level.

Option	Action
All desktops and pools	Select **Policies > Global Policies > View Policies** panel, and click **Edit Policies**.
Single pool	Select **Inventory > Pools > *specific_pool***. On the **Policies** tab, in the **View Policies** panel, click **Edit Policies**.
Single user	Select **Inventory > Pools > *specific_pool***, and on the **Policies** tab, click **User Overrides**.

2 Set the **Remote Mode** View policy to **Deny**.

Option	Action
All desktops and pools or a single pool	In the Edit View Policies dialog box, set **Remote Mode** to **Deny** and click **OK**.
Single user	Complete the Add User wizard to specify the user and set **Remote Mode** to **Deny**.

The desktop now requires a download and check out.

What to do next

If you want to prevent end users from checking the desktop in again, set the **User-initiated check in** policy to **Deny**.

If you want to prevent end users from rolling the desktop back, set the **User-initiated rollback** policy to **Deny**.

Checking Out a Local Mode Desktop for the First Time

The first time an end user checks out a View desktop to use in local mode, the check-out and download process involves several phases and takes more time than for subsequent check-out operations.

After an end user logs in with View Client and is provided with a list of one or more desktops, the user can either connect to the desktop and then check it out or else check out the desktop without connecting remotely first.

IMPORTANT You cannot check out a desktop if when you logged in, you used the **Log in as current user** feature. You must close View Client, start it again, and clear the **Log in as current user** check box.

If the end user connects to the desktop and then checks it out, the user is logged off of the remote desktop, the virtual machine in the datacenter is locked, and a copy of the virtual machine is downloaded to the end user.

After the download is complete, the first time the end user powers on the local desktop, a number of drivers are installed in the local desktop. Which drivers are installed depends on the View desktop operating system and the local computer's hardware and operating system. During installation of the drivers, performance of the View desktop is affected, especially if the View desktop runs a Windows XP operating system.

After the drivers are installed, the end user is prompted to reboot the local desktop.

NOTE Occasionally, if you click inside a View desktop window when the guest operating system is starting up or shutting down, your pointer remains inside the window. After startup is complete and VMware Tools is running, the pointer is released. If your pointer is grabbed inside the desktop window, you can release it by pressing Ctrl+Alt.

The amount of RAM and the number of CPUs that the local View desktop uses depends on the capabilities of the local computer. The View desktop uses NAT so that it shares the IP and MAC addresses of the local computer. For more information, see "Configuring Endpoint Resource Usage," on page 266.

Best Practices for Deploying Local Desktops

Best-practice recommendations address questions about the memory, processing power, and number of the various components that affect a local mode deployment.

General Recommendations for Most Deployments

Virtual machine configuration

Desktops that run in local mode automatically adjust the amount of memory and processing power they use based on that available from the client computer. Because of this capability, you can configure the minimum amount of RAM and virtual CPUs required by the guest operating system when you create the virtual machine in vCenter Server.

View Transfer Server

Some features of View Transfer Server are CPU-intensive. If you plan to use SSL for local mode operations such as checking out and checking in desktops or for replicating data back to the datacenter, the virtual machine hosting the Transfer Server might need an additional virtual CPU. You might also need more processing power if you turn on compression for replication operations. For minimum memory and processor requirements, see the topic in the *View Installation* document about system requirements for View Transfer Server.

When determining how many View Transfer Server instances to add to View Connection Server, determine whether high availability is an important consideration. If it is, add at least two instances. If one Transfer Server goes down, View Connection Server automatically sends requests to the other one.

When calculating how many Transfer Server instances you need, also take into consideration how many end users are likely to be replicating data or checking out or checking in desktops at the same time. Each Transfer Server instance can accommodate 60 concurrent disk operations, though network bandwidth will likely be saturated at a lower number. VMware tested 20 concurrent disk operations, such as 20 clients downloading a local desktop at the same time, over a 1GB per second network connection.

Transfer Server Repository

Base images of View Composer linked-clone desktops are kept in the Transfer Server Repository, on a network share. The faster your network storage disks are, the better performance will be.

Pool settings

Use View Composer to create pools of linked-clone desktops. When using the Create Pool wizard, choose dedicated assignment and create the pool only for desktops that are intended to be used in local mode. Local mode virtual machines can be placed on datastores with lower IOPS than storage intended to support large numbers of remote View desktops.

Data replication

Determine whether end users will need to replicate OS disk data, such as that contained in a customization specification. If not, set a policy so that only persistent disks are replicated.

If you set an automatic replication interval, use the default of every 12 hours or set an interval that is even less frequent.

Do not turn on deduplication or compression unless you notice problems due to a slow network connection. The deduplication and compression features reduce the amount of network bandwidth required at the expense of increased processing power required on the end user's computer or on the Transfer Server.

Small Deployment with Minimal Capital Expenditure

You can reduce the number of ESX servers required for your deployment if you increase the number of virtual machines on each server. An ESX 4.1 server can host up to 500 virtual machines if most are not powered on at the same time.

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

- Set a View policy so that end users must use their View desktops in local mode only. With this setting, the virtual machines in the datacenter remain locked and powered off.
- Set local mode policies so that end users cannot initiate desktop check-ins, rollbacks, or replication.
- Do not set automatic replication intervals.
- Configure View Connection Server settings so that deduplication and compression are not used for local mode operations. These settings might be helpful only if replication of local desktop data occurs over a slow network during a time when the end user might notice a performance reduction on their client computer.
- Configure View Connection Server settings so that SSL is not used for local mode operations or provisioning.
- Use View Composer to create linked-clone desktops, but do not use the recompose feature. Instead use traditional software update mechanisms to deploy patches and updates directly to local desktops on end users' computers.
- If the performance of View Connection Server is affected by the number of local desktops, set the heartbeat interval to be less frequent. The default is five minutes.

Managing View Transfer Server

View Transfer Server is the View component that supports data-transfer operations for local desktops.

Understanding View Transfer Server

View Transfer Server manages and streamlines data transfers between the datacenter and local desktops. View Transfer Server is required to support desktops that run View Client with Local Mode.

View Transfer Server sends data between the remote and local desktops in several situations.

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

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

An event such as a network outage or the removal of View Transfer Server from View Manager can interrupt active data transfers. View Transfer Server resumes the paused transfers when the components are running again.

Add View Transfer Server to View Manager

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

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

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

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that vCenter Server is added to View Manager. The **View Configuration > Servers** page in View Administrator displays vCenter Server instances that are added to View Manager.

Procedure

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

2 In the Transfer Servers panel, click **Add**.

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

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

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

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

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

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

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

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

Remove View Transfer Server from View Manager

When you remove all instances of View Transfer Server from View Manager, you cannot check out, check in, or replicate data for local desktops.

When you remove a View Transfer Server instance that is actively performing transfers, the active transfer operations are paused. Local desktop sessions show the transfer status as paused.

For example, if you remove View Transfer Server while you check out a desktop, the check-out operation is paused. The user can resume the paused transfer operation from the client computer.

NOTE You must remove a View Transfer Server instance from View Manager before you perform these operations:

- Uninstall or upgrade a View Transfer Server instance
- Perform maintenance operations on a View Transfer Server virtual machine in vCenter Server

---

Procedure

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

2 Select a View Transfer Server instance.

3 Click **Remove**.

4 If transfers are currently active, choose whether to cancel the active transfers or cancel this task and keep View Transfer Server.

5 Click **OK**.

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

Use Maintenance Mode to Suspend Data Transfers for Local Desktops

When you place a View Transfer Server instance in maintenance mode, you suspend active data transfers and prevent future data transfers for local desktops on that View Transfer Server instance. When you take a View Transfer Server instance out of maintenance mode, suspended transfers can be resumed from the client and future transfers can occur.

When all View Transfer Server instances are in maintenance mode, you can migrate the Transfer Server repository. See "Migrate the Transfer Server Repository to a New Location," on page 255.

While a View Transfer Server instance is added to View Manager and in active mode, its DRS automation policy is set to Manual, which effectively disables DRS. To migrate a View Transfer Server instance to another ESX host or datastore, place the instance in maintenance mode before you begin the migration.

Procedure

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

2 Select a View Transfer Server instance.

3 Click **Enter Maintenance Mode**.

4 If transfers are currently active, choose whether to cancel the active transfers or wait until active transfers are completed before placing View Transfer Server in maintenance mode.

If you cancel active transfers, View Transfer Server enters maintenance mode immediately.

If you allow active transfers to finish, View Transfer Server enters a **Pending** state. When the current disk transfer is completed, View Transfer Server enters maintenance mode.

NOTE Allowing active transfers to finish ensures that the current disk is transferred. However, virtual machines contain multiple disks. A transfer operation such as a desktop checkout might not be completed if no other View Transfer Server instances are available to transfer any remaining disks. When a View Transfer Server instance is taken out of maintenance mode, suspended transfers can be resumed.

5 Click **OK**.

What to do next

When you are ready to take View Transfer Server out of maintenance mode, select the View Transfer Server instance and click **Exit Maintenance Mode**. Suspended transfers can be resumed and new data transfers can start.

Improve Transfer Performance Over a WAN on Windows Server 2003

In a WAN environment with high network latency, you can enhance transfer performance by increasing the sizes of TCP send and receive windows.

When View Transfer Server is installed on Windows Server 2008, the TCP send and receive windows are increased to 640KB by default. You do not have to reconfigure these values.

When View Transfer Server is installed on Windows Server 2003, you must manually set registry keys to increase the TCP send and receive windows to 640KB.

Prerequisites

Verify that View Transfer Server is installed on a Windows Server 2003 operating system.

Procedure

1 Start the Windows Registry Editor on the Windows Server 2003 computer on which View Transfer Server is installed.

2 Add two new registry keys called **DefaultSendWindow** and **DefaultReceiveWindow** to `HKEY_LOCAL_MACHINE, System, CurrentControlSet, Services, AFD, Parameters`.

3 Set the **DefaultSendWindow** and **DefaultReceiveWindow** key values to **`655360`**.

You must type a positive integer. The values are configured in bytes. The key types are **REG_DWORD**.

4 Restart View Transfer Server.

View Transfer Server Status

View Transfer Server can be in various states of operation and availability. In View Administrator, you can track the status of View Transfer Server in the Transfer Servers pane on the **View Configuration > Servers** page.

Table 14-1. View Transfer Server States During Normal Operations

Status	Description
Ready	View Transfer Server and the Transfer Server repository are configured and operating properly.
Pending	View Transfer Server is being added to View Manager or is exiting Maintenance mode. View Connection Server is actively establishing a connection with View Transfer Server. When the connection is made, View Transfer Server will be moved to an operational state such as Ready.

Table 14-1. View Transfer Server States During Normal Operations (Continued)

Status	Description
Maintenance mode pending	View Transfer Server is entering Maintenance mode while waiting for active transfers and package publish operations to be completed.
Maintenance mode	Active data transfers are suspended. Users cannot initiate new transfers. Scheduled, pending transfers cannot take place. View Transfer Server cannot publish packages to the Transfer Server repository.
Initializing Transfer Server repository	View Transfer Server is initializing the Transfer Server repository. If View Transfer Server has trouble initializing the Transfer Server repository, the status will change to an error state. To resolve the issue, see the troubleshooting tip for the displayed error state.
Missing Transfer Server repository	No Transfer Server repository is configured in View Manager. This state does not indicate an error because you can perform transfer operations for full virtual machines without configuring a Transfer Server repository. However, this state does indicate an error when you use linked-clone desktops in local mode. You cannot perform transfer operations for linked-clone desktops when no Transfer Server repository is configured.

View Transfer Server enters an error state when it becomes unavailable or cannot operate normally. To resolve an issue, read the troubleshooting tip for the displayed error state. See "Troubleshooting View Transfer Server and Local Desktop Operations," on page 277.

Table 14-2. View Transfer Server Error States

Status	Description
Bad Transfer Server repository	The Transfer Server repository that View Transfer Server is configured to connect to differs from the Transfer Server repository that is currently configured in View Connection Server.
Repository connection error	View Transfer Server cannot connect to the configured Transfer Server repository.
Bad health check	View Transfer Server failed the View Manager health check. View Transfer Server is unavailable or not operating properly.
Transfer Server repository conflict	Multiple View Transfer Server instances are configured to connect to different Transfer Server repositories. This state can occur if, at the same time, multiple View Transfer Server instances are added to View Manager, and each instance is configured with a different Transfer Server repository.
Web Server down	The Apache2.2 service that supports the Transfer Server repository is not running.

Managing the Transfer Server Repository

View Transfer Server uses the Transfer Server repository to store View Composer base images that are downloaded to local desktops. The Transfer Server repository is required for checking out linked-clone desktops to run in local mode.

Using the Transfer Server Repository to Download System Images

To support linked-clone desktops that run in local mode, the Transfer Server repository stores View Composer base images in an accessible datastore. View Manager and View Transfer Server provision and update linked-clone, local desktops from the Transfer Server repository.

NOTE If you do not use View Composer linked clones in local mode, you do not have to configure a Transfer Server repository. The Transfer Server repository is not used for full virtual machine desktops that run in local mode.

Before a user can check out a linked-clone desktop so that it can run in local mode, you must publish its base image to the Transfer Server repository.

When you publish an image file to the Transfer Server repository, View Transfer Server stores the files as encrypted packages. View Transfer Server can compress the packages to streamline downloads to local desktops.

When a user checks out a linked-clone desktop for the first time, View Transfer Server performs two operations:

- Downloads the base image from the Transfer Server repository to the local computer.
- Downloads the remote linked-clone desktop from the datacenter to the local computer. The desktop consists of the linked clone's OS delta disk and a View Composer persistent disk.

When you run linked-clone desktops in the datacenter, the linked clones share access to one base image. When you run a linked-clone desktop in local mode, a copy of the base image must reside with the linked-clone desktop on the local computer.

The base image is downloaded only once if it remains unchanged. When users check in and check out their desktops again, View Transfer Server downloads the linked clones' OS delta disks and View Composer persistent disks, not the base image.

If a base image is recomposed, View Transfer Server downloads the updated image from the Transfer Server repository to the local computers the next time users check out their desktops. For details, see "Recompose Linked-Clone Desktops That Can Run in Local Mode," on page 195.

IMPORTANT A linked-clone desktop that was created from a base image must be checked into the datacenter before you can recompose it.

Determine the Size of a View Composer Base Image

The Transfer Server repository must be large enough to store the View Composer base images for all the linked-clone desktops that are used in local mode. To make sure that the Transfer Server repository can accommodate a particular base image, you can determine the approximate size of the base image.

A base image can be several gigabytes in size.

The maximum size of a base image is the sum of the provisioned sizes of the hard disks in the parent virtual machine. The actual base image size might be smaller than the maximum.

Prerequisites

Verify that you created a parent virtual machine to use for creating a linked-clone desktop pool.

Procedure

1 In vSphere Client, select the parent virtual machine.

2 Click **Edit Settings**.

3 In the **Hardware** tab, select the first configured hard disk.

For example, select **Hard Disk 1**.

4 In the Disk Provisioning pane, read the Provisioned Size.

5 If the virtual machine has more than one hard disk, repeat steps 3 and 4 for each additional hard disk.

6 Add the provisioned sizes of the hard disks.

Configure the Transfer Server Repository

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

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

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

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

Prerequisites

- Verify that View Transfer Server is installed on a Windows Server virtual machine.
- Verify that View Transfer Server is added to View Manager. See "Add View Transfer Server to View Manager," on page 248.

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

- Determine how large the Transfer Server repository must be to store your View Composer base images. A base image can be several gigabytes in size. To determine the size of a specific base image, see "Determine the Size of a View Composer Base Image," on page 252.

Procedure

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

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

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

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

3 Put all View Transfer Server instances into maintenance mode.

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

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

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

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

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

4 In the Transfer Servers panel, next to Transfer Server repository, click **None Configured**.

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

6 Type the Transfer Server repository location and other information.

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

7 Click **OK**.

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

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

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

Publish Package Files in the Transfer Server Repository

Before a user can check out a linked-clone desktop, you must publish its View Composer base image as a package in the Transfer Server repository.

When a user checks out a linked-clone desktop, View Transfer Server downloads the clone's base-image package files from the Transfer Server repository to the local computer.

You can publish packages from the **Transfer Server repository** page in View Administrator. You can also publish packages when you create a linked-clone pool. After a pool is created, you can also publish packages from the individual pool page by using the **View Composer > Publish** option.

Prerequisites

- Verify that a View Transfer Server instance is configured in View Manager. See "Add View Transfer Server to View Manager," on page 248.
- Verify that the Transfer Server repository is configured in View Manager. See "Configure the Transfer Server Repository," on page 253.
- Verify that the Transfer Server repository is large enough to accommodate the base image, which can be several gigabytes. The repository must have space for the base image before the package files are compressed. See "Determine the Size of a View Composer Base Image," on page 252.
- Verify that a linked-clone desktop pool that will be used in local mode is created.

Procedure

1 In View Administrator, click **View Configuration > Transfer Server Repository**.

2 Click **Publish**.

3 Select a View Composer base image from the list and click **Next**.

4 Click **Finish**.

The package appears in the Contents pane in the Transfer Server Repository page. The package status changes from **Initializing** to **Publishing** to **Published**.

The publication process can take time. Click the refresh icon on the Transfer Repository page to display the percent of the operation that is completed.

View Transfer Server can download the published View Composer base image to local desktops.

Delete a Package File from the Transfer Server Repository

View Transfer Server stores View Composer base images as package files in the Transfer Server repository. When these files are out of date or no longer used, you can delete the packages from the Transfer Server repository.

You can delete a package file even if linked-clone desktops still use the base image from which the package file was published. After you delete the package file, these desktops cannot be checked out.

Prerequisites

- Verify that View Transfer Server is configured in View Manager. See "Add View Transfer Server to View Manager," on page 248.
- Verify that a Transfer Server repository is configured. See "Configure the Transfer Server Repository," on page 253.

Procedure

1 In View Administrator, click **View Configuration > Transfer Server Repository**.

2 In the Contents panel, select a package file.

3 Click **Remove**.

A dialog warns you if linked-clone desktops are using the base image from which the selected package file was published. You can cancel the package removal or continue.

4 Click **OK**.

The package enters the **Pending Delete** state and is deleted.

Migrate the Transfer Server Repository to a New Location

You can migrate the Transfer Server repository to a new location if your current disk drive is running out of space.

All View Transfer Server instances that are associated with a View Connection Server must be in maintenance mode before you can migrate the Transfer Server repository.

If you have multiple View Transfer Server instances, migrate the Transfer Server repository to a network-shared drive. Other View Transfer Server instances cannot access a Transfer Server repository that is configured on a local drive on one View Transfer Server instance.

Prerequisites

- Verify that View Transfer Server is installed and configured. See "Add View Transfer Server to View Manager," on page 248.
- Do not publish packages in the Transfer Server repository while you migrate the repository. If a package is published in the current repository after you start copying the repository files to the new location, the package might not be copied to the new location.

  To enforce this prerequisite, you could put View Transfer Server in maintenance mode before you manually copy the repository, but that approach would extend the downtime for data transfers while the repository files are copied.

  Instead, this procedure directs you to copy the repository files before you put View Transfer Server in maintenance mode. This approach minimizes the time that View Transfer Server is unavailable.

Procedure

1 Configure a local or remote destination folder to which you will migrate the Transfer Server repository.

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

2 Manually copy the Transfer Server repository root directory to the destination location.

You must copy the entire root directory, not only the package files that reside under the root directory.

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

4 Put all View Transfer Server instances into maintenance mode.

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

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

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

c Repeat these steps for each instance.

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

5 In the Transfer Servers panel, click the Transfer Server repository path.

For example: `C:\TransferRepository`.

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

7 Type the destination Transfer Server repository location and other information.

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

8 Click **OK**.

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

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

10 (Optional) Manually delete the package files from the original Transfer Server repository folder.

Recover from a Corrupted Transfer Server Repository Folder

If the network-shared folder or local folder on which the Transfer Server repository is configured becomes corrupted, you must recreate the Transfer Server repository on a functioning folder.

This situation occurs if the network share or local drive is inaccessible and you cannot access the Transfer Server package files that are stored in the configured folder. In this case, you cannot manually copy the package files from the corrupted folder to a new one.

Prerequisites

- Familiarize yourself with configuring a Transfer Server repository. See "Configure the Transfer Server Repository," on page 253.
- Familiarize yourself with removing and adding View Transfer Server in View Manager and placing View Transfer Server in maintenance mode. See "Managing View Transfer Server," on page 247.
- Familiarize yourself with publishing and deleting packages in the Transfer Server repository. See "Publish Package Files in the Transfer Server Repository," on page 254 and "Delete a Package File from the Transfer Server Repository," on page 255.

Procedure

1 Remove all instances of View Transfer Server from View Manager.

  When all instances of View Transfer Server are removed, View Manager deletes the Transfer Server repository configuration, including the path and related information.

2 Configure a new path and folder for a network share or local drive.

  Follow the same procedure you use when you create a new Transfer Server repository.

3 Add the View Transfer Server instances to View Manager.

4 Place the View Transfer Server instances in maintenance mode.

5 Configure the Transfer Server repository in View Manager, specifying the new network share or local path.

  View Transfer Server validates the new Transfer Server repository path. The status of each package is **Missing Package**.

6 Return each View Transfer Server instance to a **Ready** state by exiting maintenance mode.

7 Delete the displaced packages from the Transfer Server repository.

8 Republish the packages to the Transfer Server repository.

  Use the original parent virtual machines and snapshots to publish the View Composer base images as packages in the repository.

Managing Data Transfers

You can set policies to configure replications and optimize transfer operations. You can also initiate replication requests between scheduled replications. If necessary, you can roll back a desktop to discard the locally checked out version.

Replications occur in sequence to preserve the integrity of local desktop data.

Each replication transfers data from a snapshot that is taken of the local desktop when the replication starts. Therefore, each replication represents a different state of the local desktop.

When you initiate a replication, or when a replication is scheduled to begin, the request starts the next time the client computer contacts the datacenter. View Client with Local Mode takes a snapshot and starts the replication.

View maintains only one pending replication at a time.

NOTE At the beginning and end of each replication, the end user might notice that desktop performance is affected for a few seconds while a local snapshot is taken or updated.

- Set Replication Policies on page 258

  Replication synchronizes local desktops with their corresponding remote desktops by sending user-generated changes to the datacenter. You can set policies to configure replication frequency, to allow users to defer replications, and to select the type of linked-clone disk to replicate.

- Initiate Replications of Local Desktops on page 259

  You can initiate replications for desktops that run in local mode. Your request can start a replication before the next scheduled replication. If the client policy allows it, an end user who has checked out a local desktop can also initiate a replication from within View Client.

- Roll Back a Locally Checked-Out Desktop on page 260

  If an end user loses a laptop that contains a local desktop, or if the hard disk becomes damaged, you can roll the View desktop back so that the end user can check the desktop out on another computer. If the client policy allows it, an end user who has checked out a local desktop can also roll back the desktop from within View Client.

- Delete a Local Desktop on page 260

  When you roll back a local desktop or uninstall View Client, the files that make up a local desktop on that client computer are not deleted or cleaned up. To remove a local desktop, you must manually delete its files.

Set Replication Policies

Replication synchronizes local desktops with their corresponding remote desktops by sending user-generated changes to the datacenter. You can set policies to configure replication frequency, to allow users to defer replications, and to select the type of linked-clone disk to replicate.

You configure replication features by setting local mode policies. For descriptions, see "Local Mode Policies," on page 140.

Prerequisites

Determine whether to set these policies globally, for individual desktop pools, and for individual users. For details, see "Setting Policies in View Administrator," on page 137.

Procedure

- Set the **Target replication frequency**.

  This policy specifies the interval in days, hours, or minutes between the start of one replication and the start of the next replication. You can prohibit scheduled replications by selecting **No replication**.

  The **No replication** policy does not prohibit explicit replication requests. You can initiate replications in View Administrator, and users can request replications if the **User initiated replication** policy is set to **Allow**.

  If a replication takes longer than the interval that is specified in the **Target replication frequency** policy, the next scheduled replication starts after the previous one is completed. The pending replication does not cancel the previous one.

For example, the **Target replication frequency** policy might be set to one day. A replication might start at noon on Tuesday. If the client computer is disconnected from the network, the replication might take longer than 24 hours. At noon on Wednesday, View Client with Local Mode starts the next replication request. After the previous replication is completed, View Client with Local Mode takes a snapshot and starts the pending replication.

- Set **User deferred replication**.

  This policy allows a user to pause a replication that is underway. The replication does not resume, and no new replications start, until the deferment period is over. The deferment period is two hours.

- Set **Disks replicated**.

  This policy determines whether to replicate View Composer persistent disks only, OS disks, or both OS disks and persistent disks. This policy affects linked-clone desktops only.

  This policy is set when a desktop is checked out. If you change the policy, the change takes effect after the desktop is checked out again.

- Set **User initiated replication**.

  This policy allows a user to request a replication from a local desktop.

Initiate Replications of Local Desktops

You can initiate replications for desktops that run in local mode. Your request can start a replication before the next scheduled replication. If the client policy allows it, an end user who has checked out a local desktop can also initiate a replication from within View Client.

If you initiate a replication while View Client with Local Mode is already replicating data, your replication starts after the previous replication is completed. Your pending request does not abort the previous replication.

Procedure

1 In View Administrator, click **Monitoring > Local Sessions**.

2 Select local desktops.

3 Click **Initiate Replication**.

4 Choose whether to start the replication at the next connection between the local desktop and the datacenter.

Option	Description
Yes	Starts the replication the next time View Client is running and the desktop contacts the datacenter.
No	Cancels your replication request. If you requested a replication previously and it has not started yet, you can select **No** to cancel the pending replication.

5 Click **OK**.

The replication starts the next time View Client is running and the client computer contacts the datacenter. If a replication is already active, your replication starts when the previous replication is completed.

What to do next

If you initiated the replication because you need to have the desktop checked back in without end-user interaction, you can roll back the local desktop after the replication is complete. See "Roll Back a Locally Checked-Out Desktop," on page 260.

Roll Back a Locally Checked-Out Desktop

If an end user loses a laptop that contains a local desktop, or if the hard disk becomes damaged, you can roll the View desktop back so that the end user can check the desktop out on another computer. If the client policy allows it, an end user who has checked out a local desktop can also roll back the desktop from within View Client.

If an administrator starts a rollback operation, the client takes one of the following actions:

- If the user is logged in to the checked out desktop, the session is terminated as soon as View Client receives notification. The user can no longer log in to the checked-out desktop.
- If the user is not logged in, subsequent attempts to connect are redirected to the online copy of the desktop. To continue working in local mode, the user must now check out the desktop from the server.

Prerequisites

If an administrator wants to retain most recent data from the local desktop, perform a replication operation. See "Initiate Replications of Local Desktops," on page 259.

IMPORTANT If you perform a replication, you must wait until the replication is complete before initiating a rollback operation. Rollback operations are not queued behind other operations. To determine when a replication operation is complete, in View Administrator, click **Monitoring > Local Sessions** and note the time that the last replication completed.

Procedure

- Select the **Rollback** option.

Option	Action
View Administrator user	In View Administrator, select **Monitoring > Local Sessions**, select the desktop, and click **Rollback**.
End user	If you are a user who is entitled to the desktop, in View Client, right-click the desktop in the list of available desktops and select **Rollback**. The **Rollback** option is available only if the client desktop policy allows it.

The checked out version of the desktop is discarded. A user must check out the online version again to use the desktop in local mode.

What to do next

To clean up the files on the end user's computer, have the end user delete the local mode directory for this desktop. See "Delete a Local Desktop," on page 260.

For information about checking out a View desktop for use in local mode, see the *View Installation* document.

Delete a Local Desktop

When you roll back a local desktop or uninstall View Client, the files that make up a local desktop on that client computer are not deleted or cleaned up. To remove a local desktop, you must manually delete its files.

Prerequisites

Verify that the local desktop is no longer checked out. If the local desktop contains data that has not been replicated to the View desktop that resides in the datacenter, ask the end user to check in the desktop. If checking the desktop in is not possible, use View Administrator to replicate the data. See "Initiate Replications of Local Desktops," on page 259.

Procedure

- On the client computer, select and delete the folder that contains the files that make up the local desktop that you want to delete.

  The folder resides in the local desktop check-out directory. When you downloaded your first local desktop, if you did not click **Options** and change the directory where the local desktops are stored, they are stored in the default check-out directory.

Desktop Operating System	Default Check-Out Directory
Default directory on Windows 7 and Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Default directory on Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*

  The `AppData` directory in Windows 7 operating systems is a hidden folder. You might need to show this hidden folder to navigate to the local desktop files.

Configure Security and Optimization for Local Desktop Operations

You can configure tunneled communications and SSL encryption for local desktop operations. You can also optimize data transfers between the local computers and the datacenter.

These settings are specific to a single View Connection Server instance. You might want to enable these settings on an instance that services local desktop users who connect from the Internet, but disable the settings on an instance that is dedicated to internal users who do not use local desktops.

Prerequisites

- Familiarize yourself with the SSL and tunneled-communications settings for local desktop operations. See "Setting Security Options for Local Desktop Operations," on page 262.
- Familiarize yourself with using deduplication and compression to optimize data transfers over the network. See "Optimizing Data Transfers Between Local-Desktop Host Computers and the Datacenter," on page 261.

Procedure

1. In View Administrator, click **View Configuration > Servers**.
2. In the View Servers panel, select a View Connection Server instance and click **Edit**.
3. Select security and optimization settings for data transfers and local desktop operations.

Optimizing Data Transfers Between Local-Desktop Host Computers and the Datacenter

You can reduce the amount of data that is sent over the network during transfer operations between the client computers that host local desktops and the datacenter. You use deduplication and compression to optimize data transfers.

Table 14-3 shows the deduplication and compression settings for data transfers.

Transfer operations include checking in and checking out desktops, replicating data from local desktops to the datacenter, and downloading system images to local desktops.

You can determine the impact of deduplication and compression on data transfers by reading the View Client with Local Mode logs. See "Determining the Effects of Deduplication and Compression on Data Transfers," on page 264.

Table 14-3. Deduplication and Compression Settings for Data Transfers

Setting	Description
Use deduplication for Local Mode operations	Prevents redundant data from being sent from client computers to the datacenter. Deduplication operates on transfers from the client computer to the datacenter, including replications and desktop check-ins. Deduplication does not take place when desktops are checked out. With deduplication, the client computer detects identical blocks of data and sends a reference to the original block instead of sending the entire block again. Deduplication is valuable on slow networks because it saves network bandwidth. However, deduplication can add to the CPU workload on the client computer when it checks for identical data blocks and to the I/O workload on View Transfer Server when it reads duplicate blocks from disk. On fast networks, it might be more efficient to disable deduplication. The default is not to use deduplication.
Use compression for Local Mode operations	Compresses system-image and desktop files before sending them over the network. Like deduplication, compression saves bandwidth and speeds up transfers over slow networks. However, View Transfer Server uses additional computing resources to compress files. When you decide whether to use compression, you must weigh the benefits in network performance against the cost in server computing. The default is not to use compression.

Setting Security Options for Local Desktop Operations

You can set the level of security of transfer operations by using SSL encryption and tunneled connections between the client computers that host local desktops and the datacenter.

Table 14-4 shows the security settings for local desktop operations.

Not using SSL or tunneled connection increases data-transfer speed at the expense of secure data communication.

The SSL settings do not affect local data on the client computers, which is always encrypted.

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

Table 14-4. Using Secure, Tunneled Connection and SSL for Local Desktop Operations

Setting	Description
Use secure tunnel connection for Local Mode operations	Local desktops use tunneled communications. Network traffic is routed through View Connection Server or a security server if one is configured. If you do not use this setting, data transfers take place directly between local desktops and the corresponding remote desktops in the datacenter. The default is not to use secure tunnel connections.
Use SSL for Local Mode operations	Communications and data transfers between client computers and the datacenter use SSL encryption. These operations include checking in and checking out desktops and replicating data from client computers to the datacenter, but do not include transfers of View Composer base images. They involve connections between client computers and View Transfer Server. The default is not to use SSL.
Use SSL when provisioning desktops in Local Mode	Transfers of View Composer base-image files from the Transfer Server repository to client computers use SSL encryption. These operations involve connections between client computers and View Transfer Server. The default is not to use SSL.

Change the Local Desktop Encryption Key Cipher for New Key Generation

By default, View Connection Server uses AES-128 to encrypt the virtual disk (`.vmdk`) file when users check in and check out a local desktop. If you prefer stronger encryption, you can change the encryption key cipher to AES-192 or AES-256 by editing a global property in View LDAP on your View Connection Server host.

After you change the encryption key cipher for local desktops, the new cipher is used for new key generation, for example, when a local desktop is checked out for the first time. Previously generated keys are not changed. To change the encryption key cipher for existing local desktops, see "Change the Encryption Key Cipher for an Existing Local Desktop," on page 264.

You use the ADSI Edit utility to modify View LDAP. The ADSI Edit utility is installed with View Connection Server. When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

1 Start the ADSI Edit utility on your View Connection Server host.

2 Select or connect to **DC=vdi, DC=vmware, DC=int**.

3 On the object **CN=Common, OU=Global, OU=Properties**, set the **pae-OVDIKeyCipher** attribute to the new encryption key cipher value.

You can set the encryption key cipher value to `AES-128`, `AES-192` or `AES-256`. The default value is `AES-128`.

Change the Encryption Key Cipher for an Existing Local Desktop

To change the encryption key cipher for an existing local desktop, you edit the **pae-VM** record for the local desktop in View LDAP on your View Connection Server host.

You use the ADSI Edit utility to modify View LDAP. The ADSI Edit utility is installed with View Connection Server. When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

Prerequisites

- Change the encryption key cipher for local desktops. See "Change the Local Desktop Encryption Key Cipher for New Key Generation," on page 263.
- See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows operating system version.

Procedure

1 If the local desktop is checked out, check it in and remove any existing local files.

2 Start the ADSI Edit utility on your View Connection Server host.

3 Select or connect to **DC=vdi, DC=vmware, DC=int**.

4 In the **pae-VM** record for the local desktop, clear the values for the **pae-mVDIOfflineAuthKey**, **pae-mVDIOfflineDataKey**, and **pae-mVDIOfflineObfuscationKey** attributes.

5 Check out the local desktop.

View Connection Server generates new keys for the local desktop. The new keys have the new encryption key cipher value.

Determining the Effects of Deduplication and Compression on Data Transfers

You can determine the extent to which deduplication and compression reduce the amount of data that is sent over the network during transfer operations. You can obtain data transfer sizes by reading the View Client with Local Mode logs on the client computer.

During a check in or replication, the local desktop displays the amount of data that would be transferred to the remote desktop in the datacenter if no optimization took place. This amount does not reflect the actual data that is sent over the network. The same number appears whether or not deduplication and compression are enabled.

When both features are enabled, View Client starts by using deduplication to remove redundant data blocks from the data that will be transferred. Next, View Client either compresses the remaining data or determines that the data cannot be compressed.

Reading the View Client with Local Mode Logs

To generate log entries that show deduplication and compression statistics, you must set the logs to `Debug` mode.

Table 14-5 shows the location of the View Client with Local Mode logs on the client computer.

Table 14-5. Location of View Client with Local Mode Logs

Operating System	Path
Windows 7 and Windows Vista	`C:\Users\`*`user name`*`\AppData\VMware\VDM\Logs\`
Windows XP	`C:\Documents and Settings\`*`user name`*`\Local Settings\Application Data\VMware\VDM\Logs\`

When a local desktop is checked in or replicated, View Transfer Server transfers the data that was generated on the local desktop since the last check out or replication. You can estimate the potential size of a data transfer if you know how long the desktop has been generating new data. The following sample log entry shows the amount of time, in minutes, since the last check out or replication:

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: Total checkin size over 34 minutes:
```

Determining the Impact of Deduplication and Compression

The `GetTotalCheckinSize` log entries show the size of the transfer that is predicted before the transfer occurs. These numbers encompass all disks in the local desktop from which data is transferred.

The following sample entry shows the amount of data that will not be optimized by deduplication during a check-in operation. View predicts that this amount of data will be transferred.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: non-dedupe: 2 MB
```

In the following sample entries, the `parent-dedupe` entry shows the amount of data that will be optimized by deduplication on View Transfer Server. The `self-dedupe` entry shows the amount of deduplication on the client computer. Add the numbers in these entries to derive the total amount of data that will be optimized by deduplication.

```
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: parent-dedupe: 871 MB
2010-06-28 17:22:12,281 DEBUG <536> [wswc_localvm]
GetTotalCheckinSize: self-dedupe: 0 MB
```

The `Replication statistics` log entries show the actual amounts of data that were sent over the network. Separate statistics are generated for each local desktop disk from which data is transferred.

In the following example, the `parent-dedupe` and `self-dedupe` entries show deduplication statistics on View Transfer Server and the client computer, respectively.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Replication statistics:
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Parent dedup: 871.139 MB
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Self dedup: 0.000 MB
```

The following sample entry shows the amount of data that was compressed during a transfer operation:

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm]
Compression: 0.000 MB compressed to 0.000 MB
```

The following sample entry shows the amount of data that was not compressed.

```
2010-06-28 17:24:53,046 DEBUG <BoraThread> [wswc_localvm] Raw
data: 2.198 MB
```

In this example, the local desktop displayed a message such as "`Transferring 871MB`". However, this amount of data was reduced by deduplication. Although the remaining data could not be compressed, only 2.198MB of data was transferred over the network.

Guest File System Optimization of Data Transfers

During transfer operations, View Transfer Server reduces the amount of data that must be sent over the network by taking advantage of guest file system optimization.

When a desktop virtual machine contains a primary NTFS partition, View Transfer Server transfers the blocks that are allocated by NTFS. Unallocated blocks are not transferred. This strategy minimizes the total number of blocks to be transferred.

Guest file system optimization occurs only when data is transferred from primary NTFS partitions. View Transfer Server does not perform this optimization on extended partitions, Logical Disk Manager partitions, or compressed NTFS volumes on Windows 7 or Windows Vista virtual machines.

Guest file system optimization differs from data deduplication and compression, which also optimize data transfers but are independent of the desktop's guest operating system. For details about these operations, see "Optimizing Data Transfers Between Local-Desktop Host Computers and the Datacenter," on page 261.

Configuring Endpoint Resource Usage

By default, a View desktop that is checked out for use on a local system takes advantage of the memory and CPU capabilities of that host. The virtual NICs on the desktop use NAT to share the IP and MAC addresses of the host. You can change this default behavior.

Override Local Usage of Memory and CPU Resources

After a local desktop is checked out, it takes advantage of the memory and CPU capabilities of the local system, regardless of the memory and CPU settings specified for the virtual machine in vCenter Server. You can override this default behavior.

By default, the amount of RAM allocated to a View desktop that is checked out for use in local mode is automatically adjusted to be a certain amount of the RAM that is available on the client host.

The formula takes into consideration how much memory is available to split between the host and guest View desktop. A Windows XP operating system requires a minimum of 512MB RAM. A 32-bit Windows 7 or Windows Vista operating system requires a minimum of 1GB RAM. The amount of memory available to split is the total amount of RAM on the host minus the minimum RAM required for the host and guest operating systems.

Table 14-7. Memory Allotted to Local View Desktops

Memory Allocation	Windows XP Guests	Windows 7 and Vista Guests
Minimum	512MB	1GB
Best effort	512MB + (Available/2)	1GB + (Available/2)
Maximum	2GB	4GB

For example, if a Windows 7 host has a total of 2GB of RAM, to run a Windows 7 View desktop locally would require 2GB of RAM, with 1GB of RAM allocated to the host and 1GB of RAM allocated to the local View desktop. If the host had 3GB of RAM, 1.5GB of RAM would be allocated to the host and 1.5GB of RAM would be allocated to the local View desktop.

NOTE The automatic adjustment of memory allocation never sets the memory of the local desktop to a lower value than what is configured in vCenter Server.

Similarly, the local View desktop can use up to two CPUs available on the client host if the View desktop is running a Windows Vista or later operating system.

You can change the defaults and specify the scope of the setting. The setting can apply to all local desktops on the client or, depending on the setting, it can apply to a specific desktop or to all desktops from a specific View Connection Server instance that a specific user is entitled to use on the client.

To change these defaults, you must configure Windows registry settings. You can then use standard Windows tools such as Group Policy Objects (GPOs) to deploy these registry settings.

Prerequisites

- If you plan to set a specific number of CPUs that the local desktop can use, power off the local desktop.
- Because in many cases you can specify the scope of the setting, determine the IDs you will need to specify.

Table 14-6. Identifiers Used in Registry Settings for Local Mode Resource Usage

Scope	Variable Name	Description
Broker specific	*broker_guid*	Globally unique identifier for the View Connection Server instance or group. Use the `vdmadmin -C` command to determine the GUID. See "Setting the Name of a View Connection Server Group Using the -C Option," on page 327.
User specific	*remote_user_sid*	The security ID of the end user. Use the ADSI Edit utility on a View Connection Server host and find the value of the **pae-SIDString** field of **CN=*machine_CN*,OU=Servers,DC=vdi,DC=vmware,DC=int**.
Desktop specific	*desktop_ID*	The ID of the View desktop. Use the ADSI Edit utility on a View Connection Server. The ID is listed in **OU=Applications** of **DC=vdi,DC=vmware,DC=int**. The desktop ID is the distinguished name that uses the display name of the desktop pool: **CN=*pool_display_name*,OU=Applications,DC=vdi,DC=vmware,DC=int.**

You can also find the broker GUID in the `mvdi.lst` file on the client computer. On Windows XP, the file is located in the `C:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\VMware\VDM` folder. Open the file and search for `brokerGUID`. The remote user security ID is also listed in this file. Open the file and search for `user-sid`.

Procedure

- To override the default behavior so that the local desktop uses only the amount of memory configured in vCenter Server, create and deploy a GPO to add one of the following registry keys and set the key to 1.

Scope of Setting	Path
Client-wide	`HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup`
Broker and user specific	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\disableOfflineDesktopMemoryScaleup`

The value 1 indicates that `disableOfflineDesktopMemoryScaleup` is on, and the value 0 indicates that it is off.

- To set a specific amount of memory that the View desktop can use when running locally, create and deploy a GPO to add one of the following registry keys that specify the number in megabytes, up to 32GB.

Scope of Setting	Path
Client-wide	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid*\offlineDesktopDefaultMemoryScaleupValue
Desktop specific	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid**desktop_ID*\offlineDesktopDefaultMemoryScaleupValue

  If you set the value to a number that is too large, the local desktop does not power on, and an error message appears.

- To check out a desktop that was configured to require more memory than is available on the client host, create and deploy a GPO to add the following registry key that specifies the number of megabytes that you want the local client to report that it has available.

  HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid*\offlineDesktopReportedHostMemoryValue

  Setting this value to one that is greater than or equal to the memory required by the View desktop allows you to check out and run the View desktop if the client has enough spare memory to run the virtual machine.

  If the client does not have enough spare memory, you can use the `offlineDesktopDefaultMemoryScaleupValue` setting in conjunction with the `offlineDesktopReportedHostMemoryValue` setting.

  For example, if your client system has 2GB of memory and the View desktop is configured to require 2GB of memory, you will not be able to check out the View desktop because some memory is also required for client hosted virtualization. You can, however, use the registry setting `offlineDesktopReportedHostMemoryValue = 2048`, so that you can check out the desktop, and use the registry setting `offlineDesktopDefaultMemoryScaleupValue = 1024` so that the View desktop uses only 1GB of memory when it runs locally.

- To override the default behavior so that the local desktop uses only the number of CPUs configured in vCenter Server, create and deploy a GPO to add one of the following registry keys and set the key to 1.

Scope of Setting	Path
Client-wide	HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopCPUScaleup
Broker and user specific	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid*\disableOfflineDesktopCPUScaleup

  The value 1 indicates that `disableOfflineDesktopCPUScaleup` is on, and the value 0 indicates that it is off.

- To set a specific number of CPUs that the View desktop can use when running locally, create and deploy a GPO to add one of the following registry keys that specify the number of CPUs, up to 2.

Scope of Setting	Path
Client-wide	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid*\offlineDesktopDefaultCPUScaleupValue
Desktop specific	HKCU\Software\VMware, Inc.\VMware VDM\Client*broker_guid**remote_user_sid**desktop_ID*\offlineDesktopDefaultCPUScaleupValue

If you specify an invalid value, the value is ignored and the default is used. If you specify more CPUs than are available on the host, the local desktop does not power on, and an error message appears. If you set the value to a number higher than 2, the value 2 is used.

The settings go into effect when the local desktop is powered on, except in the case of the setting that allows the reported required memory to be less than that set on vCenter Server. That setting is read only when the desktop is checked out.

Change the Network Type from NAT to Bridged

By default, the virtual network type of a View desktop changes to NAT (network address translation) when the desktop is checked out for use on a local system. You can override this behavior to use bridged networking so that the View desktop has its own identity on the network.

With bridged networking, the virtual network adapter in the View desktop connects to the physical network adapter in the host computer. Bridged networking makes the View desktop visible to other computers on the network and requires the desktop to have its own IP address.

NAT configures a virtual machine to share the IP and MAC addresses of the host. The View desktop and the client host share a single network identity on the network.

To change these defaults for all local desktops or for specific local desktops on a client host, you must configure Windows registry settings. You can then use standard Windows tools such as Group Policy Objects (GPOs) to deploy these registry settings.

Prerequisites

- Because in many cases you can specify the scope of the setting, determine the IDs you will need to specify.

Table 14-8. Identifiers Used in Registry Settings for Local Mode Resource Usage

Scope	Variable Name	Description
Broker specific	*broker_guid*	Globally unique identifier for the View Connection Server instance or group. Use the `vdmadmin -C` command to determine the GUID. See "Setting the Name of a View Connection Server Group Using the -C Option," on page 327.
User specific	*remote_user_sid*	The security ID of the end user. Use the ADSI Edit utility on a View Connection Server host and find the value of the **pae-SIDString** field of **CN=*machine_CN*,OU=Servers,DC=vdi,DC=vmware,DC=int**.
Desktop specific	*desktop_ID*	The ID of the View desktop. Use the ADSI Edit utility on a View Connection Server. The ID is listed in **OU=Applications** of **DC=vdi,DC=vmware,DC=int**. The desktop ID is the distinguished name that uses the display name of the desktop pool: **CN=*pool_display_name*,OU=Applications,DC=vdi,DC=vmware,DC=int.**

You can also find the broker GUID in the `mvdi.lst` file on the client computer. On Windows XP, the file is located in the `C:\Documents and Settings\`*`user_name`*`\Local Settings\Application Data\VMware\VDM` folder. Open the file and search for `brokerGUID`. The remote user security ID is also listed in this file. Open the file and search for `user-sid`.

Procedure

- To override the default behavior so that the local desktop uses bridged networking, create and deploy a GPO to add one of the following registry keys and set the key to 1.

Scope of Setting	Path
Client-wide	`HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking`
Connection Server and user specific	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\offlineDesktopUseBridgedNetworking`
Desktop-specific	`HKCU\Software\VMware, Inc.\VMware VDM\Client\`*`broker_guid`*`\`*`remote_user_sid`*`\`*`desktop_ID`*`\offlineDesktopUseBridgedNetworking`

  A value of 1 sets the desktop to use bridged networking. A value of 0 sets it to use NAT, which is the default.

The setting takes effect when the end user powers on the local desktop.

Configuring an HTTP Cache to Provision Local Desktops Over a WAN

You can use an HTTP cache to facilitate the provisioning of linked-clone, local desktops. Configuring an HTTP cache benefits remote offices and branch offices that are connected to the datacenter over a WAN. The HTTP cache reduces the performance cost of transferring View Composer base images over a WAN.

If you configure linked-clone desktops to use local mode at remote offices, your WAN might not have the bandwidth to efficiently download the View Composer base image directly to each local computer. For example, repeatedly transferring a 6GB base image might be prohibitive.

If you set up an HTTP cache, the base image is stored in the proxy server's cache when the first user checks out a desktop. When subsequent users check out desktops, the base image is transferred over the LAN within the local office.

To complete a check-out operation, View Transfer Server still must transfer each user's linked-clone OS disk and persistent disk from the datacenter over the WAN, but these disks are a fraction of the size of the base image.

1 Configure View Connection Server to Support HTTP Caching of View Composer Base Images on page 271

  To allow a caching proxy server to pass on View Composer base images and other data between local desktops and the datacenter, you must configure certain settings in View Connection Server.

2 Limit the Size of Base-Image Package Files to Allow Caching on page 271

  A View Composer base-image package can contain files that are larger than a gigabyte, too large for many proxy servers to cache. You can configure View Transfer Server to split base-image packages into files that are no larger than the capacity of the proxy-server cache.

3 Configure Client Computers to Transfer Data Through a Proxy Server on page 272

  To support HTTP caching, you must configure the client computers that host local desktops to transfer the desktop data through a caching proxy server. You also must configure the client computers to use the proxy server's HTTP address for internet connections.

4 Configure a Proxy Server to Cache View Composer Base Images on page 273

  When you set up a proxy server to support HTTP caching for local desktops, you must configure the capacity of the cache and the HTTP connection method.

Configure View Connection Server to Support HTTP Caching of View Composer Base Images

To allow a caching proxy server to pass on View Composer base images and other data between local desktops and the datacenter, you must configure certain settings in View Connection Server.

You use two separate View settings to configure SSL encryption for the following two types of data:

- View Composer base images
- Other linked-clone desktop data, including OS disks and persistent disks

You must disable SSL encryption of transfers of base-image package files from the Transfer Server repository to local computers. Disabling SSL allows the proxy server to access and cache the package-file contents. Disabling SSL does not expose the base-image data. The data is encrypted when you publish the base image to the Transfer Server repository and remains encrypted when it is downloaded to the proxy server over the WAN.

You can choose whether to use SSL encryption of transfers of all other local-desktop data. To permit other local-desktop data to pass through the caching proxy server, you must configure the proxy server to allow the use of the HTTP CONNECT method or you must enable SSL encryption of local-mode operations on View Connection Server.

If you use SSL encryption, you do not have to change proxy server settings, but SSL encryption can affect the performance of transfers of linked-clone OS disks and persistent disks.

You must configure these SSL settings on each View Connection Server instance that delivers View services to the clients for which you configure HTTP caching.

Procedure

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

2 In the View Servers panel, select a View Connection Server instance and click **Edit**.

3 Deselect **Use SSL when provisioning desktops in local mode**.

This setting disables SSL for downloading base-image package files from the Transfer Server repository to local computers.

4 If you do not set the caching proxy server to use the HTTP CONNECT method, select **Use SSL for Local Mode operations**.

This setting affects transfers of all other local-desktop data.

Limit the Size of Base-Image Package Files to Allow Caching

A View Composer base-image package can contain files that are larger than a gigabyte, too large for many proxy servers to cache. You can configure View Transfer Server to split base-image packages into files that are no larger than the capacity of the proxy-server cache.

When you publish a package in the Transfer Server repository, View Transfer Server creates package files of the specified size. You must configure the size limit before you begin publishing packages to the repository. View Transfer Server does not split existing package files to conform to the size limit.

You can set this value on any View Connection Server instance in a replicated group. When you change View LDAP, the change is propagated to all the replicated View Connection Server instances.

Prerequisites

Familiarize yourself with using the `vdmadmin` command with the `–T` option. See "Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option," on page 344.

Procedure

1 Start a Windows command prompt on your View Connection Server computer.

2 Type the `vdmadmin` command with the –T option.

```
vdmadmin –T [–packagelimit size_in_bytes]
```

By default, the path to the `vdmadmin` command executable file is `C:\Program Files\VMware\VMware View\Server\tools\bin`.

Example: Setting a Package File Size Limit

Set the package-file split limit to 100MB.

```
vdmadmin –T –packagelimit 104857600
```

Display the current package-file split limit.

```
vdmadmin –T
```

Configure Client Computers to Transfer Data Through a Proxy Server

To support HTTP caching, you must configure the client computers that host local desktops to transfer the desktop data through a caching proxy server. You also must configure the client computers to use the proxy server's HTTP address for internet connections.

To allow transfers to pass through a proxy server, you add a registry key to the client computers. You can create a group policy in Active Directory to set this registry key on multiple computers in a domain.

Procedure

1 Start the Windows Registry Editor on the local mode client system.

2 In the left pane, expand the registry path.

Processor	Description
64-bit	`HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM`
32-bit	`HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM`

3 Click **Edit > New > String Value** and type **`useProxyForTransfer`** in the new value entry.

4 Right-click the **useProxyForTransfer** entry, click **Modify**, type **`true`**, and click **OK**.

The entry is added to the registry.

5 Exit the Windows Registry Editor.

6 On the client computer, configure the Internet Explorer connection settings to use your caching proxy server.

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

b Click the **Connections** tab and click **LAN Settings**.

c Click **Use a proxy server for your LAN** and click **Advanced**.

d Type the proxy addresses and port numbers for the HTTP, Secure, FTP, and Socks connections and click **OK**.

Configure a Proxy Server to Cache View Composer Base Images

When you set up a proxy server to support HTTP caching for local desktops, you must configure the capacity of the cache and the HTTP connection method.

Prerequisites

- Verify the size limit of base-image package files that you set with the `vdmadmin -T` command. See "Limit the Size of Base-Image Package Files to Allow Caching," on page 271.
- Determine whether you use SSL for local mode operations. See "Configure View Connection Server to Support HTTP Caching of View Composer Base Images," on page 271.

Procedure

1 Configure the maximum size of the cache on the proxy server.

   To calculate the maximum size, consider the number and size of the View Composer base images that are used by local desktops. The base images are downloaded as package files to the proxy server. Also consider other files that you plan to cache on the proxy server.

2 Configure the size of the largest single file that can be cached.

   The single-file maximum size on the proxy server must be at least as large as the maximum package-file size that you set with the `vdmadmin -T` command.

3 If you do not enable the **Use SSL for Local Mode operations** setting for View Connection Server, set the access control list (ACL) on the proxy server to open port 80 and allow the CONNECT method to connect to port 80.

   View Transfer Server uses the CONNECT method to provide a tunnel connection through the proxy server. View Transfer Server uses this connection to transfer files and data other than View Composer base images between local desktops and the datacenter. Using port 80 enhances transfer performance.

Configuring the Heartbeat Interval for Local Desktop Client Computers

Client computers that host local desktops send heartbeat messages to View Connection Server at regular intervals to read the status of their checked-out desktops. The default heartbeat interval for all client computers is five minutes. You can change the heartbeat interval for all client computers. You can also set a different heartbeat interval for a specific client computer.

- Change the Heartbeat Interval for All Local Desktop Client Computers on page 273

  To change the heartbeat interval for all client computers that host local desktops, you use the ADSI Edit utility to edit View LDAP on your View Connection Server host. The ADSI Edit utility is installed with View Connection Server.

- Set the Heartbeat Interval for a Specific Local Desktop Client Computer on page 274

  To set the heartbeat interval for a specific client computer that hosts a local desktop, you use the Windows Registry Editor to edit the system registry on that computer.

Change the Heartbeat Interval for All Local Desktop Client Computers

To change the heartbeat interval for all client computers that host local desktops, you use the ADSI Edit utility to edit View LDAP on your View Connection Server host. The ADSI Edit utility is installed with View Connection Server.

When you change View LDAP on a View Connection Server instance, the change is propagated to all replicated View Connection Server instances.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the ADSI Edit utility on your Windows Server operating system version.

Procedure

1 Start the ADSI Edit utility on your View Connection Server host.

2 Select or connect to **DC=vdi, DC=vmware, DC=int**.

3 On the object **CN=Common, OU=Global, OU=Properties**, set the **pae-mVDIOfflineUpdateFrequency** attribute to the new heartbeat interval in minutes.

You must type a positive integer. By default, this attribute is not set. When it is not set, the default value is five minutes.

The new heartbeat interval takes effect the next time a client computer that hosts a local desktop sends a heartbeat message to View Connection Server. You do not need to restart the View Connection Server service or the client computer.

If the heartbeat interval is set to a lesser value on a client computer, View uses the client computer value instead of the View Connection Server value. By default, the heartbeat interval is not set on client computers.

Set the Heartbeat Interval for a Specific Local Desktop Client Computer

To set the heartbeat interval for a specific client computer that hosts a local desktop, you use the Windows Registry Editor to edit the system registry on that computer.

View does not use the heartbeat interval set on the client computer if the value is greater than the heartbeat interval set on the View Connection Server host. View always uses the lesser of the two values. The default View Connection Server heartbeat interval is five minutes.

Prerequisites

See the Microsoft TechNet Web site for information on how to use the Windows Registry Editor on the local mode client system's Windows operating system version.

Procedure

1 Start the Windows Registry Editor on the local desktop client computer.

2 Add a new registry key called **policyUpdateFrequency**.

The system registry location depends on client computer's processor type.

Option	Action
64-bit	Add **policyUpdateFrequency** to `HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM`.
32-bit	Add **policyUpdateFrequency** to `HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM`.

3 Set the **policyUpdateFrequency** key value to the new heartbeat interval in milliseconds.

You must type a positive integer.

Manually Downloading a Local Desktop to a Location with Poor Network Connections

For users on a network that has extremely low bandwidth, checking out a desktop can be prohibitive because you must download several gigabytes of data. To serve these users, you can download the desktop files manually and copy the files to the client computers.

For example, a user might work at home in a rural location with a dial-up network connection. The user might never go to the main office, where the desktop could be checked out to the user's laptop over the LAN.

In this case, you can manually download the desktop files to a portable device such as a USB device or DVD. After you deliver the device to the user, the user can copy the files onto a specified directory on the client computer and check out the desktop from the View datacenter.

You can take this approach only with View Composer linked-clone desktops.

- You manually download the View Composer base-image files.
- When the user checks out the desktop, the linked-clone OS-disk and persistent-disk files still must be downloaded over the network.

However, the base image contains the largest files. For example, a Windows 7 base image might be 6-10GB. The OS disk and persistent disk are a fraction of that size.

1 Copy the Base Image from the Transfer Server Repository on page 275

To download a desktop manually to a client computer to use in local mode, you must copy the View Composer base image to a portable device. The base image is published as a package in the Transfer Server repository.

2 Copy the Base-Image Files to the Client Computer on page 276

To download a desktop manually to a client computer to use in local mode, you must copy the base-image package files from a portable device to the client computer.

3 Set Permissions to Allow View to Use the Copied Package Files on page 276

To allow check-out operations to proceed for local mode, you must set permissions on the base-image package files that were copied to the check-out directory on the client computer.

4 Check Out a Desktop After Manually Copying the Base Image on page 277

After you manually copy the base image to the client computer and set permissions on the package files, you must direct the user to check out a desktop.

Copy the Base Image from the Transfer Server Repository

To download a desktop manually to a client computer to use in local mode, you must copy the View Composer base image to a portable device. The base image is published as a package in the Transfer Server repository.

Prerequisites

- Verify that you configured View Manager to deploy local desktops. See "Overview of Setting Up a Local Desktop Deployment," on page 243.
- Verify that you created a linked-clone desktop pool and published a package to the Transfer Server repository. See "Publish Package Files in the Transfer Server Repository," on page 254.

Procedure

1 In View Administrator, click **View Configuration > Transfer Server Repository**.

2 In the Contents pane, select the package that is associated with desktop pool from which you will check out a desktop and click **Details**.

3 Verify that the desktop pool is associated with this package.

4 Locate the Repository path, including the package ID.

For example: `\\mycomputer.com\ImageRepository\Published\f222434a-e52a-4ce3-92d1-c14122fca996`

5 Copy the package contents from the Transfer Server repository to the portable device.

You must copy the entire package directory to the portable device.

Copy the Base-Image Files to the Client Computer

To download a desktop manually to a client computer to use in local mode, you must copy the base-image package files from a portable device to the client computer.

Prerequisites

- Verify that the user installed View Client with Local Mode on the client computer.
- Verify that you copied the package files to a portable device. See "Copy the Base Image from the Transfer Server Repository," on page 275.

Procedure

1 Deliver the portable device that contains the desktop pool's package files to the user.

2 Copy the package files to a specified check-out directory on the client computer.

Copy the files to a subdirectory in the check-out directory that uses the display name of the desktop pool. For example, to download files from a desktop pool with the display name `LocalPool`, copy the files to *`check_out_directory`*`\LocalPool`.

Check-Out Directory	Description
Default directory on Windows 7 and Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Default directory on Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*
Custom directory	You can specify your own directory. For example, to download files from a desktop pool with the display name `LocalPool`, you might create this path: `C:\CheckOutDirectory\LocalPool`.

Set Permissions to Allow View to Use the Copied Package Files

To allow check-out operations to proceed for local mode, you must set permissions on the base-image package files that were copied to the check-out directory on the client computer.

You must remove the read-only attribute on the package files and give the user **Full control** privilege on the directory and all the files it contains.

This example describes how to set permissions on a Windows 7 computer. On other operating systems, you might take slightly different steps.

Prerequisites

Verify that you copied the package files to a directory on the client computer. See "Copy the Base-Image Files to the Client Computer," on page 276.

Procedure

1 Log in to the Windows 7 guest operating system, click the **Libraries** icon, and navigate to the check-out directory.

2 Right-click the check-out directory and click **Properties**.

3 Click the **Security** tab and click **Edit**.

4 In the Group or user names list, select the name of the user who will check out the desktop.

If the user name is not in the list, click **Add** and add the user name.

5 Check **Full control** in the **Allow** column and click **OK**.

6 Click the **General** tab and deselect **Read-only (Only applies to files in folder)**.

Make sure that the check box is fully deselected.

7 In the Confirm Attribute Changes dialog box, make sure that **Apply changes to this folder, subfolders and files** is selected and click **OK**.

Check Out a Desktop After Manually Copying the Base Image

After you manually copy the base image to the client computer and set permissions on the package files, you must direct the user to check out a desktop.

Prerequisites

- Verify that View Client with Local Mode is installed on the client computer.
- Verify that you set permissions to use the package files that were copied to the client computer. See "Set Permissions to Allow View to Use the Copied Package Files," on page 276.

Procedure

1 On the client computer, start Vmware View Client, connect to View Connection Server, log in to View Connection Server, and select a desktop pool.

2 Click the down-arrow button next to the desktop pool and click **Check out**.

3 (Optional) If you copied the package files to a custom directory, configure View Client to check out the desktop into the custom directory.

a In the Check Out dialog, click **Options**.

b Next to Check-out directory, click **Browse** and select the directory that contains the pool-name folder.

Do not select the pool-name folder itself.

For example, if you copied package files for a pool with a display name `LocalPool` into a directory named `C:\CheckOutDirectory\LocalPool`, select the `C:\CheckOutDirectory` directory.

c Click **OK**.

4 In the Check-out dialog, click **OK**.

View Manager checks out the desktop. View Transfer Server detects that the base-image files reside on the client computer and downloads only the remaining desktop files. These files include the OS disk and a persistent disk, if one is configured.

Troubleshooting View Transfer Server and Local Desktop Operations

Troubleshooting tips are available for common View Transfer Server and local desktop operations.

- Check-Out Fails with "No Available Transfer Server" Error on page 278

  When users try to check out desktops, the operations fail and an error message, `No available Transfer Server`, is displayed.

Check-Out Fails with "No Available Transfer Server" Error

When users try to check out desktops, the operations fail and an error message, `No available Transfer Server`, is displayed.

Problem

The check-out can fail when the operation is approximately 10% complete, before View Transfer Server begins transferring data to the client computer. The check-out can also fail later in the process. For example, the base image might be transferred to the client computer, but other virtual machine disks cannot be transferred.

This problem occurs with all check-out operations that are managed by a particular View Transfer Server instance.

Cause

This problem can occur because View Transfer Server is running on an ESX host that does not have access to the datastores where the desktops reside. During a check-out operation, View Transfer Server transfers desktop data from the datastores to the client computer. The datastores must be accessible from the ESX host where the View Transfer Server virtual machine is running.

Solution

- Migrate the View Transfer Server virtual machine to an ESX host with access to the datastores.
  a In View Administrator, place the View Transfer Server instance in maintenance mode.
  b In vSphere Client, use the Migration wizard to migrate the View Transfer Server virtual machine to the destination ESX host.
  c In View Administrator, select the View Transfer Server instance and exit maintenance mode.
- If you cannot migrate the View Transfer Server virtual machine, recreate View Transfer Server on another virtual machine on an ESX host with access to the datastores.
  a In View Administrator, remove the View Transfer Server instance from View Manager.
  b In vSphere Client, uninstall View Transfer Server or remove the View Transfer Server virtual machine.
  c Create a new virtual machine on the destination ESX host.
  d Install View Transfer Server on the virtual machine.
  e In View Administrator, add View Transfer Server to View Manager.

  For more information about installing View Transfer Server, see the *VMware View Installation* document.

Problems with Desktop Check-Outs After Initial Check-Out

Assuming that View Transfer Server is functioning properly, you might find that check-out problems are due to View Connection Server no longer having the encryption key for files on the local machine.

Problem

After successfully checking out a local desktop and checking it in, you check the desktop out again, but you cannot connect to the local desktop. You might see an error message such as, `Cannot access local desktop--desktop corrupted`.

Cause

If you change the encryption key cipher for a local desktop, or if you delete the desktop from its pool and create a new one, View Connection Server uses a new authentication key to generate a new configuration file.

When end users attempt to check out the desktop again, only changed files are downloaded. The new files that get downloaded use a new encryption key, but the old files already on the local machine use the old encryption key, which View Connection Server no longer has.

Solution

- End users must delete all local desktop files before checking the desktop out again.

  The folder resides in the local desktop check-out directory. When you downloaded your first local desktop, if you did not click **Options** and change the directory where the local desktops are stored, they are stored in the default check-out directory.

Desktop Operating System	Default Check-Out Directory
Default directory on Windows 7 and Windows Vista	`C:\Users\`*`User Name`*`\AppData\Local\VMware\VDM\Local Desktops\`*`pool_display_name`*
Default directory on Windows XP	`C:\Documents and Settings\`*`User Name`*`\Local Settings\Application Data\VMware\VDM\Local Desktops\`*`pool_display_name`*

Login Window Takes a Long Time to Appear

Under certain circumstances, after you open View Client and specify a View Connection Server instance, the login window does not appear for 30 or more seconds.

Problem

The login window is not accessible for sometimes as long as 30 seconds, until the connection attempt times out.

Cause

If View Client uses an IP address for View Connection Server, this problem occurs if you have a network connection but View Connection Server is not reachable. For example, you might see this problem if you attempt to log in to a local desktop from home when you have an Internet connection but do not have a VPN connection that would allow access to View Connection Server.

If View Client uses a host name rather than an IP address, on a local area network (LAN), this problem means that View Connection Server, or a proxy if you use a proxy, is down or a firewall is blocking the connection. On a wide area network (WAN) this problem could mean the same thing or it could mean that the host name is resolvable on public DNS but the server is not meant to be accessible from the WAN.

Solution

You must wait for the connection attempt to time out. The login window appears eventually.

View Transfer Server Remains in a Pending State

View Transfer Server is unavailable while it remains in a Pending state for an excessively long time. For example, the Pending state might last longer than ten minutes.

Problem

After you add View Transfer Server to View Manager, the View Transfer Server status does not change to a Ready state.

Cause

A common cause is that View Connection Server cannot connect to View Transfer Server.

Solution

- Verify that View Transfer Server is installed on the virtual machine.

- Verify that the View Transfer Server services are running.
  a On the View Transfer Server virtual machine, open the **Control Panel > Administrative Tools > Services** dialog box.
  b Make sure that the VMware View Transfer Server Service, VMware View Transfer Server Control Service, and VMware View Framework Component services are started.
- Verify that the View Transfer Server virtual machine can resolve the View Connection Server host name.
- Verify that the View Connection Server machine can ping the View Transfer Server IP address.
- Verify that the View Transfer Server virtual machine satisfies the recommended system configuration. See the View Transfer Server system requirements in the *VMware View Installation* document.

View Transfer Server Fails to Enter Maintenance Mode

When you attempt to place View Transfer Server in maintenance mode, it remains in the Maintenance mode pending state for an excessively long time.

Problem

When View Transfer Server is in the Maintenance mode pending state, you cannot perform operations such as migrating the Transfer Server repository to a new location, which you can do after View Transfer Server enters maintenance mode.

Cause

Active transfer operations or package publish operations to the Transfer Server repository are still underway.

Solution

Wait for active data transfers and publish operations to be completed. When all operations are completed, View Transfer Server enters maintenance mode.

The Transfer Server Repository Is Invalid

In View Administrator, View Transfer Server displays a status of Bad Transfer Server repository.

Problem

You cannot perform transfer operations for linked-clone desktops or publish packages while View Transfer Server is in this state.

Cause

The Transfer Server repository that View Transfer Server is configured to connect to differs from the Transfer Server repository that is currently configured in View Connection Server.

An invalid Transfer Server repository migration can cause View Transfer Server to enter this state.

Solution

Migrate the Transfer Server repository to a new location again. For instructions, see "Migrate the Transfer Server Repository to a New Location," on page 255.

View Transfer Server Cannot Connect to the Transfer Server Repository

In View Administrator, View Transfer Server displays a status of Repository Connection Error.

Problem

View Transfer Server cannot connect to the Transfer Server repository that is configured in View Connection Server.

Cause

The Transfer Server repository configuration is invalid. If the repository is configured on a network share, the network path or credentials are invalid. If the repository is local, the filesystem path is invalid.

Solution

1 Place all View Transfer Server instances in maintenance mode.

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

   b Select a View Transfer Server instance.

   c If transfers are currently active, choose whether to cancel the active transfers or wait until the active transfers are completed before placing the View Transfer Server instance in maintenance mode.

   d Click **OK**.

   e Repeat these steps for all View Transfer Server instances.

2 In View Administrator, click **View Configuration > Transfer Server Repository**.

3 Click **Edit** and configure the Transfer Server repository again.

   View Transfer Server verifies that the Transfer Server repository is valid.

View Transfer Server Fails the Health Check

In View Administrator, View Transfer Server displays a status of Bad Health Check. The View Administrator dashboard displays View Transfer Server with a red down arrow.

Problem

In a Bad Health Check state, View Transfer Server cannot function properly. You cannot perform transfer operations or publish packages in the Transfer Server repository.

Cause

View Transfer Server is not available, not running, or not functioning properly.

Solution

- Verify that View Transfer Server is installed on the virtual machine.
- Verify that the View Transfer Server services are running.

   a On the View Transfer Server virtual machine, open the **Control Panel > Administrative Tools > Services** dialog box.

   b Make sure that the VMware View Transfer Server Service, VMware View Transfer Server Control Service, and VMware View Framework Component services are started.
- Verify that the View Transfer Server virtual machine can resolve the View Connection Server host name.
- Verify that the View Connection Server machine can ping the View Transfer Server IP address.
- Verify that the View Transfer Server virtual machine satisfies the recommended system configuration. See the View Transfer Server system requirements in the *VMware View Installation Guide*.

The Transfer Server Repository Is Missing

In View Administrator, View Transfer Server displays a status of No Transfer Server Repository Configured.

Problem

You cannot perform transfer operations for linked-clone desktops or publish packages in the Transfer Server repository.

Cause

The Transfer Server repository is not configured in View Manager.

Solution

1 Place all View Transfer Server instances in maintenance mode.

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

   b Select a View Transfer Server instance.

   c If transfers are currently active, choose whether to cancel the active transfers or wait until the active transfers are completed before placing the View Transfer Server instance in maintenance mode.

   d Click **OK**.

   e Repeat these steps for all View Transfer Server instances.

2 In View Administrator, click **View Configuration > Transfer Server Repository**.

3 Click **Edit** and configure the Transfer Server repository.

   View Transfer Server verifies that the Transfer Server repository is valid.

View Transfer Server Instances Have Conflicting Transfer Server Repositories

In View Administrator, View Transfer Server instances display a status of Transfer Server Repository Conflict.

Problem

You cannot perform transfer operations for linked-clone desktops or publish packages in the Transfer Server repository.

Cause

Multiple View Transfer Server instances are configured to connect to different Transfer Server repositories.

This state can occur if, at the same time, multiple View Transfer Server instances are added to View Manager, and each instance is configured with a different Transfer Server repository.

Solution

Remove the View Transfer Server instances from View Manager and add them one at a time. If a View Transfer Server instance displays a status of Bad Transfer Server Repository, see the troubleshooting information in "The Transfer Server Repository Is Invalid," on page 281.

The View Transfer Server Web Service Is Down

In View Administrator, View Transfer Server displays a status of Web Server Down.

Problem

View Transfer Server cannot download packages from the Transfer Server repository and cannot transfer other desktop data to local desktops.

Cause

The Apache2.2 Web service that supports the Transfer Server repository is not running.

Solution

1 On the View Transfer Server virtual machine, open the **Control Panel > Administrative Tools > Services** dialog box.

2 Start the Apache2.2 service.

Virtual Disk of a Local Desktop Needs Repair

You might need to repair the virtual disk of a local desktop.

Problem

You see an error message when you try to connect to your local desktop. For example:

```
Cannot open the disk 'C:\Documents and Settings\jo\Local Settings\Application Data\View\Local
Desktops\Win7_32b_Local_Mode\52411f5e05b854ca-b5c54521f6010b22-scsi00-000002.vmdk' or one of the
snapshot disks it depends on.

Reason: The specified disk needs repair.
```

Cause

The problem can occur if you disconnect or power off the client computer while the virtual machine image is being updated.

Solution

1 Start View Client from the command line specifying the `-repairLocalDesktops` option.

For example:

```
wswc -desktopName lmdt01 -userName jo -domainName MYDOM -repairLocalDesktops
```

The repair process takes several minutes.

2 If the repair process fails, roll back the local session and check out a new local desktop.

Recover Data from a Local Desktop

VMware View secures the virtual machine of a local desktop by encrypting all of its virtual disks. If the virtual machine's checkout identifier is deleted from the configuration, or the session or policy files become corrupted, you might not be able to power on or check in the local desktop. You can decrypt the local desktop's virtual machine so that you can recover data from it.

IMPORTANT Use this procedure only if you cannot recover the data in a local desktop by any other method.

The View Connection Server instance must have access to the View LDAP configuration that holds the authentication key for the local desktop.

Depending on how much data you want to recover, you can choose to decrypt either the full virtual machine or one of its constituent disks. The decryption process is faster if you decrypt a single disk.

Prerequisites

- Verify that you cannot roll back the local desktop without data being lost.
- Verify that the data in the local desktop has not been replicated or saved in another location.
- Log in as a user in the **Administrators** role on the Windows computer on which the View Connection Server instance is installed.
- Ensure that the folder in which you intend to perform the decryption has sufficient space to store both the encrypted and decrypted virtual machine files, and that you have write permission on the folder.

Procedure

1 Copy the virtual machine files from the client machine to a local folder on the View Connection Server instance.

IMPORTANT Do not access the files using a network share or mapped drive.

2 To decrypt a file, run the `vdmadmin` command.

```
vdmadmin –V –rescue –d desktop –u domain\user –infile path_to_VM_file
```

Option	Description
–d *desktop*	Specifies the name of the desktop pool.
–infile *path_to_VM_file*	Specifies the path to the virtual machine file for the local desktop's virtual machine. To recover a full virtual machine, specify the name of the VMware virtual machine configuration file (VMX file) as the argument to the `–infile` option. To recover a single disk from a virtual machine, specify the name of the VMware virtual disk file (VMDK file) for the disk as the argument to the `–infile` option. Do not specify a VMDK file that corresponds to a disk slice.
–u *domain\user*	Specifies the domain and name of the local desktop's end user.

The `vdmadmin` command writes the decrypted virtual machine files to a subfolder named `rescued`.

Example: Decrypting Virtual Machine Files

Decrypt a full virtual machine by specifying its VMX file.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

List the files that are available for the `scsi00` disk of a local desktop's virtual machine.

```
J:\Temp\LMDT_Recovery>dir /b *scsi00*
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s001.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s002.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s003.vmdk
52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001–s004.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s001.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s002.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s003.vmdk
5215df4df635a14d–caf14c8dbbb14a3d–scsi00–s004.vmdk
```

Decrypt the current version of the `scsi00` disk by specifying its VMDK file.

```
vdmadmin –V –rescue –d lmdtpool –u MYCORP\jo –infile
"J:\Temp\LMDT_Recovery\52e52b7c26a2f683–42b945f934e0fbb2–scsi00–000001.vmdk"
```

What to do next

Use VMware Workstation to power on and examine a decrypted full virtual machine, or VMware DiskMount to mount a decrypted disk. Alternatively, examine the contents of a decrypted disk by attaching its VMDK file to a virtual machine in VMware Workstation. When you have recovered the data from the virtual machine files, roll back the local desktop.

15 Maintaining View Components

To keep your View components available and running, you can perform a variety of maintenance tasks.

This chapter includes the following topics:

Backing Up and Restoring View Configuration Data

You can back up your View Manager and View Composer configuration data by scheduling or running automatic backups in View Administrator. You can restore your View configuration by manually importing the backed-up View LDAP files and View Composer database files.

You can use the backup and restore features to preserve and migrate View configuration data.

Backing Up View Connection Server and View Composer Data

After you complete the initial configuration of View Connection Server, you should schedule regular backups of your View Manager and View Composer configuration data. You can preserve your View Manager and View Composer data by using View Administrator.

View Manager stores View Connection Server configuration data in the View LDAP repository. View Composer stores configuration data for linked-clone desktops in the View Composer database.

When you use View Administrator to perform backups, View Manager backs up the View LDAP configuration data and View Composer database. Both sets of backup files are stored in the same location. The View LDAP data is exported in LDAP data interchange format (LDIF). For a description of View LDAP, see "View LDAP Directory," on page 23.

View Manager can export configuration data from any View Connection Server instance.

If you have multiple View Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.

Do not rely on using replicated instances of View Connection Server to act as your backup mechanism. When View Manager synchronizes data in replicated instances of View Connection Server, any data lost in one instance might be lost in all members of the group.

If View Connection Server uses multiple vCenter Server instances with multiple View Composer services, View Manager backs up all the View Composer databases associated with the vCenter Server instances.

You can perform backups in several ways.

- Schedule automatic backups by using the View Manager Configuration Backup feature.
- Initiate a backup immediately by using the **Backup Now** feature in View Administrator.
- Manually export View LDAP data by using the `vdmexport` tool. This tool is provided with each instance of View Connection Server.

  NOTE The `vdmexport` tool backs up the View LDAP data only. This tool does not back up View Composer database information.

Schedule View Manager Configuration Backups

You can schedule your View Manager configuration data to be backed up at regular intervals. View Manager backs up the contents of the View LDAP repository in which your View Connection Server instances store their configuration data.

You can back up the configuration immediately by selecting the View Connection Server instance and clicking **Backup Now**.

Prerequisites

Familiarize yourself with the backup settings. See "View Manager Configuration Backup Settings," on page 289.

Procedure

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

2 Select the View Connection Server instance to be backed up and click **Edit**.

3 Specify the View Manager Configuration Backup settings to configure the backup frequency, maximum number of backups, and the folder location of the backup files.

4 Click **OK**.

View Manager Configuration Backup Settings

View Manager can back up your View Connection Server and View Composer configuration data at regular intervals. In View Administrator, you can set the frequency and other aspects of the backup operations.

Table 15-1. View Manager Configuration Backup Settings

Setting	Description
Automatic backup frequency	Every Hour. Backups take place every hour on the hour. Every 6 Hours. Backups take place at midnight, 6 am, noon, and 6 pm. Every 12 Hours. Backups take place at midnight and noon. Every Day. Backups take place every day at midnight. Every 2 Days. Backups occur at midnight on Saturday, Monday, Wednesday, and Friday. Every Week. Backups take place weekly at midnight on Saturday. Every 2 Weeks. Backups take place every other week at midnight on Saturday. Never. Backups do not take place automatically.
Max number of backups	Number of backup files that can be stored on the View Connection Server instance. The number must be an integer greater than 0. When the maximum number is reached, View Manager deletes the oldest backup file. This setting also applies to backup files that are created when you use **Backup Now**.
Folder location	Location of the backup files. The default location is on the following path on the computer where View Connection Server is running. ■ On a Windows Server 2008 computer: `C:\Programdata\VMWare\VDM\backups` ■ On a Windows Server 2003 computer: `C:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups` When you use **Backup Now**, View Manager also stores the backup files in this location.

Export Configuration Data from View Connection Server

You can back up configuration data of a View Connection Server instance by exporting the contents of its View LDAP repository.

You use the `vdmexport` command to export the data to an LDIF file. You can run the `vdmexport` command on any View Connection Server instance.

If you have multiple View Connection Server instances in a replicated group, you only need to export the data from one instance. All replicated instances contain the same configuration data.

NOTE The `vdmexport.exe` command backs up the View LDAP data only. This command does not back up View Composer database information.

Prerequisites

- Locate the `vdmexport.exe` command executable file installed with View Connection Server in the default path.

  `C:\Program Files\VMware\VMware View\Server\tools\bin`

- Log in to a View Connection Server instance as a user in the Administrators or Administrators (Read only) role.

Procedure

1 Select **Start > Command Prompt**.

2 At the command prompt, type the `vdmexport` command and redirect the output to a file.

For example:

```
vdmexport > Myexport.LDF
```

You can specify the output file name as an argument to the `-f` parameter.

For example:

```
vdmexport -f Myexport.LDF
```

The `vdmexport` command writes your View Connection Server configuration data to the specified LDIF file.

For more information about the `vdmexport` command, see the *VMware View Integration* document.

What to do next

You can use the LDIF file to maintain your configuration data in the following ways.

- Restore or transfer the configuration information of View Connection Server.
- Modify the configuration information of View Connection Server by editing the entries in the file and importing the file to the target View Connection Server instance.

For details about importing the LDIF file, see "Restoring View Connection Server and View Composer Configuration Data," on page 290.

Restoring View Connection Server and View Composer Configuration Data

You can manually restore the View Connection Server LDAP configuration files and View Composer database files that were backed up by View Manager.

You manually run separate utilities to restore View Connection Server and View Composer configuration data.

Before you restore configuration data, verify that you backed up the configuration data in View Administrator. See "Backing Up View Connection Server and View Composer Data," on page 287.

You use the `vdmimport` utility to import the View Connection Server data from the LDIF backup files to the View LDAP repository in the View Connection Server instance.

You can use the `SviConfig` utility to import the View Composer data from the `.svi` backup files to the View Composer SQL database.

Import Configuration Data into View Connection Server

You can restore configuration data of a View Connection Server instance by importing a backup copy of the data stored in an LDIF file.

You use the `vdmimport` command to import the data from the LDIF file to the View LDAP repository in the View Connection Server instance.

For information about backing up the View LDAP repository, see "Backing Up View Connection Server and View Composer Data," on page 287.

Prerequisites

- Locate the `vdmimport` command executable file installed with View Connection Server in the default path.

  ```
  C:\Program Files\VMware\VMware View\Server\tools\bin
  ```

- Log in to a View Connection Server instance as a user in the Administrators role.

Procedure

1 Select **Start > Command Prompt**.

2 At the command prompt, type the `vdmimport` command and specify an existing LDIF file as the argument to the `–f` parameter.

For example:

```
vdmimport –f Myexport.LDF
```

The `vdmimport` command updates the View LDAP repository in View Connection Server with the configuration data from the LDIF file.

For more information about the `vdmimport` command, see the *VMware View Integration* document.

Restore a View Composer Database

You can import the backup files for your View Composer configuration into the View Composer database that stores linked-clone information.

You can use the `SviConfig restoredata` command to restore View Composer database data after a system failure or to revert your View Composer configuration to an earlier state.

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

Prerequisites

Verify the location of the View Composer database backup files. By default, View Manager stores the backup files on the `C:` drive of the View Connection Server computer:

- On a Windows Server 2008 computer: `C:\Programdata\VMWare\VDM\backups`
- On a Windows Server 2003 computer: `C:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups`

View Composer backup files use a naming convention with a date stamp and an `.svi` suffix.

`Backup–`*`YearMonthDayCount–vCenter Server Name_Domain Name`*`.svi`

For example: `Backup–20090304000010–foobar_test_org.svi`

Procedure

1 Copy the View Composer backup files from the View Connection Server computer to a location that is accessible from the vCenter Server computer where View Composer service is installed.

2 On the vCenter Server computer, stop the VMware View Composer service.

3 On the vCenter Server computer, open a Windows command prompt and navigate to the `SviConfig` executable file.

The file is located with the View Composer application.

```
C:\Program Files\VMware\VMware View Composer\sviconfig.exe
```

4 Run the `SviConfig restoredata` command.

```
sviconfig –operation=restoredata
                  –DsnName=target_database_source_name_(DSN)
                  –Username=database_administrator_username
                  –Password=database_administrator_password
                  –BackupFilePath=path_to_View_Composer_backup_file
```

For example:

```
sviconfig –operation=restoredata –dsnname=LinkedClone
–username=Admin –password=Pass
–backupfilepath="C:\Program Files\VMware\VMware View
Composer\Backup–20090304000010–foobar_test_org.SVI"
```

5 Start the VMware View Composer service.

What to do next

For output result codes for the `SviConfig restoredata` command, see "Result Codes for Restoring the View Composer Database," on page 292.

Result Codes for Restoring the View Composer Database

When you restore a View Composer database, the `SviConfig restoredata` command displays a result code.

Table 15-2. Restoredata Result Codes

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

Monitor View Components

You can quickly survey the status of the View Manager and vSphere components in your View deployment by using the View Administrator dashboard.

View Administrator displays monitoring information about View Connection Server instances, the event database, security servers, View Composer services, datastores, vCenter Server instances, and domains.

NOTE View Manager cannot determine status information about Kerberos domains. View Administrator displays Kerberos domain status as unknown, even when a domain is configured and working.

Procedure

1 In View Administrator, click **Dashboard**.

2 In the System Health pane, expand **View components**, **vSphere components**, or **Other components**.

- A green up arrow indicates that a component has no problems.
- A red down arrow indicates that a component is unavailable or not functioning.

- A yellow double arrow indicates that a component is in a warning state.
- A question mark indicates that the status of a component is unknown.

3 Click a component name.

A dialog displays the name, version, status, and other component information.

Monitor Desktop Status

You can quickly survey the status of desktops in your View deployment by using the View Administrator dashboard. For example, you can display all disconnected desktops or desktops that are in maintenance mode.

Prerequisites

Familiarize yourself with the desktop states. See "Desktop Status of Virtual Machines," on page 214.

Procedure

1 In View Administrator, click **Dashboard**.

2 In the Desktop Status pane, expand a status folder.

Option	Description
Preparing	Lists the desktop states while the virtual machine is being provisioned, deleted, or in maintenance mode.
Problem Desktops	Lists the desktop error states.
Prepared for use	Lists the desktop states when the desktop is ready for use.

3 Locate the desktop status and click the hyperlinked number next to it.

The **Desktops** page displays all desktops with the selected status.

What to do next

You can click a desktop name to see details about the desktop or click the View Administrator back arrow to return to the dashboard page.

Understanding View Manager Services

The operation of View Connection Server instances and security servers depends on several services that run on the system. These systems are started and stopped automatically, but you might sometimes find it necessary to adjust the operation of these services manually.

You use the Microsoft Windows Services tool to stop or start View Manager services. If you stop View Manager services on a View Connection Server host or a security server, end users cannot log in to their desktops until you restart the services. You might also need to restart a service if it has stopped running or if the View Manager functionality that it controls appears to be unresponsive.

Stop and Start View Services

The operation of View Connection Server instances and security servers depends on several services that run on the system. You might sometimes find it necessary to stop and start these services manually when troubleshooting problems with the operation of VMware View.

When you stop View services, end users cannot log in to their desktops. You should perform such an action at a time that is already scheduled for system maintenance, or warn end users that their desktops will be unavailable temporarily.

NOTE Stop only the VMware View Connection Server service on a View Connection Server host or the VMware View Security Server service on a security server. Do not stop any other component services.

Prerequisites

Familiarize yourself with the services that run on View Connection Server hosts and security servers as described in "Services on a View Connection Server Host," on page 294 and "Services on a Security Server," on page 295.

Procedure

1 Start the Windows Services tool by entering **`services.msc`** at the command prompt.

2 Select the VMware View Connection Server service on a View Connection Server host or the VMware View Security Server service on a security server, and click **Stop**, **Restart**, or **Start** as appropriate.

3 Verify that the status of the listed service changes as expected.

Services on a View Connection Server Host

The operation of View Manager depends on several services that run on a View Connection Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

Table 15-3. View Connection Server Host Services

Service Name	Startup Type	Description
VMware View Connection Server	Automatic	Provides connection broker services. This service must be running for the correct operation of View Manager. If you start or stop this service, it also starts or stops the Framework, Message Bus, Security Gateway, and Web services. This service does not start or stop the VMwareVDMDS service or the VMware View Script Host service.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services for View Manager. This service must be running for the correct operation of View Manager.
VMware View Message Bus Component	Manual	Provides messaging services between View Manager components. This service must be running for the correct operation of View Manager.
VMware View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to View Connection Server through the PCoIP Secure Gateway.
VMware View Script Host	Automatic (if enabled)	Provides support for third-party scripts that run when you delete virtual machines. This service is disabled by default. You should enable this service if you want to run scripts.
VMware View Security Gateway Component	Manual	Provides secure tunnel services for View Manager. This service must be running for the correct operation of View Manager.

Table 15-3. View Connection Server Host Services (Continued)

Service Name	Startup Type	Description
VMware View Web Component	Manual	Provides web services for View Manager. This service must be running for the correct operation of View Manager.
VMwareVDMDS	Automatic	Provides LDAP directory services for View Manager. This service must be running for the correct operation of View Manager. This service must also be running during upgrades of VMware View to ensure that existing data is migrated correctly.

Services on a Security Server

The operation of View Manager depends on several services that run on a security server. If you want to adjust the operation of these services, you must first familiarize yourself with them.

Table 15-4. Security Server Services

Service Name	Startup Type	Description
VMware View Security Server	Automatic	Provides security server services. This service must be running for the correct operation of a security server. If you start or stop this service, it also starts or stops the Framework and Security Gateway services.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services. This service must be running for the correct operation of a security server.
VMware View PCoIP Secure Gateway	Manual	Provides PCoIP Secure Gateway services. This service must be running if clients connect to a security server through the PCoIP Secure Gateway.
VMware View Security Gateway Component	Manual	Provides secure tunnel services. This service must be running for the correct operation of a security server.

Services on a View Transfer Server Host

Transfer operations for local desktops depend on services that run on a View Transfer Server host. If you want to adjust the operation of these services, you must first familiarize yourself with them.

All of the services that are installed with View Transfer Server must be running for the correct operation of local desktops in View Manager.

Table 15-5. View Transfer Server Host Services

Service Name	Startup Type	Description
VMware View Transfer Server	Automatic	Provides services that coordinate the View Transfer Server related services. If you start or stop this service, it also starts or stops the View Transfer Server Control Service and Framework service.
VMware View Transfer Server Control Service	Manual	Provides management capabilities for View Transfer Server and handles communication with View Connection Server.
VMware View Framework Component	Manual	Provides event logging, security, and COM+ framework services for View Manager.
Apache2.2 service	Automatic	Provides data-transfer capabilities for client computers that run View desktops in local mode. The Apache2.2 service is started when you add View Transfer Server to View Manager.

Add Licenses to VMware View

If the current licenses on a system expire, or if you want to access VMware View features that are currently unlicensed, you can use View Administrator to add licenses.

You can add a license to VMware View while View Manager is running. You do not need to reboot the system, and access to desktops is not interrupted.

Prerequisites

For the successful operation of View Manager and add-on features such as View Composer and local desktops, obtain a valid license key.

Procedure

1 In View Administrator, select **View Configuration > Product licensing and usage** and click **Edit license**.

2 Enter the license serial number and click **OK**.

The Product Licensing window shows the updated licensing information.

Update General User Information from Active Directory

You can update View Manager with the current user information that is stored in Active Directory. This feature updates the name, phone, email, user name, and default Windows domain of View users. The trusted external domains are also updated.

Use this feature if you modify the list of trusted external domains in Active Directory, especially if the altered trust relationships between domains affect user permissions in View Manager.

This feature scans Active Directory for the latest user information and refreshes the View Manager configuration.

You can also use the `vdmadmin` command to update user and domain information. See "Updating Foreign Security Principals Using the -F Option," on page 328.

Procedure

1 In View Administrator, click **Users and Groups**.

2 Choose whether to update information for all users or an individual user.

Option	Action
For all users	Click **Update General User Information**. Updating all users and groups can take a long time.
For an individual user	a Click the user name to update. b Click **Update General User Information**.

Migrating View Composer with an Existing Database

In some situations, you might need to migrate a View Composer service to a new computer. You can continue to use the existing View Composer database.

For example, you might migrate a vCenter Server instance to a new ESX host or cluster to expand your deployment or recover from a hardware failure. To preserve your linked-clone desktops, you must also migrate the View Composer service installed with vCenter Server.

To migrate the View Composer service, you uninstall the service on the old computer and install the service on the new computer. For installation instructions, see the *VMware View Installation* document.

The existing View Composer database must be configured on an available computer in the same domain as the computer on which you install the new View Composer service, or on a trusted domain.

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

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

Prepare a Microsoft .NET Framework for Migrating RSA Keys

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

Prerequisites

Download the .NET Framework and read about the ASP.NET IIS registration tool from the following locations:

- http://www.microsoft.com/net
- http://msdn.microsoft.com/library/k6h9cz8h(VS.80).aspx

Procedure

1 Install the .NET Framework on the computer on which the View Composer service associated with the existing database is installed.

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

What to do next

Migrate the RSA key container to the destination computer. See "Migrate the RSA Key Container to the New View Composer Service," on page 297.

Migrate the RSA Key Container to the New View Composer Service

To use an existing View Composer database, you must migrate the RSA key container from the source computer on which the existing View Composer service resides to the vCenter Server computer on which you want to install the new View Composer service.

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

Prerequisites

Verify that the Microsoft .NET Framework and the ASP.NET IIS registration tool are installed on the source and destination computers. See "Prepare a Microsoft .NET Framework for Migrating RSA Keys," on page 297.

Procedure

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

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

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

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

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

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

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

```
aspnet_regiis –pi "SviKeyContainer" "path\keys.xml"
```

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

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

What to do next

Install the new View Composer service on the destination vCenter Server computer. For installation instructions, see the *VMware View Installation* document.

Update the Certificates on a View Connection Server Instance or Security Server

When you receive updated server SSL certificates or intermediate certificates, you import the certificates into a new keystore file and update the `locked.properties` file on each View Connection Server or security server host to use the new keystore file.

Typically, server certificates expire after 12 months. Root and intermediate certificates expire after 5 or 10 years.

When you import certificates into a keystore file, the `keytool` command creates the keystore if the specified file does not exist.

The new keystore file must have a different name from the existing keystore file. VMware recommends that you include the expiry date in the file name. For example: `keys_2014123.jks`.

You must specify a Java keystore file if you import intermediate certificates. If you do not use intermediate certificates, you can specify a PKCS#12 or PFX file instead of a Java keystore (`jks`) file.

For more information about creating a keystore file and importing server and intermediate certificates into it, see the *VMware View Installation* document.

Prerequisites

Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.

Procedure

1 If you use intermediate certificates, import the most recent update to the intermediate certificates into a new keystore file in the same directory as the existing keystore file.

For example:

```
keytool –importcert –keystore keys_20141231.jks –storepass secret –trustcacerts –alias
intermediateCA –file intermediateCA.cer
```

2 Import the most recent update to the server certificate into the new keystore file.

For example:

```
keytool –importcert –keystore keys_20141231.jks –storepass secret –keyalg "RSA" –trustcacerts
–file certificate.p7
```

3 Edit the `keyfile` and `keypass` properties in the `locked.properties` file on the View Connection Server or security server host.

   a Set the `keyfile` property to the name of the new keystore file.

   For example:

   ```
   keyfile=keys_20141231.jks
   ```

   b If the password for the keystore file has changed, set the `keypass` property to the new password.

   For example:

   ```
   keypass=NEW_PASS
   ```

4 Verify that the `storetype` property in the `locked.properties` file matches the type of the keystore file.

Option	Description
PKCS#12 or PFX file	Set the value of `storetype` to **`pkcs12`**.
Java keystore file	Set the value of `storetype` to **`jks`**.

   For example:

   ```
   storetype=jks
   ```

   You must specify the `storetype` property for a Java keystore file.

5 Restart the View Connection Server service or Security Server service to make your changes take effect.

Troubleshooting View Components 16

You can use a variety of procedures for diagnosing and fixing problems that you might encounter when using View Manager, View Composer, and View Client.

Administrators might encounter unexpected behavior when using View Manager and View Composer, and users might experience difficulty when using View Client to access their desktops. You can use troubleshooting procedures to investigate the causes of such problems and attempt to correct them yourself, or you can obtain assistance from VMware Technical Support.

This chapter includes the following topics:

Monitoring System Health

You can use the system health dashboard in View Administrator to quickly see problems that might affect the operation of View or access to desktops by end users.

The system health dashboard in the top left of the View Administrator display provides a number of links that you can use to view reports about the operation of View Manager:

Remote Sessions	Provides a link to the Global Remote Sessions screen, which displays information about the status of remote sessions.
Local Sessions	Provides a link to the Global Local Sessions View screen, which displays information about the status of local desktop sessions.
Problem Desktops	Provides a link to the Global Desktop View screen, which displays information about desktops that View Manager has flagged as having problems.
Events	Provides links to the Events screen filtered for error events and for warning events.
System Health	Provides links to the Dashboard screen, which displays summaries of the status of View components, vSphere components, domains, desktops, and datastore usage.

The system health dashboard displays a numbered link against each item. This value indicates the number of items that the linked report provides details about.

Monitor Events in View Manager

The event database stores information about events that occur in the View Connection Server host or group, View Agents, and the View Administrator, and notifies you of the number of events on the dashboard. You can examine the events in detail on the Events screen.

NOTE Events are listed in the View Administrator interface for a limited time period. After this time, the events are only available in the historical database tables. You can use Microsoft SQL Server or Oracle database reporting tools to examine events in the database tables. For more information, see the *VMware View Integration* document.

Prerequisites

Create and configure the event database as described in the *VMware View Installation* document.

Procedure

1 In View Administrator, select **Monitoring > Events**.

2 (Optional) In the Events window, you can select the time range of the events, apply filtering to the events, and sort the listed events by one or more of the columns.

View Manager Event Messages

View Manager reports events whenever the state of the system changes or it encounters a problem. You can use the information in the event messages to take the appropriate action.

Table 16-1 shows the types of events that View Manager reports.

Table 16-1. Types of Event Reported by View Manager

Event Type	Description
Audit Failure or Audit Success	Reports the failure or success of a change that an administrator or user makes to the operation or configuration of VMware View.
Error	Reports a failed operation by View Manager.
Information	Reports normal operations within VMware View.
Warning	Reports minor problems with operations or configuration settings that might lead to more serious problems over time.

You might need to take some action if you see messages that are associated with Audit Failure, Error, or Warning events. You do not need to take any action for Audit Success or Information events.

Send Messages to Desktop Users

You might sometimes need to send messages to users who are currently logged into desktops. For example, If you need to perform maintenance on a desktop, you can ask the user to log out temporarily, or warn them of a future interruption of service.

Procedure

1 In View Administrator, select **Users and Groups**.

2 Click on the user to whom you want to send a message.

3 Under the **Sessions** tab, select the user's session, and click **Send Message**.

4 Type in the message, select the message type, and click **OK**.

Display Desktops with Suspected Problems

You can display a list of the desktops whose operation View Manager has detected as being suspect.

View Administrator displays desktops that exhibit the following problems:

- Are powered on, but which are not responding.
- Remain in the provisioning state for a long time.
- Are ready, but which report that they are not accepting connections.
- Appear to be missing from a vCenter Server.
- Have active logins on the console, logins by users who are not entitled, or logins not made via a View Connection Server instance.

Procedure

1 In View Administrator, select **Desktops**.

2 Under the **VirtualCenter VMs** tab, click **Problem Desktops**.

What to do next

The action that you should take depends on the problem that View Administrator reports for a desktop.

- If a desktop is powered on, but does not respond, restart its virtual machine. If the desktop still does not respond, verify that the version of the View Agent is supported for the desktop operating system. See "Configuring Logging in View Agent Using the -A Option," on page 325.
- If a desktop remains in the provisioning state for a long time, delete its virtual machine, and clone it again. Verify that there is sufficient disk space to provision the desktop. See "Virtual Machines Are Stuck in the Provisioning State," on page 314.

- If a desktop reports that it is ready, but does not accept connections, check the firewall configuration to make sure that the display protocol (RDP or PCoIP) is not blocked. See "Connection Problems Between Desktops and View Connection Server Instances," on page 311.
- If a desktop appears to be missing from a vCenter Server, verify whether its virtual machine is configured on the expected vCenter Server, or if it has been moved to another vCenter Server.
- If a desktop has an active login, but this is not on the console, the session must be remote. If you cannot contact the logged-in users, you might need to restart the virtual machine to forcibly log out the users.

Manage Desktops and Policies for Unentitled Users

You can display the desktops that are allocated to users whose entitlement has been removed, and you can also display the policies that have been applied to unentitled users.

A user who is unentitled might have left the organization permanently, or you might have suspended their account for an extended period of time. These users are assigned a desktop but they are no longer entitled to use the desktop pool.

You can also use the `vdmadmin` command to display unentitled desktops and policies. See "Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options," on page 338.

Procedure

1 In View Administrator, select **Desktops**.

2 Select **More Commands > View Unentitled Machines**.

3 Remove the desktop assignments for unentitled users and roll back local desktops that unentitled users have checked out.

4 Select **More Commands > View Unentitled Machines** or **More Commands > View Unentitled Policies** as appropriate.

5 Change or remove the policies that are applied to unentitled users.

Collecting Diagnostic Information for VMware View

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with VMware View.

You can collect diagnostic information for various components of VMware View. How you collect this information varies depending on the VMware View component.

- Create a Data Collection Tool Bundle for View Agent on page 305

  To assist VMware Technical Support in troubleshooting View Agent, you might need to use the `vdmadmin` command to create a Data Collection Tool (DCT) bundle.

- Save Diagnostic Information for View Client on page 305

  If you encounter problems using View Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

- Collect Diagnostic Information for View Composer Using the Support Script on page 306

  You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

- Collect Diagnostic Information for View Connection Server Using the Support Tool on page 306

  You can use the support tool to set logging levels and generate log files for View Connection Server.

- Collect Diagnostic Information for View Agent, View Client, or View Connection Server from the Console on page 307

  If you have direct access to the console, you can use the support scripts to generate log files for View Connection Server, View Client, or desktops that are running View Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

Create a Data Collection Tool Bundle for View Agent

To assist VMware Technical Support in troubleshooting View Agent, you might need to use the `vdmadmin` command to create a Data Collection Tool (DCT) bundle.

You must be logged into a standard or replica instance View Connection Server as a user in the **Administrators** role.

Procedure

- To specify the names of the output bundle file, desktop pool, and machine, use the `–outfile`, `–d`, and `–m` options with the `vdmadmin` command.

  ```
  vdmadmin –A [–b authentication_arguments] –getDCT –outfile local_file –d desktop –m machine
  ```

The command writes the bundle to the specified output file.

Example: Creating a Bundle File for View Agent

Create the DCT bundle for the machine machine1 in the desktop pool dtpool2 and write it to the zip file `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

What to do next

If you have an existing support request, you can update it by attaching the DCT bundle file.

Save Diagnostic Information for View Client

If you encounter problems using View Client, and cannot resolve the problems using general network troubleshooting techniques, you can save a copy of the log files and information about the configuration.

You can attempt to resolve connection problems for View Client before saving the diagnostic information and contacting VMware Technical Support . For more information, see “Connection Problems Between View Client and View Connection Server,” on page 308.

Procedure

1. In View Client, click **Support Information**, or on the virtual desktop menu, select **Options > Support Information**.
2. In the Support Information window, click **Collect Support Data** and click **Yes** when prompted.

   A command window shows the progress of gathering the information. This process can take several minutes.
3. In the command window, respond to the prompts by entering the URLs of the View Connection Server instances against which you want to test the configuration of View Client, and, if required, selecting to generate diagnostic dumps of the VMware View processes.

   The information is written to a zip file in a folder on the client machine's desktop.
4. File a support request on the Support page of the VMware Web site, and attach the output zip file.

Collect Diagnostic Information for View Composer Using the Support Script

You can use the View Composer support script to collect configuration data and generate log files for View Composer. This information helps VMware customer support diagnose any issues that arise with View Composer.

Prerequisites

Log in to the vCenter Server on which View Composer is installed.

Because you must use the Windows Script Host utility (`cscript`) to run the support script, familiarize yourself with using `cscript`. See http://technet.microsoft.com/library/bb490887.aspx.

Procedure

1 Open a command prompt window and change to the `C:\Program Files\VMware\VMware View Composer` directory.

If you did not install the software in the default directories, substitute the appropriate drive letter and path.

2 Type the command to run the `svi-support` script.

```
cscript ".\svi-support.wsf /zip"
```

You can use the `/?` option to display information about other command options that are available with the script.

When the script finishes, it informs you of the name and location of the output file.

3 File a support request on the Support page of the VMware Web site and attach the output file.

Collect Diagnostic Information for View Connection Server Using the Support Tool

You can use the support tool to set logging levels and generate log files for View Connection Server.

The support tool collects logging data for View Connection Server. This information helps VMware Technical Support diagnose any issues that arise with View Connection Server. The support tool is not intended to collect diagnostic information for View Client or View Agent. You must instead use the support script. See "Collect Diagnostic Information for View Agent, View Client, or View Connection Server from the Console," on page 307.

Prerequisites

Log in to a standard or replica instance View Connection Server instance as a user in the **Administrators** role.

Procedure

1 Select **Start > All Programs > VMware > Set View Connection Server Log Levels**.

2 In the **Choice** text box, type a numeric value to set the logging level and press Enter.

Option	Description
0	Resets the logging level to the default value.
1	Selects a normal level of logging (default).
2	Selects a debug level of logging.
3	Selects full logging.

You should usually enter **2** to select a debug level of logging.

The system starts recording log information with the level of detail that you have selected.

3 When you have collected enough information about the behavior of View Connection Server, select **Start > All Programs > VMware > Generate View Connection Server Log Bundle**.

The support tool writes the log files to a folder called `vdm-sdct` on the desktop of the View Connection Server instance.

4 File a support request on the Support page of the VMware Web site and attach the output files.

Collect Diagnostic Information for View Agent, View Client, or View Connection Server from the Console

If you have direct access to the console, you can use the support scripts to generate log files for View Connection Server, View Client, or desktops that are running View Agent. This information helps VMware Technical Support diagnose any issues that arise with these components.

Prerequisites

Log in to the system that you want to collect information for.

- For View Agent, log in to the virtual machine with View Agent installed.
- For View Client, log in to the system with View Client installed.
- For View Connection Server, log in to the View Connection Server host.

Procedure

1 Open a command prompt window and change to the appropriate directory for the VMware View component that you want to collect diagnostic information for.

Option	Description
View Agent	Change to the `C:\Program Files\VMware View\Agent\DCT` directory.
View Client	Change to the `C:\Program Files\VMware View\Client\DCT` directory.
View Connection Server	Change to the `C:\Program Files\VMware View\Server\DCT` directory.

If you did not install the software in the default directories, substitute the appropriate drive letter and path.

2 Type the command to run the support script.

```
.\support.bat [loglevels]
```

If you want to enable advanced logging, specify the `loglevels` option and enter the numeric value for the logging level when prompted.

Option	Description
0	Resets the logging level to the default value.
1	Selects a normal level of logging (default).
2	Selects a debug level of logging.
3	Selects full logging.
4	Selects informational logging for PCoIP (View Agent and View Client only).
5	Selects debug logging for PCoIP (View Agent and View Client only).
6	Selects informational logging for virtual channels (View Agent and View Client only).

Option	Description
7	Selects debug logging for virtual channels (View Agent and View Client only).
8	Selects trace logging for virtual channels (View Agent and View Client only).

The script writes the zipped log files to the folder `vdm-sdct` on the desktop.

3 You can find the View Composer guest agent logs in the `C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support` directory.

4 File a support request on the Support page of the VMware Web site and attach the output file.

Update Support Requests

You can update your existing support request at the Support Web site.

After you file a support request, you might receive an email request from VMware Technical Support asking for the output file from the `support` or `svi-support` scripts. When you run the scripts, they inform you of the name and location of the output file. Reply to the email message and attach the output file to the reply.

If the output file is too large to include as an attachment (10MB or more), contact VMware Technical Support, tell them the number of your support request, and request FTP upload instructions. Alternatively, you can attach the file to your existing support request at the Support Web site.

Procedure

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 the output that you obtained by running the `support` or `svi-support` script.

Further Troubleshooting Information

You can find further troubleshooting information in VMware Knowledge Base articles.

The VMware Knowledge Base (KB) is continually updated with new troubleshooting information for VMware products.

For more information about troubleshooting View Manager, see the KB articles that are available on the VMware KB Web site:

http://kb.vmware.com/selfservice/microsites/microsite.do

Troubleshooting Network Connection Problems

You can use a variety of procedures for diagnosing and fixing problems with network connections with desktops, View Clients and View Connection Server instances.

Connection Problems Between View Client and View Connection Server

You might experience connection problems between View Client and View Connection Server.

Problem

If the connectivity between View Client and a View Connection Server instance fails, you see one of the following View Client errors:

- `A secure connection to the server 'servername' cannot be established.`

- `The View Connection Server connection failed.`

Opening a desktop might also fail after contacting a View Connection Server instance and obtaining a list of available desktops.

Cause

Connectivity problems between View Client and a View Connection Server instance can occur for different reasons.

- Incorrect network proxy or firewall settings on View Client.
- Lookup failure for the DNS name of the View Connection Server host when setting up a secure connection.

Solution

Try the following solutions in sequence. If a solution does not resolve the issue, try the next one.

- Use a browser to access the View Connection Server instance by using HTTP or HTTPS.

  If you do not see the login page, apply general network troubleshooting techniques to resolve the issue.
- Enter valid credentials on the login page.
- If you receive an error message about being unable to start the secure connection, the most likely reason is that View Client (or proxy server, if configured) is unable to resolve the DNS name of the View Connection Server host. Configure the host to provide its IP address rather than its FQDN when it directs View Client to open a secure connection.

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

  b Select the security server or View Connection Server instance and click **Edit**.

  c In the External URL text box, change the URL so that it contains the external IP address for the security server or View Connection Server instance that View clients can access over the Internet.

  d Click **OK**.

  The external URL is updated immediately. You do not need to restart the View Connection Server service for the change to take effect.
- If the preceding solution does not resolve the issue, restart the View Connection Server instance.

Connection Problems Between View Client and the PCoIP Secure Gateway

You might experience connection problems between View Client and a security server or View Connection Server host when the PCoIP Secure Gateway is configured to authenticate external users that communicate over PCoIP.

Problem

View clients that use PCoIP cannot connect to or display View desktops. The initial login to a security server or View Connection Server instance succeeds, but the connection fails when the user selects a View desktop. This issue occurs when the PCoIP Secure Gateway is configured on a security server or View Connection Server host.

NOTE Typically, the PCoIP Secure Gateway is leveraged on a security server. In a network configuration in which external clients connect directly to a View Connection Server host, the PCoIP Secure Gateway can also be configured on View Connection Server.

Cause

Problems connecting to the PCoIP Secure Gateway can occur for different reasons.

- Windows Firewall has closed a port that is required for the PCoIP Secure Gateway.

- The PCoIP Secure Gateway is not enabled on the security server or View Connection Server instance.
- The PCoIP External URL setting is configured incorrectly. You must specify this setting as the external IP address that View clients can access over the Internet.
- The PCoIP External URL or secure tunnel External URL is configured to point to a different security server or View Connection Server host. When you configure these two external URLs on a security server or View Connection Server host, both external URLs must be addresses for the current host.
- The View client is connecting through an external web proxy that has closed a port required for the PCoIP Secure Gateway. For example, a web proxy in a hotel network or public wireless connection might block the required ports.
- The View Connection Server instance that is paired with the security server on which the PCoIP Secure Gateway is configured is version View 4.5 or earlier. The security server and paired View Connection Server instance must be View 4.6 or later.

Solution

- Check that the following network ports are opened on the firewall for the security server or View Connection Server host.

Port	Description
TCP 4172	From View Client to the security server or View Connection Server host.
UDP 4172	Between View client and the security server or View Connection Server host, in both directions.
TCP 4172	From the security server or View Connection Server host to the View desktop.
UDP 4172	Between the security server or View Connection Server host and the View desktop, in both directions.

- In View Administrator, enable the PCoIP Secure Gateway and make sure that the PCoIP External URL is configured correctly.
  a Click **View Configuration > Servers**.
  b Select the security server or View Connection Server instance and click **Edit**.
  c Select **Use PCoIP Secure Gateway for PCoIP connections to desktop**.

  The PCoIP Secure Gateway is disabled by default.
  d In the **PCoIP External URL** text box, make sure that the URL contains the external IP address for the security server or View Connection Server instance that View clients can access over the Internet.

  Specify port 4172. Do not include a protocol name.

  For example: `100.200.300.400:4172`
  e Make sure that both the **PCoIP External URL** and secure tunnel **External URL** are the addresses that client systems use to reach this host.

  For example, if you configure a View Connection Server host, do not specify the **PCoIP External URL** for this host and the secure tunnel **External URL** for a paired security server.
  f Click **OK**.
- If the user is connecting through a web proxy that is outside of your network, and the proxy is blocking a required port, direct the user to connect from a different network location.
- Make sure that both the security server and the paired View Connection Server instance are View 4.6 or later.

Connection Problems Between Desktops and View Connection Server Instances

You might experience connection problems between desktops and View Connection Server instances.

Problem

If connectivity between a desktop and a View Connection Server instance fails, you see one of the following messages in the event database.

- `Provisioning error occurred for Machine Machine_Name: Customization error due to no network communication between the View agent and Connection Server`
- `Provisioning error occurred on Pool Desktop_ID because of a networking problem with a View Agent`
- `Unable to launch from Pool Desktop_ID for user User_Display_Name: Failed to connect to Machine MachineName using Protocol`

Cause

The connectivity problems between a desktop and a View Connection Server instance can occur for different reasons.

- Lookup failure on the desktop for the DNS name of the View Connection Server host.
- The ports for JMS, RDP, or AJP13 communication being blocked by firewall rules.
- The failure of the JMS router on the View Connection Server host.

Solution

- At a command prompt on the desktop, type the `nslookup` command.

  `nslookup CS_FQDN`

  CS_FQDN is the fully qualified domain name (FQDN) of the View Connection Server host. If the command fails to return the IP address of the View Connection Server host, apply general network troubleshooting techniques to correct the DNS configuration.

- At a command prompt on the desktop, verify that TCP port 4001, which View Agent uses to establish JMS communication with the View Connection Server host, is working by typing the `telnet` command.

  `telnet CS_FQDN 4001`

  If the `telnet` connection is established, network connectivity for JMS is working.

- If a security server is deployed in the DMZ, verify that exception rules are configured in the inner firewall to allow RDP connectivity between the security server and desktop virtual machines on TCP port 3389.
- If secure connections are bypassed, verify that the firewall rules allow a client to establish either a direct RDP connection to the desktop virtual machine on TCP port 3389, or a direct PCoIP connection to the desktop virtual machine on TCP port 4172 and UDP port 4172.
- Verify that exception rules are configured in the inner firewall to allow connections between each Security Server and its associated View Connection Server host on TCP port 4001 (JMS) and TCP port 8009 (AJP13).

Connection Problems Due to Incorrect Assignment of IP Addresses to Cloned Desktops

You might not be able to connect to cloned desktops if they have static IP addresses.

Problem

You cannot use View Client to connect to cloned desktops.

Cause

Cloned desktops are incorrectly configured to use a static IP address instead of using DHCP to obtain their IP addresses.

Solution

1 Verify that the template for a desktop pool on vCenter is configured to use DHCP to assign IP addresses to desktops.

2 In the VMware Infrastructure Client, clone one virtual machine manually from the desktop pool and verify that it obtains its IP address from DHCP correctly.

Troubleshooting Desktop Pool Creation Problems

You can use several procedures for diagnosing and fixing problems with the creation of desktop pools.

Pool Creation Fails if Customization Specifications Cannot Be Found

If you try to create a desktop pool, the operation fails if the customization specifications cannot be found.

Problem

You cannot create a desktop pool, and you see the following message in the event database.

`Provisioning error occurred for Machine` *`Machine_Name`*`: Customization failed for Machine`

Cause

The most likely cause of this problem is that you have insufficient permissions to access the customization specifications, or to create a pool. Another possible cause is that the customization specification has been renamed or deleted.

Solution

- Verify that you have sufficient permissions to access the customization specifications, and to create a pool.
- If the customization specification no longer exists because it has been renamed or deleted, choose a different specification.

Pool Creation Fails Because of a Permissions Problem

You cannot create a desktop pool if there is a permissions problem with an ESX/ESXi host, ESX/ESXi cluster, or datacenter.

Problem

You cannot create a desktop pool in View Administrator because the templates, ESX/ESXi host, ESX/ESXi cluster, or datacenter are not accessible.

Cause

This problem has a number of possible causes.

- You do not have the correct permissions to create a pool.
- You do not have the correct permissions to access the templates.
- You do not have the correct permissions to access the ESX/ESXi host, ESX/ESXi cluster, or datacenter.

Solution

- If the Template Selection screen does not show any available templates, verify that you have sufficient permissions to access the templates.

- Verify that you have sufficient permissions to access the ESX/ESXi host, ESX/ESXi cluster, or datacenter.
- Verify that you have sufficient permissions to create a pool.

Pool Provisioning Fails Due to a Configuration Problem

If a template is not available or a virtual machine image has been moved or deleted, provisioning of a desktop pool can fail.

Problem

A desktop pool is not provisioned, and you see the following message in the event database.

`Provisioning error occurred on Pool` *`Desktop_ID`* `because of a configuration problem`

Cause

This problem has a number of possible causes.

- A template is not accessible.
- The name of a template has been changed in vCenter.
- A template has been moved to a different folder in vCenter.
- A virtual machine image has been moved between ESX/ESXi hosts, or it has been deleted.

Solution

- Verify that the template is accessible.
- Verify that the correct name and folder are specified for the template.
- If a virtual machine image has been moved between ESX/ESXi hosts, move the virtual machine to the correct vCenter folder.
- If a virtual machine image has been deleted, delete the entry for the virtual machine in View Administrator and recreate or restore the image.

Pool Provisioning Fails Due to a View Connection Server Instance Being Unable to Connect to vCenter

If a Connection Server is not able to connect to vCenter, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see one of the following error messages in the event database.

- `Cannot log in to vCenter at address` *`VC_Address`*
- `The status of vCenter at address` *`VC_Address`* `is unknown`

Cause

The View Connection Server instance cannot connect to vCenter for one of the following reasons.

- The Web service on the vCenter Server has stopped.
- There are networking problems between the View Connection Server host and the vCenter Server.
- The port numbers and login details for vCenter or View Composer have changed.

Solution

- Verify that the Web service is running on the vCenter.
- Verify that there are no network problems between the View Connection Server host and the vCenter.

- In View Administrator, verify the port numbers and login details that are configured for vCenter and View Composer.

Pool Provisioning Fails Due to Datastore Problems

If a datastore is out of disk space, or you do not have permission to access the datastore, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see one of the following error messages in the event database.

- `Provisioning error occurred for Machine Machine_Name: Cloning failed for Machine`
- `Provisioning error occurred on Pool Desktop_ID because available free disk space is reserved for linked clones`
- `Provisioning error occurred on Pool Desktop_ID because of a resource problem`

Cause

You do not have permission to access the selected datastore, or the datastore being used for the pool is out of disk space.

Solution

- Verify that you have sufficient permissions to access the selected datastore.
- Verify whether the disk on which the datastore is configured is full.
- If the disk is full or the space is reserved, free up space on the disk, rebalance the available datastores, or migrate the datastore to a larger disk.

Pool Provisioning Fails Due to vCenter Being Overloaded

If vCenter is overloaded with requests, provisioning of a desktop pool can fail.

Problem

Provisioning of a desktop pool fails, and you see the following error message in the event database.

`Provisioning error occurred on Pool Desktop_ID because of a timeout while customizing`

Cause

vCenter is overloaded with requests.

Solution

- In View Administrator, reduce the maximum number of concurrent provisioning and power operations for vCenter.
- Configure additional vCenter Servers.

  For more information about configuring vCenter, see the *VMware View Installation* document.

Virtual Machines Are Stuck in the Provisioning State

After being cloned, virtual machines are stuck in the Provisioning state.

Problem

Virtual machines are stuck in the Provisioning state.

Cause

The most likely cause of this problem is that you restarted the View Connection Server instance during a cloning operation.

Solution

- Delete the virtual machines and clone them again.

Virtual Machines Are Stuck in the Customizing State

After being cloned, virtual machines are stuck in the Customizing state.

Problem

Virtual machines are stuck in the Customizing state.

Cause

The most likely cause of this problem is that there is not enough disk space to start the virtual machine. A virtual machine must start before customization can take place.

Solution

- Delete the virtual machine to recover from a stuck customization.
- If the disk is full, free up space on the disk or migrate the datastore to a larger disk.

Troubleshooting USB Redirection Problems

Various problems can arise with USB redirection in View Client.

Problem

USB redirection in View Client fails to make local devices available on the remote desktop, or some devices do not appear to be available for redirection in View Client.

Cause

The following are possible causes for USB redirection failing to function correctly or as expected.

- USB redirection is not supported for Windows 2003 or Windows 2008 systems or for View desktops that are managed by Microsoft Terminal Services.
- Webcams are not supported for redirection.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle.
- USB redirection is not supported for boot devices. If you run View Client on a Windows system that boots from a USB device, and you redirect this device to the remote desktop, the local operating system might become unresponsive or unusable. See http://kb.vmware.com/kb/1021409.
- By default, View Client for Windows does not allow you to select Human Interface Devices (HIDs) and Bluetooth devices that are paired with an HID for redirection. See http://kb.vmware.com/kb/1011600.
- RDP does not support the redirection of USB HIDs for the console session, or of smart card readers. See http://kb.vmware.com/kb/1011600.
- RDP can cause unexpected problems when using USB flash cards. See http://kb.vmware.com/kb/1019547.
- Windows Mobile Device Center can prevent the redirection of USB devices for RDP sessions. See http://kb.vmware.com/kb/1019205.

- For some USB HIDs, you must configure the virtual machine to update the position of the mouse pointer. See http://kb.vmware.com/kb/1022076.
- Some audio devices might require changes to policy settings or to registry settings. See http://kb.vmware.com/kb/1023868.
- Network latency can cause slow device interaction or cause applications to appear frozen because they are designed to interact with local devices. Very large USB disk drives might take several minutes to appear in Windows Explorer.
- USB flash cards formatted with the FAT32 file system are slow to load. See http://kb.vmware.com/kb/1022836.
- A process or service on the local system opened the device before you connected to the remote desktop.
- A redirected USB device stops working if you reconnect a desktop session even if the desktop shows that the device is available.
- USB redirection is disabled in View Administrator.
- Missing or disabled USB redirection drivers on the guest.
- Missing or disabled USB redirection drivers or missing or disabled drivers for the device that is being redirected on the client.

Solution

- If available, use PCoIP instead of RDP as the desktop protocol.
- If a redirected device remains unavailable or stops working after a temporary disconnection, remove the device, plug it in again, and retry the redirection.
- In View Administrator, go to **Policies > Global Policies**, and verify that USB access is set to **Allow** under View Policies.
- Examine the log on the guest for entries of class `wssm_usb`, and the log on the client for entries of class `wswc_usb`.

  Entries with these classes are written to the logs if a user is not an administrator, or if the USB redirection drivers are not installed or are not working.
- Open the Device Manager on the guest, expand Universal Serial Bus controllers, and reinstall the VMware View Virtual USB Device Manager and VMware View Virtual USB Hub drivers if these drivers are missing or re-enable them if they are disabled.
- Open the Device Manager on the client, expand Universal Serial Bus controllers, and reinstall the VMware View Generic USB Device driver and the USB driver for the redirected device if these drivers are missing or re-enable them if they are disabled.

Troubleshooting QuickPrep Customization Problems

A View Composer QuickPrep customization script can fail for a variety of reasons.

Problem

A QuickPrep post-synchronization or power-off script does not execute. In some cases, a script might complete successfully on some linked clones, but fail on others.

Cause

A few common causes exist for QuickPrep script failures:

- The script times out
- The script path refers to a script that requires an interpreter

- The account under which the script runs does not have sufficient permission to execute a script task

Solution

- Examine the customization script log.

  QuickPrep customization information is written to a log file in Windows `temp` directory:

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```

- Determine if the script timed out.

  View Composer terminates a customization script that takes longer than 20 seconds. The log file displays a message showing that the script has started and a later message indicating the timeout:

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script: cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  To solve a timeout problem, increase the timeout limit for the script and run it again.

- Determine if the script path is valid.

  If you use a scripting language that needs an interpreter to execute the script, the script path must start with the interpreter binary.

  For example, if you specify the path `C:\script\myvb.vbs` as a QuickPrep customization script, View Composer Agent cannot execute the script. You must specify a path that starts with the interpreter binary path:

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- Determine if the account under which the script runs has appropriate permissions to perform script tasks.

  QuickPrep runs the scripts under the account under which the VMware View Composer Guest Agent Server service is configured to run. By default, this account is `Local System`.

  Do not change this log on account. If you do, the linked clones do not start.

View Composer Provisioning Errors

If an error occurs when View Composer provisions or recomposes linked-clone desktops, an error code indicates the cause of the failure. The error code appears in the desktop-status column in View Administrator.

Table 16-2 describes the View Composer provisioning error codes.

This table lists errors that are associated with View Composer and QuickPrep customization. Additional errors can occur in View Connection Server and other View components that can interfere with desktop provisioning.

Table 16-2. View Composer Provisioning Errors

Error	Description
0	The policy was applied successfully. **NOTE** Result code 0 does not appear in View Administrator. The linked-clone desktop proceeds to a Ready state, unless a View Manager error outside the domain of View Composer occurs. This result code is included for completeness.
1	Failed to set the computer name.
2	Failed to redirect the user profiles to the View Composer persistent disk.
3	Failed to set the computer's domain account password.

Table 16-2. View Composer Provisioning Errors (Continued)

Error	Description
4	Failed to back up a user's profile keys. The next time the user logs in to this linked-clone desktop after the recompose operation, the OS creates a new profile directory for the user. As a new profile is created, the user cannot not see the old profile data.
5	Failed to restore a user's profile. The user should not log in to the desktop in this state because the profile state is undefined.
6	Errors not covered by other error codes. The View Composer agent log files in the guest OS can provide more information about the causes of these errors. For example, a Windows Plug and Play (PnP) timeout can generate this error code. In this situation, View Composer times out after waiting for the PnP service to install new volumes for the linked-clone virtual machine. PnP mounts up to three disks, depending on how the pool was configured: ■ View Composer persistent disk ■ Nonpersistent disk for redirecting guest OS temp and paging files ■ Internal disk that stores QuickPrep configuration and other OS-related data. This disk is always configured with a linked clone. The timeout length is 10 minutes. If PnP does not finish mounting the disks within 10 minutes, View Composer fails with error code 6.
7	Too many View Composer persistent disks are attached to the linked clone. A clone can have at most three View Composer persistent disks.
8	A persistent disk could not be mounted on the datastore that was selected when the pool was created.
9	View Composer could not redirect disposable-data files to the nonpersistent disk. Either the paging file or the temp-files folders were not redirected.
10	View Composer cannot find the QuickPrep configuration policy file on the specified internal disk.
12	View Composer cannot find the internal disk that contains the QuickPrep configuration policy file and other OS-related data.
13	More than one persistent disk is configured to redirect the Windows user profile.
14	View Composer failed to unmount the internal disk.
15	The computer name that View Composer read from configuration-policy file does not match the current system name after the linked clone is initially powered on.
16	The View Composer agent did not start because the volume license for the guest OS was not activated.
17	The View Composer agent did not start. The agent timed out while waiting for Sysprep to start.
18	The View Composer agent failed to join the linked-clone virtual machine to a domain during customization.
19	The View Composer agent failed to execute a post-synchronization script.
20	The View Composer agent failed to handle a machine password synchronization event. This error might be transient. If the linked clone joins the domain, the password is fine. If the clone fails to join the domain, restart the operation you performed before the error occurred. If you restarted the clone, restart it again. If you refreshed the clone, refresh it again. If the clone still fails to join the domain, recompose the clone.

Windows XP Linked Clones Fail to Join the Domain

Windows XP linked-clone desktops can fail to join the domain if your Active Directory runs on Windows Server 2008.

Problem

When linked-clone desktops are provisioned, the linked clones fail to join the domain. View Administrator displays View Composer provisioning error messages. For example:

```
5/17/10 3:11:50 PM PDT: View Composer agent initialization state error (18): Failed to join the domain (waited 565 seconds)
```

Cause

This issue can occur if your Active Directory runs on Windows Server 2008. The Windows Server 2008 read-only domain controller (RODC) is not backward-compatible with Windows XP virtual machines.

Solution

1 Check the View Composer log for the following error message:

```
0x4f1: The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you.
```

By default, the View Composer log file is generated in the Windows `Temp` directory: `C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

2 On the parent virtual machine, apply the Windows Server 2008 RODC compatibility update for Windows XP.

See Microsoft Support Article 944043 at the following location: http://support.microsoft.com/kb/944043/en-us.

3 Take a snapshot of the updated parent virtual machine.

4 Recompose the linked-clone desktops from the updated parent virtual machine and snapshot.

Troubleshooting GINA Problems on Windows XP Desktops

On Windows XP desktops, problems can occur with chaining the VMware View Graphical Identification and Authentication (GINA) dynamic link library (dll) files.

Problem

The following problems can occur on Windows XP desktops:

- A desktop does not start up
- When a desktop starts up or shuts down, the following error is displayed: `Cannot start gina.dll module. A required component is missing: gina.dll. Please install the application again.`
- When you start a desktop, an unexpected login prompt appears
- You cannot log in to your desktop

Cause

Startup and login problems can occur on Windows XP desktops when the View GINA `dll` files are not chained properly with third-party GINAs that might reside on the virtual machines.

To ensure that the GINA is chained properly, you must configure the `WinLogon` GINA to be the View GINA and make sure that the `vdmGinaChainDLL` is created and contains the third-party GINAs.

If you did not install any software that chains to a different GINA, the default is `msgina.dll`, which is located at `%systemroot%\system32\msgina.dll` on the virtual machine.

Solution

1 Log in to the parent virtual machine, template virtual machine, or View desktop.

2 Click **Start > Run**, type **`Regedit`**, and press Enter.

3 Navigate to the following Windows registry key:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\GinaDLL`

4 Ensure that the `GinaDLL` key has the following value:

install_directory\VMware\VMware View\Agent\bin\wsgina.dll

install_directory is the path where you installed View Agent.

5 If the `vdmGinaChainDLL` string value does not exist, create it.

a Navigate to the following registry key:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version`

b Create the `vdmGinaChainDLL` key.

6 Place the third-party GINA `dll` names in the `vdmGinaChainDLL` key.

7 If you still experience problems with the Windows XP desktops, ensure that no vendor-specific GINA keys are loaded in the registry.

If third-party GINA keys are loaded, the chaining GINA might still be calling the default GINA, `msgina`. Some network management and security software products place their GINA replacement `dlls` in their own installation directories, in registry paths such as this one:

`HKEY_LOCAL_MACHINE\Software\`*`Vendor_ID_or_Name`*`\`*`GINA_key_reference`*`\`*`GINA_Load_Instruction`* `= msgina`

Remove these GINA keys from the vendor-specific location and place them in the `vdmGinaChainDLL` key.

17 Using the vdmadmin Command

You can use the vdmadmin command line interface to perform a variety of administration tasks on a View Connection Server instance.

You can use vdmadmin to perform administration tasks that are not possible from within the View Administrator user interface or to perform administration tasks that need to run automatically from scripts.

For a comparison of the operations that are possible in View Administrator, View cmdlets, and vdmadmin, see the *VMware View Integration* document.

- Configuring Domain Filters Using the -N Option on page 332

  You can use the vdmadmin command with the –N option to control the domains that View Manager makes available to end users.

- Configuring Domain Filters on page 334

  You can configure domain filters to limit the domains that a View Connection Server instance or security server makes available to end users.

- Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options on page 338

  You can use the vdmadmin command with the –O and –P options to display the desktops and policies that are assigned to users who are no longer entitled to use the system.

- Configuring Clients in Kiosk Mode Using the -Q Option on page 339

  You can use the vdmadmin command with the –Q option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

- Displaying the First User of a Desktop Using the -R Option on page 343

  You can use the vdmadmin command with the –R option to find out the initial assignment of a managed desktop. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign desktops to users.

- Removing the Entry for a View Connection Server Instance Using the -S Option on page 343

  You can use the vdmadmin command with the –S option to remove the entry for a View Connection Server instance from the View Manager configuration.

- Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option on page 344

  You can use the vdmadmin command with the –T option to set the split limit for publishing View Transfer Server packages. You might want to specify a split limit if you use a proxy cache that defines a maximum object size for its cache.

- Displaying Information About Users Using the -U Option on page 345

  You can use the vdmadmin command with the –U option to display detailed information about users.

- Decrypting the Virtual Machine of a Local Desktop Using the -V Option on page 345

  VMware View secures the virtual machine of a local desktop by encrypting its base image. If you are not able to power on or check in the local desktop, you can use the vdmadmin command with the –V option to decrypt the virtual machine so that you can recover data from it.

- Unlocking or Locking Virtual Machines Using the -V Option on page 346

  You can use the vdmadmin command with the –V option to unlock or lock virtual machines in the datacenter.

- Detecting and Resolving LDAP Entry Collisions Using the -X Option on page 347

  You can use the vdmadmin command with the –X option to detect and resolve colliding LDAP entries on replicated View Connection Server instances in a group.

vdmadmin Command Usage

The syntax of the vdmadmin command controls its operation.

Use the following form of the vdmadmin command from a Windows command prompt.

vdmadmin *command_option* [*additional_option argument*] ...

The additional options that you can use depend on the command option.

By default, the path to the vdmadmin command executable file is C:\Program Files\VMware\VMware View\Server\tools\bin. To avoid having to enter the path on the command line, add the path to your *PATH* environment variable.

- vdmadmin Command Authentication on page 323

  You must run the vdmadmin command as a user who is in the **Administrators** role for a specified action to succeed.

- vdmadmin Command Output Format on page 323

  Some vdmadmin command options allow you to specify the format of the output information.

- vdmadmin Command Options on page 324

  You use the command options of the vdmadmin command to specify the operation that you want it to perform.

vdmadmin Command Authentication

You must run the vdmadmin command as a user who is in the **Administrators** role for a specified action to succeed.

You can use View Administrator to assign the **Administrators** role to a user. See Chapter 2, "Configuring Role-Based Delegated Administration," on page 25.

If you are logged in as a user with insufficient privileges, you can use the –b option to run the command as a user who has been assigned the **Administrators** role, if you know that user's password. You can specify the –b option to run the vdmadmin command as the specified user in the specified domain. The following usage forms of the –b option are equivalent.

```
–b username domain [password | *]
–b username@domain [password | *]
–b domain\username [password | *]
```

If you specify an asterisk (*) instead a password, you are prompted to enter the password. You can use the –b option with all command options except the –R and –T options.

vdmadmin Command Output Format

Some vdmadmin command options allow you to specify the format of the output information.

Table 17-1 shows the options that some vdmadmin command options provide for formatting output text.

Table 17-1. Options for Selecting Output Format

Option	Description
–csv	Formats the output as comma-separated values.
–n	Display the output using ASCII (UTF-8) characters. This is the default character set for comma-separated values and plain text output.
–w	Display the output using Unicode (UTF-16) characters. This is the default character set for XML output.
–xml	Formats the output as XML.

vdmadmin Command Options

You use the command options of the `vdmadmin` command to specify the operation that you want it to perform.

Table 17-2 shows the command options that you can use with the `vdmadmin` command to control and examine the operation of View Manager.

Table 17-2. Vdmadmin Command Options

Option	Description
`-A`	Administers the information that a View Agent records in its log files. See "Configuring Logging in View Agent Using the -A Option," on page 325. Overrides the IP address reported by a View Agent. See "Overriding IP Addresses Using the -A Option," on page 326
`-C`	Sets the name for a View Connection Server group. See "Setting the Name of a View Connection Server Group Using the -C Option," on page 327.
`-F`	Updates the Foreign Security Principals (FSPs) in Active Directory for all users or for specified users. See "Updating Foreign Security Principals Using the -F Option," on page 328.
`-H`	Displays health information about View Manager services. See "Listing and Displaying Health Monitors Using the -H Option," on page 328.
`-I`	Generates reports about View Manager operation. See "Listing and Displaying Reports of View Manager Operation Using the -I Option," on page 329.
`-L`	Assigns a dedicated desktop to a user or removes an assignment. See "Assigning Dedicated Desktops Using the -L Option," on page 330.
`-M`	Displays information about a virtual machine or physical computer. See "Displaying Information About Machines Using the -M Option," on page 331.
`-N`	Configures the domains that a View Connection Server instance or group makes available to View Clients. See "Configuring Domain Filters Using the -N Option," on page 332.
`-O`	Displays the desktops that are assigned to users who are no longer entitled to those desktops. See "Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options," on page 338.
`-P`	Displays the user policies that are associated with the desktops of unentitled users. See "Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options," on page 338.
`-Q`	Configures the account in Active Directory account and View Manager configuration of a client device in kiosk mode. See "Configuring Clients in Kiosk Mode Using the -Q Option," on page 339.
`-R`	Reports the first user who accessed a desktop. See "Displaying the First User of a Desktop Using the -R Option," on page 343.
`-S`	Removes a configuration entry for a View Connection Server instance from the configuration of View Manager. See "Removing the Entry for a View Connection Server Instance Using the -S Option," on page 343.
`-T`	Sets the split limit for View Transfer Server packages. See "Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option," on page 344.
`-U`	Displays information about a user including their desktop entitlements and ThinApp assignments, and Administrator roles. See "Displaying Information About Users Using the -U Option," on page 345.
`-V`	Allows data to be recovered from a local desktop by decrypting its virtual machine. See "Decrypting the Virtual Machine of a Local Desktop Using the -V Option," on page 345. Unlocks or locks virtual machines including local desktops and View Transfer Server instances. See "Unlocking or Locking Virtual Machines Using the -V Option," on page 346.
`-X`	Detects and resolves duplicated LDAP entries on replicated View Connection Server instances. See "Detecting and Resolving LDAP Entry Collisions Using the -X Option," on page 347.

Configuring Logging in View Agent Using the -A Option

You can use the `vdmadmin` command with the `–A` option to configure logging by View Agent.

Syntax

```
vdmadmin –A [–b authentication_arguments] –getDCT–outfile local_file –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –getlogfile logfile –outfile local_file –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –getloglevel [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –getstatus [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –getversion [–xml] –d desktop [–m machine]

vdmadmin –A [–b authentication_arguments] –list [–xml] [–w | –n] –d desktop –m machine

vdmadmin –A [–b authentication_arguments] –setloglevel level –d desktop [–m machine]
```

Usage Notes

To assist VMware Technical Support in troubleshooting a View Agent, you can create a Data Collection Tool (DCT) bundle. You can also change the logging level, display the version and status of View Agent, and save individual log files to your local disk.

Options

Table 17-3 shows the options that you can specify to configure logging in View Agent.

Table 17-3. Options for Configuring Logging in View Agent

Option	Description
`–d` *desktop*	Specifies the desktop pool.
`–getDCT`	Creates a Data Collection Tool (DCT) bundle and saves it to a local file.
`–getlogfile` *logfile*	Specifies the name of the log file to save a copy of.
`–getloglevel`	Displays the current logging level of View Agent.
`–getstatus`	Displays the status of View Agent.
`–getversion`	Displays the version of View Agent.
`–list`	List the log files for View Agent.
`–m` *machine*	Specifies the machine within a desktop pool.
`–outfile` *local_file*	Specifies the name of the local file in which to save a DCT bundle or a copy of a log file.
`–setloglevel` *level*	Sets the logging level of View Agent. **debug** Logs error, warning, and debugging events. **normal** Logs error and warning events. **trace** Logs error, warning, informational, and debugging events.

Examples

Display the logging level of the Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getloglevel
```

Set the logging level of the View Agent for the machine machine1 in the desktop pool dtpool2 to debug.

```
vdmadmin –A –d dtpool2 –m machine1 –setloglevel debug
```

Display the list of View Agent log files for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –list
```

Save a copy of the View Agent log file `log–2009–01–02.txt` for the machine machine1 in the desktop pool dtpool2 as `C:\mycopiedlog.txt`.

```
vdmadmin –A –d dtpool2 –m machine1 –getlogfile log–2009–01–02.txt –outfile C:\mycopiedlog.txt
```

Display the version of the View Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getversion
```

Display the status of the View Agent for the machine machine1 in the desktop pool dtpool2.

```
vdmadmin –A –d dtpool2 –m machine1 –getstatus
```

Create the DCT bundle for the machine machine1 in the desktop pool dtpool2 and write it to the zip file `C:\myfile.zip`.

```
vdmadmin –A –d dtpool2 –m machine1 –getDCT –outfile C:\myfile.zip
```

Overriding IP Addresses Using the -A Option

You can use the `vdmadmin` command with the `–A` option to override the IP address reported by a View Agent.

Syntax

```
vdmadmin –A [–b authentication_arguments] –override –i ip_or_dns –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –list –d desktop –m machine
```

```
vdmadmin –A [–b authentication_arguments] –override –r –d desktop [–m machine]
```

Usage Notes

A View Agent reports the discovered IP address of the machine on which it is running to the View Connection Server instance. In secure configurations where the View Connection Server instance cannot trust the value that the View Agent reports, you can override the value provided by the View Agent and specify the IP address that the managed machine should be using. If the address of a machine that the View Agent reports does not match the defined address, you cannot use a View client to access the machine.

Options

Table 17-4 shows the options that you can specify to override IP addresses.

Table 17-4. Options for Overriding IP Addresses

Option	Description
`–d` *desktop*	Specifies the desktop pool.
`–i` *ip_or_dns*	Specifies the IP address or resolvable domain name in DNS.
`–m` *machine*	Specifies the name of the machine in a desktop pool.

Table 17-4. Options for Overriding IP Addresses (Continued)

Option	Description
–override	Specifies an operation for overriding IP addresses.
–r	Removes an overridden IP address.

Examples

Override the IP address for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –i 10.20.54.165 –d dtpool2 –m machine2
```

Display the IP addresses that are defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –list –d dtpool2 –m machine2
```

Remove the IP addresses that is defined for the machine machine2 in the desktop pool dtpool2.

```
vdmadmin –A –override –r –d dtpool2 –m machine2
```

Remove the IP addresses that are defined for the desktops in the desktop pool dtpool3.

```
vdmadmin –A –override –r –d dtpool3
```

Setting the Name of a View Connection Server Group Using the -C Option

You can use the vdmadmin command with the –C option to set the name of a View Connection Server group. The Microsoft System Center Operations Manager (SCOM) console displays this name to help you identify the group within SCOM.

Syntax

```
vdmadmin –C [–b authentication_arguments] [–c groupname]
```

Usage Notes

You must name a View Connection Server group if you intend to use SCOM to monitor and manage the state of View Manager components. View Administrator does not display the name of a group. Run the command on a member of the group that you want to name.

If you do not specify a name for the group, the command returns the GUID of the group to which the local View Connection Server instance belongs. You can use the GUID to verify whether a View Connection Server instance is a member of the same View Connection Server group as another View Connection Server instance.

For a description of how to use SCOM with VMware View, see the *VMware View Integration* document.

Options

The –c option specifies the name of the View Connection Server group. If you do not specify this option, the command returns the GUID of the group.

Examples

Set the name of a View Connection Server group to VCSG01.

```
vdmadmin –C –c VCSG01
```

Return the GUID of the group.

```
vdmadmin –C
```

Updating Foreign Security Principals Using the -F Option

You can use the vdmadmin command with the –F option to update the foreign security principals (FSPs) of Windows users in Active Directory who are authorized to use a desktop.

Syntax

```
vdmadmin –F [–b authentication_arguments] [–u domain\user]
```

Usage Notes

If you trust domains outside of your local domains, you allow access by security principals in the external domains to the local domains' resources. Active Directory uses FSPs to represent security principals in trusted external domains. You might want to update the FSPs of users if you modify the list of trusted external domains.

Options

The –u option specifies the name and domain of the user whose FSP you want to update. If you do not specify this option, the command updates the FSPs of all users in Active Directory.

Examples

Update the FSP of the user Jim in the EXTERNAL domain.

```
vdmadmin –F –u EXTERNAL\Jim
```

Update the FSPs of all users in Active Directory.

```
vdmadmin –F
```

Listing and Displaying Health Monitors Using the -H Option

You can use the vdmadmin command –H to list the existing health monitors, to monitor instances for View Manager components, and to display the details of a specific health monitor or monitor instance.

Syntax

```
vdmadmin –H [–b authentication_arguments] –list –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –list –monitorid monitor_id –xml [–w | –n]
```

```
vdmadmin –H [–b authentication_arguments] –monitorid monitor_id –instanceid instance_id –xml [–w | –n]
```

Usage Notes

Table 17-5 shows the health monitors that View Manager uses to monitor the health of its components.

Table 17-5. Health Monitors

Monitor	Description
CBMonitor	Monitors the health of View Connection Server instances.
DBMonitor	Monitors the health of the events database.
DomainMonitor	Monitors the health of the View Connection Server host's local domain and all trusted domains.
SGMonitor	Monitors the health of security gateway services and security servers.

Table 17-5. Health Monitors (Continued)

Monitor	Description
TSMonitor	Monitors the health of transfer servers.
VCMonitor	Monitors the health of vCenter servers.

If a component has several instances, View Manager creates a separate monitor instance to monitor each instance of the component.

The command outputs all information about health monitors and monitor instances in XML format.

Options

Table 17-6 shows the options that you can specify to list and display health monitors.

Table 17-6. Options for Listing and Displaying Health Monitors

Option	Description
`–instanceid` *instance_id*	Specifies a health monitor instance
`–list`	Displays the existing health monitors if a health monitor ID is not specified.
`–list –monitorid` *monitor_id*	Displays the monitor instances for the specified health monitor ID.
`–monitorid` *monitor_id*	Specifies a health monitor ID.

Examples

List all existing health monitors in XML using Unicode characters.

```
vdmadmin –H –list –xml
```

List all instances of the vCenter monitor (VCMonitor) in XML using ASCII characters.

```
vdmadmin –H –list –monitorid VCMonitor –xml –n
```

Display the health of a specified vCenter monitor instance.

```
vdmadmin –H –monitorid VCMonitor –instanceid 4aec2c99–4879–96b2–de408064d035 –xml
```

Listing and Displaying Reports of View Manager Operation Using the -I Option

You can use the `vdmadmin` command with the `–I` option to list the available reports of View Manager operation and to display the results of running one of these reports.

Syntax

```
vdmadmin –I [–b authentication_arguments] –list [–xml] [–w | –n]
```

```
vdmadmin –I [–b authentication_arguments] –report report –view view [–startdate yyyy–MM–dd–HH:mm:ss][–enddate yyyy–MM–dd–HH:mm:ss] [–w | –n] –xml | –csv
```

Usage Notes

You can use the command to display the available reports and views, and to display the information that View Manager has recorded for a specified report and view.

Options

Table 17-7 shows the options that you can specify to list and display reports and views.

Table 17-7. Options for Listing and Displaying Reports and Views

Option	Description
`–enddate` *yyyy-MM-dd-HH:mm:ss*	Specifies a upper limit for the date of information to be displayed.
`–list`	Lists the available reports and views.
`–report` *report*	Specifies a report.
`–startdate` *yyyy-MM-dd-HH:mm:ss*	Specifies a lower limit for the date of information to be displayed.
`–view` *view*	Specifies a view.

Examples

List the available reports and views in XML using Unicode characters.

```
vdmadmin –I –list –xml –w
```

Display a list of user events that occurred since August 1, 2010 as comma-separated values using ASCII characters.

```
vdmadmin –I –report events –view user_events –startdate 2010–08–01–00:00:00 –csv –n
```

Assigning Dedicated Desktops Using the -L Option

You can use the `vdmadmin` command with the `–L` option to assign desktops from a dedicated pool to users.

Syntax

```
vdmadmin –L [–b authentication_arguments] –d desktop –m  machine –u domain\user
```

```
vdmadmin –L [–b authentication_arguments] –d desktop [–m machine | –u domain\user] –r
```

Usage Notes

View Manager assigns desktops to users when they first connect to a dedicated desktop pool. Under some circumstances, you might want to preassign desktops to users. For example, you might want to prepare their system environments in advance of their initial connection. After a user connects to a desktop that View Manager assigns from a dedicated pool, that desktop remains assigned to the user for the life span of the desktop source. You can assign a user to a single virtual machine in a dedicated pool.

You can assign a desktop to any entitled user. You might want to do this when recovering from the loss of View LDAP data on a View Connection Server instance, or when you want to change ownership of a particular desktop source.

After a user connects to a desktop that View Manager assigns from a dedicated pool, that desktop remains assigned to the user for the life span of the desktop source. You might want to remove the assignment of a desktop to a user who has left the organization, who no longer requires access to the desktop, or who will use a desktop in a different desktop pool. You can also remove assignments for all users who access a desktop pool.

Options

Table 17-8 shows the options that you can specify to assign a desktop to a user or to remove an assignment.

Table 17-8. Options for Assigning Dedicated Desktops

Option	Description
`-d` *desktop*	Specifies the name of the desktop pool.
`-m` *machine*	Specifies the name of the virtual machine.
`-r`	Removes an assignment to a specified user, or all assignments to a specified machine.
`-u` *domain\user*	Specifies the login name and domain of the user.

Examples

Assign the machine machine2 in the desktop pool dtpool1 to the user Jo in the CORP domain.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

Remove the assignments for the user Jo in the CORP domain to desktops in the pool dtpool1.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

Remove all user assignments to the machine machine1 in the desktop pool dtpool3.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

Displaying Information About Machines Using the -M Option

You can use the `vdmadmin` command with the `-M` option to display information about the configuration of virtual machines or physical computers.

Syntax

```
vdmadmin -M [-b authentication_arguments] [-m machine | [[-u domain\user][-d desktop]] [-xml |
-csv] [-w | -n]
```

Usage Notes

The command displays information about a desktop's underlying virtual machine or physical computer.

- Display name of the machine.
- Name of the desktop pool.
- State of the machine.
- SID of the assigned user.
- Account name of the assigned user.
- Domain name of the assigned user.
- Offline status of a local desktop (not applicable to release 4.0 or earlier).
- Inventory path of the virtual machine (if applicable).
- Date on which the machine was created.
- Template path of the machine (if applicable).
- URL of the vCenter Server (if applicable).

Options

Table 17-9 shows the options that you can use to specify the machine whose details you want to display.

Table 17-9. Options for Displaying Information About Machines

Option	Description
–d *desktop*	Specifies the name of the desktop pool.
–m *machine*	Specifies the name of the virtual machine.
–u *domain\user*	Specifies the login name and domain of the user.

Examples

Display information about the underlying machine for the desktop in the pool dtpool2 that is assigned to the user Jo in the CORP domain and format the output as XML using ASCII characters.

```
vdmadmin –M –u CORP\Jo –d dtpool2 –xml –n
```

Display information about the machine machine3 and format the output as comma-separated values.

```
vdmadmin –M –m machine3 –csv
```

Configuring Domain Filters Using the -N Option

You can use the `vdmadmin` command with the `–N` option to control the domains that View Manager makes available to end users.

Syntax

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain
–add [–s connsvr]
```

```
vdmadmin –N [–b authentication_arguments] –domains –list [–w | –n] [–xml]
```

```
vdmadmin –N [–b authentication_arguments] –domains –list –active [–w | –n] [–xml]
```

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –domain domain
–remove [–s connsvr]
```

```
vdmadmin –N [–b authentication_arguments] –domains {–exclude | –include | –search} –removeall [–s
connsvr]
```

Usage Notes

Specify one of the `–exclude`, `–include`, or `–search` options to apply an operation to the exclusion list, inclusion list, or search exclusion list respectively.

If you add a domain to a search exclusion list, the domain is excluded from an automated domain search.

If you add a domain to an inclusion list, the domain is included in the results of the search.

If you add a domain to an exclusion list, the domain is excluded from the results of the search.

Options

Table 17-10 shows the options that you can specify to configure domain filters.

Table 17-10. Options for Configuring Domain Filters

Option	Description
–add	Adds a domain to a list.
–domain *domain*	Specifies the domain to be filtered. You must specify domains by their NetBIOS names and not by their DNS names.

Table 17-10. Options for Configuring Domain Filters (Continued)

Option	Description
–domains	Specifies a domain filter operation.
–exclude	Specifies an operation on a exclusion list.
–include	Specifies an operation on an inclusion list.
–list	Displays the domains that are configured in the search exclusion list, exclusion list, and inclusion list on each View Connection Server instance and for the View Connection Server group.
–list –active	Displays the available domains for the View Connection Server instance on which you run the command.
–remove	Removes a domain from a list.
–removeall	Removes all domains from a list.
–s *connsvr*	Specifies that the operation applies to the domain filters on a View Connection Server instance. You can specify the View Connection Server instance by its name or IP address. If you do not specify this option, any change that you make to the search configuration applies to all View Connection Server instances in the group.
–search	Specifies an operation on a search exclusion list.

Examples

Add the domain FARDOM to the search exclusion list for the View Connection Server instance csvr1.

```
vdmadmin –N –domains –search –domain FARDOM –add –s csvr1
```

Add the domain NEARDOM to the exclusion list for a View Connection Server group.

```
vdmadmin –N –domains –exclude –domain NEARDOM –add
```

Display the domain search configuration on both View Connection Server instances in the group, and for the group.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

View Manager limits the domain search on each View Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that View Manager excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

Display the domain filters in XML using ASCII characters.

```
vdmadmin –N –domains –list –xml –n
```

Display the domains that are available to View Manager on the local View Connection Server instance.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Display the available domains in XML using ASCII characters.

```
vdmadmin –N –domains –list –active –xml –n
```

Remove the domain NEARDOM from the exclusion list for a View Connection Server group.

```
vdmadmin –N –domains –exclude –domain NEARDOM –remove
```

Remove all domains from the inclusion list for the View Connection Server instance csvr1.

```
vdmadmin –N –domains –include –removeall –s csvr1
```

Configuring Domain Filters

You can configure domain filters to limit the domains that a View Connection Server instance or security server makes available to end users.

View Manager determines which domains are accessible by traversing trust relationships, starting with the domain in which a View Connection Server instance or security server resides. For a small, well-connected set of domains, View Manager can quickly determine a full list of domains, but the time that this operation takes increases as the number of domains increases or as the connectivity between the domains decreases. View Manager might also include domains in the search results that you would prefer not to offer to users when they log in to their desktops.

If you have previously set the value of the Windows registry key that controls recursive domain enumeration (`HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum`) to false, recursive domain searching is disabled, and the View Connection Server instance uses only the primary domain. To use the domain filtering feature, delete the registry key or set its value to true, and restart the system. You must do this for every View Connection Server instance on which you have set this key.

Table 17-11 shows the types of domain lists that you can specify to configure domain filtering.

Table 17-11. Types of Domain List

Domain List Type	Description
Search exclusion list	Specifies the domains that View Manager can traverse during an automated search. The search ignores domains that are included in the search exclusion list, and does not attempt to locate domains that the excluded domain trusts. You cannot exclude the primary domain from the search.
Exclusion list	Specifies the domains that View Manager excludes from the results of a domain search. You cannot exclude the primary domain.
Inclusion list	Specifies the domains that View Manager does not exclude from the results of a domain search. All other domains are removed apart from the primary domain.

The automated domain search retrieves a list of domains, excluding those domains that you specify in the search exclusion list and domains that are trusted by those excluded domains. View Manager selects the first non-empty exclusion or inclusion list in this order.

1 Exclusion list configured for the View Connection Server instance.

2 Exclusion list configured for the View Connection Server group.

3 Inclusion list configured for the View Connection Server instance.

4 Inclusion list configured for the View Connection Server group

View Manager applies only the first list that it selects to the search results.

If you specify a domain for inclusion, and its domain controller is not currently accessible, View Manager does not include that domain in the list of active domains.

You cannot exclude the primary domain to which a View Connection Server instance or security server belongs.

Example of Filtering to Include Domains

You can use an inclusion list to specify the domains that View Manager does not exclude from the results of a domain search. All other domains, apart from the primary domain, are removed.

A View Connection Server instance is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX domain.

Display the currently active domains for the View Connection Server instance.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains appear in the list because they are trusted domains of the DEPTX domain.

Specify that the View Connection Server instance should make only the YOURDOM and DEPTX domains available, in addition to the primary MYDOM domain.

```
vdmadmin –N –domains –include –domain YOURDOM –add
vdmadmin –N –domains –include –domain DEPTX –add
```

Display the currently active domains after including the YOURDOM and DEPTX domains.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR)
===========================
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

View Manager applies the include list to the results of a domain search. If the domain hierarchy is very complex or network connectivity to some domains is poor, the domain search can be slow. In such cases, use search exclusion instead.

Example of Filtering to Exclude Domains

You can use an inclusion list to specify the domains that View Manager excludes from the results of a domain search.

A group of two View Connection Server instances, CONSVR-1 and CONSVR-2, is joined to the primary MYDOM domain and has a trusted relationship with the YOURDOM domain. The YOURDOM domain has a trusted relationship with the DEPTX and FARDOM domains.

The FARDOM domain is in a remote geographical location, and network connectivity to that domain is over a slow, high-latency link. There is no requirement for users in the FARDOM domain to be able to access the View Connection Server group in the MYDOM domain.

Display the currently active domains for a member of the View Connection Server group.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

The DEPTY and DEPTZ domains are trusted domains of the DEPTX domain.

To improve connection performance for View clients, exclude the FARDOM domain from being searched by the View Connection Server group.

```
vdmadmin –N –domains –search –domain FARDOM –add
```

The command displays the currently active domains after excluding the FARDOM domain from the search.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

Extend the search exclusion list to exclude the DEPTX domain and all its trusted domains from the domain search for all View Connection Server instances in a group. Also, exclude the YOURDOM domain from being available on CONSVR-1.

```
vdmadmin –N –domains –search –domain DEPTX –add
vdmadmin –N –domains –exclude –domain YOURDOM –add –s CONSVR–1
```

Display the new domain search configuration.

```
C:\ vdmadmin –N –domains –list

Domain Configuration
====================
Cluster Settings
   Include:
   Exclude:
   Search :
     FARDOM
     DEPTX

Broker Settings: CONSVR–1
   Include:
(*)Exclude:
     YOURDOM
   Search :

Broker Settings: CONSVR–2
   Include:
   Exclude:
   Search :
```

View Manager limits the domain search on each View Connection Server host in the group to exclude the domains FARDOM and DEPTX. The characters (*) next to the exclusion list for CONSVR-1 indicates that View Manager excludes the YOURDOM domain from the results of the domain search on CONSVR-1.

On CONSVR-1, display the currently active domains.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–1)
=============================
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

On CONSVR-2, display the currently active domains.

```
C:\ vdmadmin –N –domains –list –active

Domain Information (CONSVR–2)
=============================
```

```
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options

You can use the `vdmadmin` command with the `–O` and `–P` options to display the desktops and policies that are assigned to users who are no longer entitled to use the system.

Syntax

`vdmadmin –O [–b` *`authentication_arguments`*`] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath` *`path`*`]]`

`vdmadmin –P [–b` *`authentication_arguments`*`] [–ld | –lu] [–w | –n] [–xml [–noxslt | –xsltpath` *`path`*`]]`

Usage Notes

If you revoke a user's entitlement to a persistent desktop or to a physical system, the associated desktop assignment is not automatically revoked. This condition might be acceptable if you have temporarily suspended a user's account or if the user is on a sabbatical. When you reenable entitlement, the user can continue using the same desktop as previously. If a user has left the organization, other users cannot access the desktop, and it is considered to be orphaned. You might also want to examine any policies that are assigned to unentitled users.

Options

Table 17-12 shows the options that you can specify to display the desktops and policies of unentitled users.

Table 17-12. Options for Displaying the Desktops and Policies of Unentitled Users

Option	Description
`–ld`	Orders output entries by desktop.
`–lu`	Orders output entries by user.
`–noxslt`	Specifies that the default stylesheet should not be applied to the XML output.
`–xsltpath` *path*	Specifies the path to the stylesheet that is used to transform XML output.

Table 17-13 shows the stylesheets that you can apply to the XML output to transform it into HTML. The stylesheets are located in the directory `C:\Program Files\VMware\VMware View\server\etc`.

Table 17-13. XSL Stylesheets

Stylesheet File Name	Description
`list–checkedout–unentitled.xsl`	Transforms reports containing a list of desktops that are checked out by unentitled users.
`unentitled–machines.xsl`	Transforms reports containing a list of unentitled desktops, grouped either by user or system, and which are currently assigned to a user. This is the default stylesheet.
`unentitled–policies.xsl`	Transforms reports containing a list of desktops with user-level policies that are applied to unentitled users.

Examples

Display the desktops that are assigned to unentitled users, grouped by desktop in text format.

```
vdmadmin -O -ld
```

Display desktops that are assigned to unentitled users, grouped by user, in XML format using ASCII characters.

```
vdmadmin -O -lu -xml -n
```

Apply your own stylesheet `C:\tmp\unentitled-users.xsl` and redirect the output to the file `uu-output.html`.

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

Display the user policies that are associated with unentitled users' desktops, grouped by desktop, in XML format using Unicode characters.

```
vdmadmin -P -ld -xml -w
```

Apply your own stylesheet `C:\tmp\unentitled-policies.xsl` and redirect the output to the file `up-output.html`.

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

Configuring Clients in Kiosk Mode Using the -Q Option

You can use the `vdmadmin` command with the `-Q` option to set defaults and create accounts for clients in kiosk mode, to enable authentication for these clients, and to display information about their configuration.

Syntax

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup] [-description "description_text"]
```

```
vdmadmin -Q -disable [-b authentication_arguments] -s connection_server
```

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdmadmin -Q -clientauth -getdefaults [-b authentication_arguments] [-xml]
```

```
vdmadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

```
vdmadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdmadmin -Q -clientauth -removeall [-b authentication_arguments] [-force]
```

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword | -noexpirepassword ] [-group group_name | -nogroup]
```

```
vdmadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-description "description_text"]
```

Usage Notes

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients use to connect to their desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all View Connection Server instances in a group.

When you add a client in kiosk mode, View Manager creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with the characters "custom-" or with one of the alternate strings that you can define in ADAM, and it cannot be more than 20 characters long. You should use each specified name with no more than one client device.

You can define alternate prefixes to "custom-" in the `pae-ClientAuthPrefix` multi-valued attribute under `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` in ADAM on a View Connection Server instance. Avoid using these prefixes with ordinary user accounts.

If you do not specify a name for a client, View Manager generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with View Connection Server instances that you enable to authenticate clients.

Some thin clients allow only account names that start with the characters "custom-" or "cm-" to be used with kiosk mode.

An automatically generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, you must use the `-password` option to specify the password.

If you use the `-group` option to specify a group or you have previously set a default group, View Manager adds the client's account to this group. You can specify the `-nogroup` option to prevent the account being added to any group.

If you enable a View Connection Server instance to authenticate clients in kiosk mode, you can optionally specify that clients must provide a password. If you disable authentication, clients cannot connect to their desktops.

Although you enable or disable authentication for an individual View Connection Server instance, all View Connection Server instances in a group share all other settings for client authentication. You need only add a client once for all View Connection Server instances in a group to be capable of accepting requests from the client.

If you specify the `-requirepassword` option when enabling authentication, the View Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a View Connection Server instance to specify this option, such clients cannot authenticate themselves, and they fail with the error message `Unknown username or bad password`.

Options

Table 17-14 shows the options that you can specify to configure clients in kiosk mode.

Table 17-14. Options for Configuring Clients in Kiosk Mode

Option	Description
`-add`	Adds an account for a client in kiosk mode.
`-clientauth`	Specifies an operation that configures authentication for a client in kiosk mode.
`-clientid` *client_id*	Specifies the name or the MAC address of the client.
`-description` "*description_text*"	Creates a description of the account for the client device in Active Directory.
`-disable`	Disables authentication of clients in kiosk mode on a specified View Connection Server instance.
`-domain` *domain_name*	Specifies the domain for the account for the client device.
`-enable`	Enables authentication of clients in kiosk mode on a specified View Connection Server instance.

Table 17-14. Options for Configuring Clients in Kiosk Mode (Continued)

Option	Description
`–expirepassword`	Specifies that the expiry time for the password on client accounts is the same as for the View Connection Server group. If no expiry time is defined for the group, passwords do not expire.
`–force`	Disables the confirmation prompt when removing the account for a client in kiosk mode.
`–genpassword`	Generates a password for the client's account. This is the default behavior if you do not specify either `–password` or `–genpassword`.
`–getdefaults`	Gets the default values that are used for adding client accounts.
`–group` *group_name*	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.
`–list`	Displays information about clients in kiosk mode and about the View Connection Server instances on which you have enabled authentication of clients in kiosk mode.
`–noexpirepassword`	Specifies that the password on an account does not expire.
`–nogroup`	When adding an account for a client, specifies that the client's account is not added to the default group. When setting the default values for clients, clears the setting for the default group.
`–ou` *DN*	Specifies the distinguished name of the organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com **Note** You cannot use the `–setdefaults` option to change the configuration of an organizational unit.
`–password` "*password*"	Specifies an explicit password for the client's account.
`–remove`	Removes the account for a client in kiosk mode.
`–removeall`	Removes the accounts of all clients in kiosk mode.
`–requirepassword`	Specifies that clients in kiosk mode must provide passwords. View Manager will not accept generated passwords for new connections.
`–s` *connection_server*	Specifies the NetBIOS name of the View Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.
`–setdefaults`	Sets the default values that are used for adding client accounts.
`–update`	Updates an account for a client in kiosk mode.

Examples

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group
kc–grp
```

Get the current default values for clients in plain text format.

```
vdmadmin –Q –clientauth –getdefaults
```

Get the current default values for clients in XML format.

```
vdmadmin –Q –clientauth –getdefaults –xml
```

Add an account for a client specified by its MAC address to the MYORG domain, and use the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, and use an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –genpassword –ou "OU=kiosk–ou,DC=myorg,DC=com" –group kc–grp
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou "OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Update an account for a client, specifying a new password and descriptive text.

```
vdmadmin –Q –clientauth –update –domain MYORG –clientid custom–Terminal21 –password "Secret1!" –description "Foyer Entry Workstation"
```

Remove the account for a kiosk client specified by its MAC address from the MYORG domain.

```
vdmadmin –Q –clientauth –remove –domain MYORG –clientid 00:10:db:ee:54:12
```

Remove the accounts of all clients without prompting to confirm the removal.

```
vdmadmin –Q –clientauth –removeall –force
```

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to View Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

Disable authentication of clients for the View Connection Server instance csvr-1.

```
vdmadmin –Q –disable –s csvr–1
```

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to View Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password, and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
```

```
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

Displaying the First User of a Desktop Using the -R Option

You can use the `vdmadmin` command with the `–R` option to find out the initial assignment of a managed desktop. For example, in the event of the loss of LDAP data, you might need this information so that you can reassign desktops to users.

Syntax

```
vdmadmin –R –i network_address
```

Usage Notes

You cannot use the `–b` option to run this command as a privileged user. You must be logged in as a user in the **Administrator** role.

Options

The `–i` option specifies the IP address of the desktop.

Examples

Display the first user who accessed the machine at the IP address 10.20.34.120.

```
vdmadmin –R –i 10.20.34.120
```

Removing the Entry for a View Connection Server Instance Using the -S Option

You can use the `vdmadmin` command with the `–S` option to remove the entry for a View Connection Server instance from the View Manager configuration.

Syntax

```
vdmadmin –S [–b authentication_arguments] –r –s server
```

Usage Notes

To ensure high availability, View Manager allows you to configure one or more replica View Connection Server instances in a View Connection Server group. If you disable a View Connection Server instance in a group, the entry for the server persists within the View Manager configuration.

To make the removal permanent, perform these tasks:

1 Uninstall the View Connection Server instance from the Windows Server computer by running the View Connection Server installer.

2 Remove the Adam Instance VMwareVDMDS program from the Windows Server computer by running the Add or Remove Programs tool.

3 On another View Connection Server instance, use the `vdmadmin` command to remove the entry for the uninstalled View Connection Server instance from the configuration.

If you want to reinstall VMware View on the removed systems without replicating the View configuration of the original group, restart all the View Connection Server hosts in the original group before performing the reinstallation. This prevents the reinstalled View Connection Server instances from receiving configuration updates from their original group.

Options

The `–s` option specifies the NetBIOS name of the View Connection Server instance to be removed.

Examples

Remove the entry for the View Connection Server instance connsvr3.

```
vdmadmin –S –r –s connsvr3
```

Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option

You can use the `vdmadmin` command with the `–T` option to set the split limit for publishing View Transfer Server packages. You might want to specify a split limit if you use a proxy cache that defines a maximum object size for its cache.

Syntax

```
vdmadmin –T [–packagelimit  size]
```

Usage Notes

On a network with a proxy cache, you can improve performance by limiting the size of published View Transfer Server package files so that they are no larger than the maximum object size of the cache. If you specify a split limit, View Transfer Server divides a package file into parts that are no larger than the limit.

Options

The `–packagelimit` option specifies the size of the split limit in bytes. If you do not specify this option, the command returns the current split limit.

Examples

Set the split limit to 100MB.

```
vdmadmin –T –packagelimit 104857600
```

Display the current split limit.

```
vdmadmin –T
```

Displaying Information About Users Using the -U Option

You can use the `vdmadmin` command with the `–U` option to display detailed information about users.

Syntax

```
vdmadmin –U [–b authentication_arguments] –u domain\user [–w | –n] [–xml]
```

Usage Notes

The command displays information about a user obtained from Active Directory and View Manager.

- Details from Active Directory about the user's account.
- Membership of Active Directory groups.
- Desktop entitlements including the desktop ID, display name, description, folder, and whether a desktop has been disabled.
- ThinApp assignments.
- Administrator roles including the administrative rights of a user and the folders in which they have those rights.

Options

The `–u` option specifies the name and domain of the user.

Examples

Display information about the user Jo in the CORP domain in XML using ASCII characters.

```
vdmadmin –U –u CORP\Jo –n –xml
```

Decrypting the Virtual Machine of a Local Desktop Using the -V Option

VMware View secures the virtual machine of a local desktop by encrypting its base image. If you are not able to power on or check in the local desktop, you can use the `vdmadmin` command with the `–V` option to decrypt the virtual machine so that you can recover data from it.

Syntax

```
vdmadmin –V –rescue [–b authentication_arguments] –d desktop –u domain\user –infile path_to_VM_file
```

Usage Notes

To decrypt a full virtual machine, copy all of the virtual machine files from the client machine. Specify the name of the VMware virtual machine configuration file (VMX file) as the argument to the `–infile` option.

To decrypt a single disk from a virtual machine, copy all of the VMware virtual disk files (VMDK files) that correspond to that disk. If you created the local desktop from a linked-clone desktop, you must also copy the subfolder that contains the VMDK files for the base image. Specify the name of the VMDK file for the disk as the argument to the `–infile` option. Do not specify a VMDK file that corresponds to a disk slice.

The `vdmadmin` command writes the decrypted files to a subfolder named `rescued`.

The decryption fails if the correct authentication key is not available in the View LDAP configuration, or if any of the required virtual machine files are corrupted or missing.

Options

Table 17-15 shows the options that you must specify to decrypt a full virtual machine or one of its disks.

Table 17-15. Options for Decrypting the Virtual Machine of a Local Desktop

Option	Description
`-d` *desktop*	Specifies the name of the desktop pool.
`-infile` *path_to_VM_file*	Specifies the path to the VMX or VMDK file for the local desktop's virtual machine.
`-u` *domain\user*	Specifies the domain and name of the local desktop's end user.

Examples

Decrypt a full virtual machine by specifying its VMX file.

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile
"J:\Temp\LMDT_Recovery\CN=lmdtpool,OU=Applications,DC=mycorp,DC=com.vmx"
```

Decrypt the current version of the virtual machine's `scsi00` disk by specifying its VMDK file.

```
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile
"J:\Temp\LMDT_Recovery\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk"
```

Unlocking or Locking Virtual Machines Using the -V Option

You can use the `vdmadmin` command with the `-V` option to unlock or lock virtual machines in the datacenter.

Syntax

```
vdmadmin -V [-b authentication_arguments] -e -d desktop -m machine [-m machine] ...

vdmadmin -V [-b authentication_arguments] -e -vcdn vCenter_dn -vmpath inventory_path

vdmadmin -V [-b authentication_arguments] -p -d desktop -m machine [-m machine] ...

vdmadmin -V [-b authentication_arguments] -p -vcdn vCenter_dn -vmpath inventory_path
```

Usage Notes

You should only use the `vdmadmin` command to unlock or lock a virtual machine if you encounter a problem that has left a View desktop in an incorrect state. Do not use the command to administer desktops that are operating normally. For example, do not use `vdmadmin` to unlock a checked-out remote desktop if you can use View Administrator to roll back the local session.

If a desktop is locked and cannot be rolled back, and the entry for its virtual machine exists in ADAM, use the `-d` and `-m` options to specify the desktop pool and virtual machine for the desktop that you want to unlock. You can use the `vdmadmin-M` command to discover the name of the virtual machine that is assigned to a user.

If a desktop is locked and the entry for its virtual machine no longer exists in ADAM, use the `-vmpath` and `-vcdn` options to specify the inventory path of the virtual machine and the vCenter Server. You can use vCenter Client to find out the inventory path of a virtual machine for a desktop or View Transfer Server instance under `Home/Inventory/VMs and Templates`. You can use ADAM ADSI Edit to find out the distinguished name of the vCenter Server under the `OU=Properties` heading.

Options

Table 17-16 shows the options that you can specify to unlock or lock virtual machines.

Table 17-16. Options for Unlocking or Locking Virtual Machines

Option	Description
`-d` *desktop*	Specifies the desktop pool.
`-e`	Unlocks a virtual machine.
`-m` *machine*	Specifies the name of the virtual machine.
`-p`	Locks a virtual machine.
`-vcdn` *vCenter_dn*	Specifies the distinguished name of the vCenter Server.
`-vmpath` *inventory_path*	Specifies the inventory path of the virtual machine.

Examples

Unlock the virtual machines machine 1 and machine2 in desktop pool dtpool3.

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

Unlock the virtual machine for a View Transfer Server instance on a vCenter Server.

```
vdmadmin -V -e -vcdn  "CN=f1060058-
dde2-4940-947b-5d83757b1787,OU=VirtualCenter,OU=Properties,DC=myorg,DC=com" -vmpath
"/DataCenter1/vm/Desktops/LocalMode/LDwin7"
```

Lock the virtual machine machine3 in desktop pool dtpool3.

```
vdmadmin -V -p -d dtpool3 -m machine3
```

Detecting and Resolving LDAP Entry Collisions Using the -X Option

You can use the `vdmadmin` command with the `-X` option to detect and resolve colliding LDAP entries on replicated View Connection Server instances in a group.

Syntax

```
vdmadmin -X [-b authentication_arguments] -collisions [-resolve]
```

Usage Notes

If duplicate LDAP entries are created on two or more View Connection Server instances, this can cause problems with the integrity of LDAP data in View. For example, this condition can happen during an upgrade while LDAP replication is inoperative. Although View Manager checks for this error condition at regular intervals, you can run the `vdmadmin` command on one of the View Connection Server instances in the group to detect and resolve LDAP entry collisions manually.

Options

Table 17-17 shows the options that you can specify to detect and resolve colliding LDAP entries.

Table 17-17. Options for Detecting and Resolving LDAP Entry Collisions

Option	Description
`–collisions`	Specifies an operation for detecting LDAP collisions in a View Connection Server group.
`–resolve`	Resolves all detected LDAP collisions.

Examples

Detect LDAP entry collisions in a View Connection Server group.

```
vdmadmin –X –collisions
```

Detect and resolve LDAP entry collisions.

```
vdmadmin –X –collisions –resolve
```

18 Setting Up Clients in Kiosk Mode

You can set up unattended clients that can obtain access to their desktops from VMware View.

A client in kiosk mode is a thin client or a lock-down PC that runs View Client to connect to a View Connection Server instance and launch a remote session. End users do not typically need to log in to access the client device, although the desktop might require them to provide authentication information for some applications. Sample applications include medical data entry workstations, airline check-in stations, customer self-service points, and information terminals for public access.

You should ensure that the desktop application implements authentication mechanisms for secure transactions, that the physical network is secure against tampering and snooping, and that all devices connected to the network are trusted.

Clients in kiosk mode support the standard features for remote access such as automatic redirection of USB devices to the remote session and location-based printing.

View Manager uses the Flexible Authentication feature in VMware View 4.5 and later to authenticate a client device in kiosk mode rather than the end user. You can configure a View Connection Server instance to authenticate clients that identify themselves by their MAC address or by a user name that starts with the characters "custom-" or with an alternate prefix string that you have defined in ADAM. If you configure a client to have an automatically generated password, you can run View Client on the device without specifying a password. If you configure an explicit password, you must specify this password to View Client. As you would usually run View Client from a script, and the password would appear in clear text, you should take precautions to make the script unreadable by unprivileged users.

Only View Connection Server instances that you enable to authenticate clients in kiosk mode can accept connections from accounts that start with the characters "cm-" followed by a MAC address, or that start with the characters "custom-" or an alternate string that you have defined. View Client in VMware View 4.5 and later does not allow the manual entry of user names that take these forms.

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

Configure Clients in Kiosk Mode

To configure Active Directory and View Manager to support clients in kiosk mode, you must perform several tasks in sequence.

Prerequisites

Verify that you have the privileges required to perform the configuration tasks.

- **Domain Admins** or **Account Operators** credentials in Active Directory to make changes to the accounts of users and groups in a domain.

- **Administrators**, **Inventory Administrators**, or an equivalent role to use View Administrator to entitle users or groups to desktops.
- **Administrators** or an equivalent role to run the `vdmadmin` command.

Procedure

1 Prepare Active Directory and View Manager for Clients in Kiosk Mode on page 350

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

2 Set Default Values for Clients in Kiosk Mode on page 351

You can use the `vdmadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

3 Display the MAC Addresses of Client Devices on page 352

If you want to create an account for a client that is based on its MAC address, you can use View Client to discover the MAC address of the client device.

4 Add Accounts for Clients in Kiosk Mode on page 353

You can use the `vdmadmin` command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

5 Enable Authentication of Clients in Kiosk Mode on page 354

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their desktops via a View Connection Server instance.

6 Verify the Configuration of Clients in Kiosk Mode on page 355

You can use the `vdmadmin` command to display information about clients in kiosk mode and View Connection Server instances that are configured to authenticate such clients.

7 Connect to Desktops from Clients in Kiosk Mode on page 356

You can run View Client from the command line or use a script to connect a client to a remote session.

Prepare Active Directory and View Manager for Clients in Kiosk Mode

You must configure Active Directory to accept the accounts that you create to authenticate client devices. Whenever you create a group, you must also entitle that group to the desktop pool that a client accesses. You can also prepare the desktop pool that the clients use.

As a best practice, create a separate organizational unit and group to help minimize your work in administering clients in kiosk mode. You can add individual accounts for clients that do not belong to any group, but this creates a large administrative overhead if you configure more than a small number of clients.

Procedure

1 In Active Directory, create a separate organizational unit and group to use with clients in kiosk mode.

You must specify a pre-Windows 2000 name for the group. You use this name to identify the group to the `vdmadmin` command.

2 Create the image or template for the guest virtual machine.

You can use a virtual machine that is managed by vCenter Server as a template for an automated pool, as a parent for a linked-clone pool, or as the desktop source for a manual pool. You can also install and configure applications on the guest virtual machine.

3 Configure the guest virtual machine so that the clients are not locked when they are left unattended.

View suppresses the pre-login message for clients that connect in kiosk mode. If you require an event to unlock the screen and display a message, you can configure a suitable application on the guest virtual machine.

4 In View Administrator, create the desktop pool that the clients will use and entitle the group to this pool.

For example, you might choose to create a floating-assignment, linked-clone desktop pool as being most suitable for the requirements of your client application. You might also associate one or more ThinApp applications with the desktop pool.

IMPORTANT Do not entitle a client or a group to more than one desktop pool. If you do, View Manager assigns a desktop at random from the pools to which a client is entitled, and generates a warning event.

5 If you want to enable location-based printing for the clients, configure the Active Directory group policy setting `AutoConnect Location-based Printing for VMware View`, which is located in the Microsoft Group Policy Object Editor in the `Software Settings` folder under `Computer Configuration`.

6 Configure other policies that you need to optimize and secure the View desktops of the clients.

For example, you might want to override the policies that connect local USB devices to the desktop when it is launched or when the devices are plugged in. By default, View Client for Windows enables these policies for clients in kiosk mode.

Example: Preparing Active Directory for Clients in Kiosk Mode

A company intranet has a domain MYORG, and its organizational unit has the distinguished name OU=myorg-ou,DC=myorg,DC=com. In Active Directory, you create the organizational unit kiosk-ou with the distinguished name OU=kiosk-ou,DC=myorg,DC=com and the group kc-grp for use with clients in kiosk mode.

What to do next

Set default values for the clients.

Set Default Values for Clients in Kiosk Mode

You can use the `vdmadmin` command to set the default values for the organizational unit, password expiry, and group membership in Active Directory for clients in kiosk mode.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their desktops.

When you configure defaults for password expiry and Active Directory group membership, these settings are shared by all View Connection Server instances in a group.

Procedure

- Set the default values for clients.

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword
| -noexpirepassword ] [-group group_name | -nogroup]
```

Option	Description
-expirepassword	Specifies that the expiry time for passwords on the client accounts is the same as for the View Connection Server group. If no expiry time is defined for the group, passwords do not expire.
-group *group_name*	Specifies the name of the default group to which client accounts are added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory.
-noexpirepassword	Specifies that passwords on client accounts do not expire.

Option	Description
–nogroup	Clears the setting for the default group.
–ou *DN*	Specifies the distinguished name of the default organizational unit to which client accounts are added. For example: OU=kiosk-ou,DC=myorg,DC=com NOTE You cannot use the command to change the configuration of an organizational unit.

The command updates the default values for clients in the View Connection Server group.

Example: Setting Default Values for Cients in Kiosk Mode

Set the default values for the organizational unit, password expiry, and group membership of clients.

```
vdmadmin –Q –clientauth –setdefaults –ou "OU=kiosk–ou,DC=myorg,DC=com" –noexpirepassword –group
kc–grp
```

What to do next

Find out the MAC addresses of client devices that use their MAC address for authentication.

Display the MAC Addresses of Client Devices

If you want to create an account for a client that is based on its MAC address, you can use View Client to discover the MAC address of the client device.

Prerequisites

Log in on the console of the client.

Procedure

- To display the MAC address, type the appropriate command for your platform.

Option	Action
Windows	Enter **C:\Program Files\VMware\VMware View\Client\bin\wswc –printEnvironmentInfo** View Client uses the default View Connection Server instance that you configured for it. If you have not configured a default value, View Client prompts you for the value. The command displays the IP address, MAC address, and machine name of the client device.
Linux	Enter **vmware–view ––printEnvironmentInfo –s *connection_server*** You must specify the IP address or FQDN of the View Connection Server instance that View Client will use to connect to the desktop. The command displays the IP address, MAC address, machine name, domain, name and domain of any logged-on user, and time zone of the client device.

What to do next

Add accounts for the clients.

Add Accounts for Clients in Kiosk Mode

You can use the vdmadmin command to add accounts for clients to the configuration of a View Connection Server group. After you add a client, it is available for use with a View Connection Server instance on which you have enabled authentication of clients. You can also update the configuration of clients, or remove their accounts from the system.

You must run the vdmadmin command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their desktops.

When you add a client in kiosk mode, View Manager creates a user account for the client in Active Directory. If you specify a name for a client, this name must start with a recognized prefix string, such as "custom-", or with an alternate prefix string that you have defined in ADAM, and it cannot be more than 20 characters long. If you do not specify a name for a client, View Manager generates a name from the MAC address that you specify for the client device. For example, if the MAC address is 00:10:db:ee:76:80, the corresponding account name is cm-00_10_db_ee_76_80. You can only use these accounts with View Connection Server instances that you enable to authenticate clients.

IMPORTANT Do not use a specified name with more than one client device. Future releases might not support this configuration.

Procedure

- Run the vdmadmin command using the –domain and –clientid options to specify the domain and the name or the MAC address of the client.

  ```
  vdmadmin –Q –clientauth –add [–b authentication_arguments] –domain domain_name –clientid
  client_id [–password "password" | –genpassword] [–ou DN] [–expirepassword | –noexpirepassword]
  [–group group_name | –nogroup] [–description "description_text"]
  ```

Option	Description
–clientid *client_id*	Specifies the name or the MAC address of the client.
–description "*description_text*"	Creates a description of the account for the client device in Active Directory.
–domain *domain_name*	Specifies the domain for the client.
–expirepassword	Specifies that the expiry time for the password on the client's account is the same as for the View Connection Server group. If no expiry time is defined for the group, the password does not expire.
–genpassword	Generates a password for the client's account. This is the default behavior if you do not specify either –password or –genpassword. A generated password is 16 characters long, contains at least one uppercase letter, one lowercase letter, one symbol, and one number, and can contain repeated characters. If you require a stronger password, use the –password option to specify the password.
–group *group_name*	Specifies the name of the group to which the client's account is added. The name of the group must be specified as the pre-Windows 2000 group name from Active Directory. If you previously set a default group, client's account is added to this group.
–noexpirepassword	Specifies that the password on the client's account does not expire.
–nogroup	Specifies that the client's account is not added to the default group.
–ou *DN*	Specifies the distinguished name of the organizational unit to which the client's account is added. For example: OU=kiosk-ou,DC=myorg,DC=com
–password "*password*"	Specifies an explicit password for the client's account.

The command creates a user account in Active Directory for the client in the specified domain and group (if any).

Example: Adding Accounts for Clients

Add an account for a client specified by its MAC address to the MYORG domain, using the default settings for the group kc-grp.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a client specified by its MAC address to the MYORG domain, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid 00:10:db:ee:76:80 –group kc–grp
```

Add an account for a named client, and specify a password to be used with the client.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Terminal21 –password "guest" –ou
"OU=kiosk–ou,DC=myorg,DC=com" –description "Terminal 21"
```

Add an account for a named client, using an automatically generated password.

```
vdmadmin –Q –clientauth –add –domain MYORG –clientid custom–Kiosk11 –ou "OU=kiosk–
ou,DC=myorg,DC=com" –description "Kiosk 11"
```

What to do next

Enable authentication of the clients.

Enable Authentication of Clients in Kiosk Mode

You can use the `vdmadmin` command to enable authentication of clients that attempt to connect to their desktops via a View Connection Server instance.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their desktops.

Although you enable authentication for an individual View Connection Server instance, all View Connection Server instances in a group share all other settings for client authentication. You need only add an account for a client once. In a View Connection Server group, any enabled View Connection Server instance can authenticate the client.

Procedure

- Enable authentication of clients on a View Connection Server instance.

  ```
  vdmadmin –Q –enable [–b authentication_arguments] –s connection_server [–requirepassword]
  ```

Option	Description
–requirepassword	Specifies that you require clients to provide passwords. **IMPORTANT** If you specify this option, the View Connection Server instance cannot authenticate clients that have automatically generated passwords. If you change the configuration of a View Connection Server instance to specify this option, such clients cannot authenticate themselves and they fail with the error message `Unknown username or bad password`.
–s *connection_server*	Specifies the NetBIOS name of the View Connection Server instance on which to enable authentication of clients.

  The command enables the specified View Connection Server instance to authenticate clients.

Example: Enabling Authentication of Clients in Kiosk Mode

Enable authentication of clients for the View Connection Server instance csvr-2. Clients with automatically generated passwords can authenticate themselves without providing a password.

```
vdmadmin –Q –enable –s csvr–2
```

Enable authentication of clients for the View Connection Server instance csvr-3, and require that the clients specify their passwords to View Client. Clients with automatically generated passwords cannot authenticate themselves.

```
vdmadmin –Q –enable –s csvr–3 –requirepassword
```

What to do next

Verify the configuration of the View Connection Server instances and the clients.

Verify the Configuration of Clients in Kiosk Mode

You can use the `vdmadmin` command to display information about clients in kiosk mode and View Connection Server instances that are configured to authenticate such clients.

You must run the `vdmadmin` command on one of the View Connection Server instances in the group that contains the View Connection Server instance that clients will use to connect to their desktops.

Procedure

- Display information about clients in kiosk mode and client authentication.

  ```
  vdmadmin –Q –clientauth –list [–b authentication_arguments] [–xml]
  ```

  The command displays information about clients in kiosk mode and the View Connection Server instances on which you have enabled client authentication.

Example: Displaying Information for Clients in Kiosk Mode

Display information about clients in text format. Client cm-00_0c_29_0d_a3_e6 has an automatically generated password, and does not require an end user or an application script to specify this password to View Client. Client cm-00_22_19_12_6d_cf has an explicitly specified password and requires the end user to provide this. The View Connection Server instance CONSVR2 accepts authentication requests from clients with automatically generated passwords. CONSVR1 does not accept authentication requests from clients in kiosk mode.

```
C:\ vdmadmin –Q –clientauth –list
Client Authentication User List
================================
GUID              : 94be6344–0c9b–4a92–8d54–1brc1c2dc282
ClientID          : cm–00_0c_29_0d_a3_e6
Domain            : myorg.com
Password Generated: true

GUID              : 471d9d35–68b2–40ee–b693–56a7d92b2e25
ClientID          : cm–00_22_19_12_6d_cf
Domain            : myorg.com
Password Generated: false

Client Authentication Connection Servers
========================================
Common Name                   : CONSVR1
Client Authentication Enabled : false
Password Required             : false

Common Name                   : CONSVR2
Client Authentication Enabled : true
Password Required             : false
```

What to do next

Verify that the clients can connect to their desktops.

Connect to Desktops from Clients in Kiosk Mode

You can run View Client from the command line or use a script to connect a client to a remote session.

You would usually use a command script to run View Client on a deployed client device.

For an example of a script that runs View Client on a Windows system, examine the file `C:\Program Files\VMware\VMware View\Client\bin\kiosk_mode.cmd`.

NOTE On a Windows client, USB devices on the client are not forwarded automatically if they are in use by another application or service when the desktop session starts. You must ensure that you have installed the drivers on the client for any device that you want to forward. On both Windows and Linux clients, human interface devices (HIDs) and smart card readers are not forwarded by default.

Procedure

- To connect to a remote session, type the appropriate command for your platform.

Option	Description	
Windows	Enter **C:\Program Files\VMware\VMware View\Client\bin\wswc –unattended [–serverURL *connection_server*] [–userName *user_name*] [–password *password*]**	
	–password *password*	Specifies the password for the client's account. If you defined a password for the account, you must specify this password.
	–serverURL *connection_server*	Specifies the IP address or FQDN of the View Connection Server instance that View Client will use to connect to its desktop. If you do not specify the IP address or FQDN of the View Connection Server instance that View Client will use to connect to its desktop, View Client uses the default View Connection Server instance that you configured for it.
	–userName *user_name*	Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.
Linux	Enter **vmware-view --unattended -s *connection_server* [--once] [-u *user_name*] [-p *password*]**	
	--once	Specifies that you do not want View Client to retry connecting in the case of an error occurring. IMPORTANT You should usually specify this option, and use the exit code to handle the error. Otherwise, you might find it difficult to kill the `vmware-view` process remotely.
	-p *password*	Specifies the password for the client's account. If you defined a password for the account, you must specify this password.
	-s *connection_server*	Specifies the IP address or FQDN of the View Connection Server instance that View Client will use to connect to its desktop.
	-u *user_name*	Specifies the name of the client's account. If you want a client to authenticate itself using an account name that begins with a recognized prefix string, such as "custom-", rather than using its MAC address, you must specify this name.

If View Manager authenticates the kiosk client and a View desktop is available, the command starts the remote session.

Example: Running View Client on Clients in Kiosk Mode

Run View Client on a Windows client whose account name is based on its MAC address, and which has an automatically generated password.

```
C:\Program Files\VMware\VMware View\Client\bin\wswc –unattended –serverURL consvr2.myorg.com
```

Run View Client on a Linux client using an assigned name and password.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Running View Client from the Command Line

19

You can run View Client for Windows from the command line or from scripts. You might want to do this if you are implementing a kiosk-based application that grants end users access to desktop applications.

You use the `wswc` command to run the View Client for Windows from the command line. The command includes options that you can specify to change the behavior of View Client.

This chapter includes the following topics:

View Client Command Usage

The syntax of the `wswc` command controls the operation of View Client.

Use the following form of the `wswc` command from a Windows command prompt.

`wswc [`*`command_line_option`* `[`*`argument`*`]] ...`

The command-line options that you specify alter the behavior of View Client.

By default, the path to the `vdmadmin` command executable file is `C:\Program Files\VMware\VMware View\Client\bin\wswc.exe`. For your convenience, add this path to your *PATH* environment variable.

Table 19-1 shows the command-line options that you can use with the `wswc` command.

Table 19-1. View Client Command-Line Options

Option	Description
`/?`	Displays the list of command options.
`–checkin`	(Local Desktop only) Checks in the specified desktop and unlocks the online equivalent. This option requires that you also specify the `–desktopName` option.
`–checkout`	(Local Desktop only) Checks out the specified desktop, and locks the online equivalent.
`–confirmRollback`	(Local Desktop only) Suppresses the confirmation dialog box that appears when you use the `–rollback` option. To perform rollback in non-interactive mode, also specify the `–nonInteractive` option.
`–connectUSBOnStartup`	Redirects all USB devices to the desktop that are currently connected to the host. This option is implicitly set if you specify the `–unattended` option.

Table 19-1. View Client Command-Line Options (Continued)

Option	Description
`–connectUSBOnInsert`	Connects a USB device to the foreground desktop when you plug in the device. This option is implicitly set if you specify the `–unattended` option.
`–desktopLayout` *window_size*	Specifies how to display the window for the desktop: **`fullscreen`** Full screen display **`multimonitor`** Multiple-monitor display **`windowLarge`** Large window **`windowSmall`** Small window
`–desktopName` *desktop_name*	Specifies the name of the desktop as it would appear in the Select Desktop dialog box. This is the name as you see it in the select desktop dialog.
`–desktopProtocol` *protocol*	Specifies the desktop protocol to use as it would appear in the Select Desktop dialog box. The protocol can be PCOIP or RDP.
`–domainName` *domain_name*	Specifies the domain that the end user uses to log in to View Client.
`–file` *file_path*	Specifies the path of a configuration file that contains additional command options and arguments. See "View Client Configuration File," on page 361.
`–languageId` *Locale_ID*	Provides localization support for different languages in View Client. If a resource library is available, specify the Locale ID (LCID) to use. For US English, enter the value 0x409.
`–localDirectory` *directory_path*	(Local Desktop only) Specifies which directory on the local system to use for downloading the local desktop. This option requires that you also specify the `–desktopName` option.
`–logInAsCurrentUser`	Uses the credential information that the end user provides when logging in to the client system to log in to the View Connection Server instance and ultimately to the View desktop.
`–nonInteractive`	Suppresses error message boxes when starting View Client from a script. This option is implicitly set if you specify the `–unattended` option.
`–password` *password*	Specifies the password that the end user uses to log in to View Client. You do not need to specify this option for clients in kiosk mode if you generate the password automatically.
`–printEnvironmentInfo`	Displays the IP address, MAC address, and machine name of the client device.
`–rollback`	(Local Desktop only) Unlocks the online version of a checked out desktop and discards the local session. This option requires that you also specify the `–desktopName` option. To perform rollback in non-interactive mode, also specify the `–nonInteractive` option and the `–confirmRollback` option.
`–serverURL` *connection_server*	Specifies the URL, IP address, or FQDN of the View Connection Server instance.
`–smartCardPIN` *PIN*	Specifies the PIN when an end user inserts a smart card to login.

Table 19-1. View Client Command-Line Options (Continued)

Option	Description
`–unattended`	Runs View Client in a noninteractive mode that is suitable for clients in kiosk mode. You must also specify: ■ The account name of the client, if you did not generate the account name from the MAC address of the client device. The name must begin with the string "custom-" or an alternate prefix that you have configured in ADAM. ■ The password of the client, if you did not generate a password automatically when you set up the account for the client. The `–unattended` option implicitly sets the `–nonInteractive`, `–connectUSBOnStartup`, and `–connectUSBOnInsert` options.
`–userName` *user_name*	Specifies the account name that the end user uses to log in to View Client. You do not need to specify this option for clients in kiosk mode if you generate the account name from the MAC address of the client device.

Options that you specify on the command line or in the configuration file take precedence over any global system policies that you have defined, which in turn override user policies.

You can specify all options by Active Directory group policies except for `–checkin`, `–checkout`, `–file`, `–languageId`, `–localDirectory`, `–printEnvironmentInfo`, `–rollback`, `–smartCardPIN`, and `–unattended`.

View Client Configuration File

You can read command-line options for View Client from a configuration file.

You can specify the path of the configuration file as an argument to the `–f` option of the `wswc` command. The file must be a Unicode (UTF-16) or ASCII text file.

Example: Example of a Configuration File for a Noninteractive Application

The following example shows the contents of a configuration file for a noninteractive application.

```
–serverURL https://view.yourcompany.com
–userName autouser
–password auto123
–domainName companydomain
–desktopName autodesktop
–nonInteractive
```

Example: Example of a Configuration File for a Client in Kiosk Mode

The following example shows a client in kiosk mode whose account name is based on its MAC address. The client has an automatically generated password.

```
–serverURL 145.124.24.100
–unattended
```

View Client Registry Settings

You can define default settings for the View Client in the Windows registry instead of specifying these settings on the command line.

Table 19-2 shows the registry settings for View Client. All the settings are located under `HKLM\Software\VMware, Inc.\VMware VDM\Client\` in the registry.

Policy entries take precedence over registry settings, and command-line settings take precedence over policy entries.

Table 19-2. View Client Registry Settings

Registry Setting	Description
DomainName	Specifies the default domain name.
EnableShade	Specifies whether the menu bar (shade) at the top of the View Client window is enabled. The menu bar is enabled by default except for clients in kiosk mode. A value of false disables the menu bar.
Password	Specifies the default password.
ServerURL	Specifies the default View Connection Server instance by its URL, IP address, or FQDN.
UserName	Specifies the default user name.

View Client Exit Codes

The wswc command can return exit codes to indicate the nature of any error that View Client encounters.

Table 19-3 shows the exit codes that the wswc command can return.

Table 19-3. View Client Exit Codes

Exit Code	Description
-1	Fatal error in kiosk mode.
0	Success.
1	Connection failed.
2	Login failed.
3	Desktop failed to start.
4	RDP failed to start.
5	RDP operation failed.
6	Tunnel connection lost.
7	Local desktop transfer failure.
8	Local desktop check-in failure.
9	Local desktop check-out failure.
10	Local desktop rollback failure.
11	Unknown result received during authentication.
12	Authentication error.
13	Received request to use an unknown authentication method.
14	Invalid server response.
15	Desktop was disconnected.
16	Tunnel was disconnected.
17	Reserved for future development.
18	Reserved for future development.
19	Unsupported kiosk operation.
20	Remote mouse, keyboard, or screen (RMKS) connection error.
21	PIN error.
22	PIN mismatch.
23	Password mismatch.

Table 19-3. View Client Exit Codes (Continued)

Exit Code	Description
24	View Connection Server error.
25	Desktop was not available.

Index

D

E

F

G

M

Q

R

S

T

U

V

W

X