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.
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
Contents

VMware Horizon View Administration 9

1 Configuring View Connection Server 11
   Using View Administrator 11
   Configuring vCenter Server and View Composer 14
   Backing Up View Connection Server 26
   Configuring Settings for Client Sessions 26
   Disable or Enable View Connection Server 35
   Edit the External URLs 35
   Join or Withdraw from the Customer Experience Program 36
   View LDAP Directory 36

2 Configuring Role-Based Delegated Administration 39
   Understanding Roles and Privileges 39
   Using Folders to Delegate Administration 40
   Understanding Permissions 41
   Manage Administrators 42
   Manage and Review Permissions 43
   Manage and Review Folders 45
   Manage Custom Roles 47
   Predefined Roles and Privileges 48
   Required Privileges for Common Tasks 51
   Best Practices for Administrator Users and Groups 53

3 Preparing Unmanaged Desktop Sources 55
   Prepare an Unmanaged Desktop Source for View Desktop Deployment 55
   Install View Agent on an Unmanaged Desktop Source 55

4 Creating and Preparing Virtual Machines 59
   Creating Virtual Machines for View Desktop Deployment 59
   Install View Agent on a Virtual Machine 64
   Install View Agent Silently 66
   Configure a Virtual Machine with Multiple NICs for View Agent 70
   Optimize Windows Guest Operating System Performance 70
   Optimize Windows 7 and Windows 8 Guest Operating System Performance 71
   Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops 73
   Preparing Virtual Machines for View Composer 79
   Creating Virtual Machine Templates 85
   Creating Customization Specifications 86
Managing Desktops and Desktop Pools 265
Managing Desktop Pools 265
Reducing Adobe Flash Bandwidth 271
Managing Virtual-Machine Desktops 272
Export View Information to External Files 278

Managing Physical Computers and Terminal Servers 281
Add an Unmanaged Desktop Source to a Pool 281
Remove an Unmanaged Desktop Source from a Pool 282
Delete a Pool That Contains Unmanaged Desktops 282
Unregister an Unmanaged Desktop Source 283
Desktop Status of Physical Computers and Terminal Servers 283

Managing ThinApp Applications in View Administrator 285
View Requirements for ThinApp Applications 285
Capturing and Storing Application Packages 286
Assigning ThinApp Applications to Desktops and Pools 289
Maintaining ThinApp Applications in View Administrator 296
Monitoring and Troubleshooting ThinApp Applications in View Administrator 299
ThinApp Configuration Example 302

Managing Local Desktops 303
Benefits of Using View Desktops in Local Mode 303
Managing View Transfer Server 309
Managing the Transfer Server Repository 313
Managing Data Transfers 319
Configure Security and Optimization for Local Desktop Operations 323
Configuring Endpoint Resource Usage 328
Configuring an HTTP Cache to Provision Local Desktops Over a WAN 332
Configuring the Heartbeat Interval for Local Desktop Client Computers 336
Manually Downloading a Local Desktop to a Location with Poor Network Connections 337
Troubleshooting View Transfer Server and Local Desktop Operations 340

Maintaining View Components 351
Backing Up and Restoring View Configuration Data 351
Monitor View Components 358
Monitor Desktop Status 358
Understanding View Manager Services 359
Add Licenses to VMware Horizon View 361
Update General User Information from Active Directory 361
Migrate View Composer to Another Computer 362
Update the Certificates on a View Connection Server Instance, Security Server, or View Composer 367
Information Collected by the Customer Experience Improvement Program 368

Troubleshooting View Components 379
Monitoring System Health 380
Monitor Events in View Manager 380
Send Messages to Desktop Users 381
17 Using the vdmadmin Command 407
   vdmadmin Command Usage 409
   Configuring Logging in View Agent Using the -A Option 411
   Overriding IP Addresses Using the -A Option 413
   Setting the Name of a View Connection Server Group Using the -C Option 414
   Updating Foreign Security Principals Using the -F Option 414
   Listing and Displaying Health Monitors Using the -H Option 415
   Listing and Displaying Reports of View Manager Operation Using the -I Option 416
   Generating View Event Log Messages in Syslog Format Using the -I Option 417
   Assigning Dedicated Desktops Using the -L Option 418
   Displaying Information About Machines Using the -M Option 419
   Reclaiming Disk Space on Virtual Machines Using the -M Option 420
   Configuring Domain Filters Using the -N Option 421
   Configuring Domain Filters 423
   Displaying the Desktops and Policies of Unentitled Users Using the -O and -P Options 427
   Configuring Clients in Kiosk Mode Using the -Q Option 428
   Displaying the First User of a Desktop Using the -R Option 432
   Removing the Entry for a View Connection Server Instance or Security Server Using the -S Option 432
   Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option 433
   Decrypting the Virtual Machine of a Local Desktop Using the -V Option 434
   Recovering a Local Desktop by Using the -V Option When the Desktop Was Modified in the Datacenter 435
   Unlocking or Locking Virtual Machines Using the -V Option 437
   Detecting and Resolving LDAP Entry Collisions Using the -X Option 438

18 Setting Up Clients in Kiosk Mode 439
   Configure Clients in Kiosk Mode 439
Index  449
VMware Horizon View Administration

VMware Horizon View Administration describes how to configure and administer VMware Horizon 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 Horizon View components.

Intended Audience

This information is intended for anyone who wants to configure and administer VMware Horizon View. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.
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,” on page 11
- “Configuring vCenter Server and View Composer,” on page 14
- “Backing Up View Connection Server,” on page 26
- “Configuring Settings for Client Sessions,” on page 26
- “Disable or Enable View Connection Server,” on page 35
- “Edit the External URLs,” on page 35
- “Join or Withdraw from the Customer Experience Program,” on page 36
- “View LDAP Directory,” on page 36

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 Horizon 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. You access View Administrator by using a secure (SSL) connection.

**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 Horizon View Installation* document.

**Procedure**

1. Open your Web browser and enter the following URL, where `server` is the host name of the View Connection Server instance.
   
   ```
   https://server/admin
   ```

   **NOTE** You can use the IP address if you have to access a View Connection Server instance when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance, resulting in blocked access or access with reduced security.

   Your access to View Administrator depends on the type of certificate that is configured on the View Connection Server computer.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>You configured a certificate signed by a CA for View Connection Server.</td>
<td>When you first connect, your Web browser displays View Administrator.</td>
</tr>
<tr>
<td>The default, self-signed certificate supplied with View Connection Server is configured.</td>
<td>When you first connect, your Web browser might display a page warning that the security certificate associated with the address is not issued by a trusted certificate authority. Click Ignore to continue using the current SSL certificate.</td>
</tr>
</tbody>
</table>

2. Log in as a user with credentials to access the View Administrators account.

   You specify the View Administrators account when you install a standalone View Connection Server instance or the first View Connection Server instance in a replicated group. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

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

<table>
<thead>
<tr>
<th>View Administrator Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigating backward and forward in View Administrator pages</td>
<td>Click your browser’s Back button to go to the previously displayed View Administrator page. Click the Forward button to return to the current page. If you click the browser’s Back button while you are using a View Administrator wizard or dialog box, you return to the main View Administrator page. The information you entered in the wizard or dialog is lost. In View versions that preceded the View 5.1 release, you could not use your browser’s Back and Forward buttons to navigate within View Administrator. Separate Back and Forward buttons in the View Administrator window were provided for navigation. These buttons are removed in the View 5.1 release.</td>
</tr>
<tr>
<td>Bookmarking View Administrator pages</td>
<td>You can bookmark View Administrator pages in your browser.</td>
</tr>
<tr>
<td>Multicolumn sorting</td>
<td>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 &gt; 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 &gt; Pools, double-click the pool ID, click the Inventory tab, click the Datastore heading, and Ctrl+click the Status heading.</td>
</tr>
</tbody>
</table>
| Customizing table columns                                      | You can customize the display of View Administrator table columns by hiding selected columns and locking the first column. This feature lets you control the display of large tables such as Inventory > Desktops that contain many columns. Right-click any column header to display a context menu that lets you take the following actions: 
  - Hide the selected column. 
  - Customize columns. A dialog displays all columns in the table. You can select the columns to display or hide. 
  - Lock the first column. This option forces the left-hand column to remain displayed as you scroll horizontally across a table with many columns. For example, on the Inventory > Desktops page, the desktop ID remains displayed as you scroll horizontally to see other desktop characteristics. Your customized settings persist while you remain on the current View Administrator page. The settings do not persist if you navigate to another page. |
### 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.

You can also configure storage settings for View. You can allow ESXi hosts to reclaim disk space on linked-clone virtual machines. To allow ESXi hosts to cache virtual machine data, you must enable View Storage Accelerator for vCenter Server.
Create a User Account for View Composer

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

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

**Procedure**

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

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

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

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

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

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

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

**What to do next**

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

Add vCenter Server Instances to View Manager

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

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

View Manager connects to the vCenter Server instance using a secure channel (SSL).
Prerequisites

- Install the View Connection Server product license key.

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

  For details about configuring a vCenter Server user for View Manager, see the *VMware Horizon View Installation* document.

- Verify that an SSL server certificate is installed on the vCenter Server host. In a production environment, install a valid SSL certificate that is signed by a trusted Certificate Authority (CA).

  In a testing environment, you can use the default certificate that is installed with vCenter Server, but you must accept the certificate thumbprint when you add vCenter Server to View.

- Verify that all View Connection Server instances in the replicated group trust the root CA certificate for the server certificate that is installed on the vCenter Server host. Check if the root CA certificate is in the *Trusted Root Certification Authorities > Certificates* folder in the Windows local computer certificate stores on the View Connection Server hosts. If it is not, import the root CA certificate into the Windows local computer certificate stores.

  See “Import a Root Certificate and Intermediate Certificates into a Windows Certificate Store” in the *VMware Horizon View Installation* document.

- Verify that the vCenter Server instance contains ESXi hosts. If no hosts are configured in the vCenter Server instance, you cannot add the instance to View.

- Familiarize yourself with the settings that determine the maximum operations limits for vCenter Server and View Composer. See “Concurrent Operations Limits for vCenter Server and View Composer,” on page 21 and “Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms,” on page 22.

Procedure

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

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

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

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

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

4. Type the name of the vCenter Server user.

   For example: `domain\user` or `user@domain.com`

5. Type the vCenter Server user password.

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

7. Type the TCP port number.

   The default port is 443.

8. Under Advanced Settings, set the concurrent operations limits for vCenter Server and View Composer operations.
9 Click Next to display the View Composer Settings page.

What to do next

Configure View Composer settings.

- If the vCenter Server instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Settings page.

- If the vCenter Server instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See “Accept the Thumbprint of a Default SSL Certificate,” on page 23.

If View Manager uses multiple vCenter Server instances, repeat this procedure to add the other vCenter Server instances.

Configure View Composer Settings

To use View Composer, you must configure settings that allow View Manager to connect to the View Composer service. View Composer can be installed on its own separate host or on the same host as vCenter Server.

There must be a one-to-one mapping between each View Composer service and vCenter Server instance. A View Composer service can operate with only one vCenter Server instance. A vCenter Server instance can be associated with only one View Composer service.

After the initial View deployment, you can migrate the View Composer service to a new host to support a growing or changing View deployment. You can edit the initial View Composer settings in View Administrator, but you must perform additional steps to ensure that the migration succeeds. See “Migrate View Composer to Another Computer,” on page 362.

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 15.

- Verify that you configured View Manager to connect to vCenter Server. To do so, you must complete the vCenter Server Information page in the Add vCenter Server wizard. See “Add vCenter Server Instances to View Manager,” on page 15.

- Verify that this View Composer service is not already configured to connect to a different vCenter Server instance.

Procedure

1 In View Administrator, complete the vCenter Server Information page in the Add vCenter Server wizard.
   a Click View Configuration > Servers.
   b In the vCenter Servers tab, click Add and provide the vCenter Server settings.

2 On the View Composer Settings page, if you are not using View Composer, select Do not use View Composer.

   If you select Do not use View Composer, the other View Composer settings become inactive. When you click Next, the Add vCenter Server wizard displays the Storage Settings page. The View Composer Domains page is not displayed.
3 If you are using View Composer, select the location of the View Composer host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| View Composer is installed on the same host as vCenter Server. | a Select View Composer co-installed with the vCenter Server.  
b Make sure that the port number is the same as the port that you specified when you installed the View Composer service on vCenter Server. The default port number is 18443. |
| View Composer is installed on its own separate host. | a Select Standalone View Composer Server.  
b In the View Composer server address text box, type the fully qualified domain name (FQDN) of the View Composer host.  
c Type the name of the View Composer user.  
For example: domain.com\user or user@domain.com  
d Type the password of the View Composer user.  
e Make sure that the port number is the same as the port that you specified when you installed the View Composer service. The default port number is 18443. |

4 Click Next to display the View Composer Domains page.

**What to do next**

Configure View Composer domains.

- If the View Composer instance is configured with a signed SSL certificate, and View Connection Server trusts the root certificate, the Add vCenter Server wizard displays the View Composer Domains page.
- If the View Composer instance is configured with a default certificate, you must first determine whether to accept the thumbprint of the existing certificate. See “Accept the Thumbprint of a Default SSL Certificate,” on page 23.

**Configure View Composer Domains**

You must configure an Active Directory domain in which View Composer deploys linked-clone desktops. You can configure multiple domains for View Composer. After you first add vCenter Server and View Composer settings to View, you can add more View Composer domains by editing the vCenter Server instance in View Administrator.

**Prerequisites**

In View Administrator, verify that you completed the vCenter Server Information and View Composer Settings pages in the Add vCenter Server wizard.

**Procedure**

1 On the View Composer Domains page, click Add to add the domain user for View Composer account information.
2 Type the domain name of the Active Directory domain.  
For example: domain.com
3 Type the domain user name, including the domain name.  
For example: domain.com\admin
4 Type the account password.
5 Click OK.
6 To add domain user accounts with privileges in other Active Directory domains in which you deploy linked-clone pools, repeat the preceding steps.
7 Click Next to display the Storage Settings page.

**What to do next**

Enable virtual machine disk space reclamation and configure View Storage Accelerator for View.

**Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines**

In vSphere 5.1 and later, you can enable the disk space reclamation feature for View. Starting in vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space in the linked clones, reducing the total storage space required for linked clones.

As users interact with linked-clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with their desktops.

Disk space reclamation is especially useful for deployments that cannot take advantage of storage-saving strategies such as refresh on logoff. For example, knowledge workers who install user applications on dedicated desktops might lose their personal applications if the desktops were refreshed or recomposed. With disk space reclamation, View can maintain linked clones at close to the reduced size they start out with when they are first provisioned.

This feature has two components: space-efficient disk format and space reclamation operations.

In a vSphere 5.1 or later environment, when a parent virtual machine is virtual hardware version 9 or later, View creates linked clones with space-efficient OS disks, whether or not space reclamation operations are enabled.

To enable space reclamation operations, you must use View Administrator to enable space reclamation for vCenter Server and reclaim VM disk space for individual desktop pools. The space reclamation setting for vCenter Server gives you the option to disable this feature on all desktop pools that are managed by the vCenter Server instance. Disabling the feature for vCenter Server overrides the setting at the desktop pool level.

The following guidelines apply to the space reclamation feature:

- It operates only on space-efficient OS disks in linked clones.
- It does not affect View Composer persistent disks.
- It works only with vSphere 5.1 or later and only on desktops that are virtual hardware version 9 or later.
- It does not operate on full-clone desktops.
- It operates on virtual machines with SCSI controllers. IDE controllers are not supported.
- It operates on Windows XP and Windows 7 desktops only. It does not operate on Windows 8 desktops.

Native NFS snapshot technology (VAAI) is not supported in pools that contain virtual machines with space-efficient disks.

**Prerequisites**

- Verify that your vCenter Server and ESXi hosts are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.
  - In an ESXi cluster, verify that all the hosts are version 5.1 with download patch ESXi510-201212001 or later.
Procedure

1. In View Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
   a. Select View Configuration > Servers.
   b. In the vCenter Servers tab, click Add.
   c. Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.

2. On the Storage Settings page, make sure that Enable space reclamation is selected.
   
   Space reclamation is selected by default if you are performing a fresh installation of View 5.2 or later. You must select Enable space reclamation if you are upgrading to View 5.2 or later from View 5.1 or an earlier release.

What to do next

On the Storage Settings page, configure View Storage Accelerator.

Configure View Storage Accelerator for vCenter Server

In vSphere 5.0 and later, you can configure ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator improves View performance during I/O storms, which can take place when many desktops start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. Instead of reading the entire OS or application from the storage system over and over, a host can read common data blocks from cache.

By reducing the number of IOPS during boot storms, View Storage Accelerator lowers the demand on the storage array, which lets you use less storage I/O bandwidth to support your View deployment.

You enable caching on your ESXi hosts by selecting the View Storage Accelerator setting in the vCenter Server wizard in View Administrator, as described in this procedure.

Make sure that View Storage Accelerator is also configured for individual desktop pools. View Storage Accelerator is enabled for pools by default, but this feature can be disabled or enabled when you create or edit a pool. To operate on a pool, View Storage Accelerator must be enabled for vCenter Server and for the individual pool.

You can enable View Storage Accelerator on pools that contain linked clones and pools that contain full virtual machines.

View Storage Accelerator is also supported with local mode. Users can check out desktops in pools that are enabled for View Storage Accelerator. View Storage Accelerator is disabled while a desktop is checked out and reenabled after the desktop is checked in.

Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator.

View Storage Accelerator is now qualified to work in configurations that use View replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using View Storage Accelerator with View replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. Hence, this combination is tested and supported.
Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.
  - In an ESXi cluster, verify that all the hosts are version 5.0 or later.
- Verify that the vCenter Server user was assigned the Global > Act as vCenter Server privilege in vCenter Server. See the topics in the VMware Horizon View Installation documentation that describe View Manager and View Composer privileges required for the vCenter Server user.

Procedure

1. In View Administrator, complete the Add vCenter Server wizard pages that precede the Storage Settings page.
   a. Select View Configuration > Servers.
   b. In the vCenter Servers tab, click Add.
   c. Complete the vCenter Server Information, View Composer Settings, and View Composer Domains pages.
2. On the Storage Settings page, make sure that the Enable View Storage Accelerator check box is selected. This check box is selected by default.
3. Specify a default host cache size.
   - The default cache size applies to all ESXi hosts that are managed by this vCenter Server instance.
   - The default value is 1,024MB. The cache size must be between 100MB and 2,048MB.
4. To specify a different cache size for an individual ESXi host, select an ESXi host and click Edit cache size.
   a. In the Host cache dialog box, check Override default host cache size.
   b. Type a Host cache size value between 100MB and 2,048MB and click OK.
5. On the Storage Settings page, click Next.
6. Click Finish to add vCenter Server, View Composer, and Storage Settings to View.

What to do next


To complete View Storage Accelerator settings in View, configure View Storage Accelerator for desktop pools. See “Configure View Storage Accelerator for Desktop Pools,” on page 145.

Concurrent Operations Limits for vCenter Server and View Composer

When you add vCenter Server to View or edit the vCenter Server settings, you can configure several options that set the maximum number of concurrent operations that are performed by vCenter Server and View Composer.

You configure these options in the Advanced Settings panel on the vCenter Server Information page.
### Table 1-2. Concurrent Operations Limits for vCenter Server and View Composer

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max concurrent vCenter provisioning operations</td>
<td>Determines the maximum number of concurrent requests that View Manager can make to provision and delete full virtual machines in this vCenter Server instance. The default value is 20. This setting applies to full virtual machines only.</td>
</tr>
<tr>
<td>Max concurrent power operations</td>
<td>Determines the maximum number of concurrent power operations (startup, shutdown, suspend, and so on) that can take place on virtual machines managed by View Manager in this vCenter Server instance. The default value is 50. For guidelines for calculating a value for this setting, see “Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms,” on page 22. This setting applies to full virtual machines and linked clones.</td>
</tr>
<tr>
<td>Max concurrent View Composer maintenance operations</td>
<td>Determines the maximum number of concurrent View Composer refresh, recompose, and rebalance operations that can take place on linked clones managed by this View Composer instance. The default value is 12. Desktops that have active sessions must be logged off before a maintenance operation can begin. If you force users to log off as soon as a maintenance operation begins, the maximum number of concurrent operations on desktops that require logoffs is half the configured value. For example, if you configure this setting as 24 and force users to log off, the maximum number of concurrent operations on desktops that require logoffs is 12. This setting applies to linked clones only.</td>
</tr>
<tr>
<td>Max concurrent View Composer provisioning operations</td>
<td>Determines the maximum number of concurrent creation and deletion operations that can take place on linked clones managed by this View Composer instance. The default value is 8. This setting applies to linked clones only.</td>
</tr>
</tbody>
</table>

### Setting a Concurrent Power Operations Rate to Support View Desktop Logon Storms

The **Max concurrent power operations** setting governs the maximum number of concurrent power operations that can occur on View desktop virtual machines in a vCenter Server instance. Starting in View 5.0, this limit is set to 50 by default. You can change this value to support peak power-on rates when many users log on to their desktops at the same time.

As a best practice, you can conduct a pilot phase to determine the correct value for this setting. For planning guidelines, see "Architecture Design Elements and Planning Guidelines" in the *VMware Horizon View Architecture Planning* document.

The required number of concurrent power operations is based on the peak rate at which desktops are powered on and the amount of time it takes for the desktop to power on, boot, and become available for connection. In general, the recommended power operations limit is the total time it takes for the desktop to start multiplied by the peak power-on rate.

For example, the average desktop takes two to three minutes to start. Therefore, the concurrent power operations limit should be 3 times the peak power-on rate. The default setting of 50 is expected to support a peak power-on rate of 16 desktops per minute.
View waits a maximum of five minutes for a desktop to start. If the start time takes longer, other errors are likely to occur. To be conservative, you can set a concurrent power operations limit of 5 times the peak power-on rate. With a conservative approach, the default setting of 50 supports a peak power-on rate of 10 desktops per minute.

Logons, and therefore desktop power on operations, typically occur in a normally distributed manner over a certain time window. You can approximate the peak power-on rate by assuming that it occurs in the middle of the time window, during which about 40% of the power-on operations occur in 1/6th of the time window. For example, if users log on between 8:00 AM and 9:00 AM, the time window is one hour, and 40% of the logons occur in the 10 minutes between 8:25 AM and 8:35 AM. If there are 2,000 users, 20% of whom have their desktops powered off, then 40% of the 400 desktop power-on operations occur in those 10 minutes. The peak power-on rate is 16 desktops per minute.

Accept the Thumbprint of a Default SSL Certificate

When you add vCenter Server and View Composer instances to Horizon View, you must ensure that the SSL certificates that are used for the vCenter Server and View Composer instances are valid and trusted by View Connection Server. If the default certificates that are installed with vCenter Server and View Composer are still in place, you must determine whether to accept these certificates' thumbprints.

If a vCenter Server or View Composer instance is configured with a certificate that is signed by a CA, and the root certificate is trusted by View Connection Server, you do not have to accept the certificate thumbprint. No action is required.

If you replace a default certificate with a certificate that is signed by a CA, but View Connection Server does not trust the root certificate, you must determine whether to accept the certificate thumbprint. A thumbprint is a cryptographic hash of a certificate. The thumbprint is used to quickly determine if a presented certificate is the same as another certificate, such as the certificate that was accepted previously.

**NOTE** If you install vCenter Server and View Composer on the same Windows Server host, they can use the same SSL certificate, but you must configure the certificate separately for each component.

For details about configuring SSL certificates, see “Configuring SSL Certificates for View Servers” in the VMware Horizon View Installation document.

You first add vCenter Server and View Composer in View Administrator by using the Add vCenter Server wizard. If a certificate is untrusted and you do not accept the thumbprint, you cannot add vCenter Server and View Composer.

After these servers are added, you can reconfigure them in the Edit vCenter Server dialog box.

**NOTE** You also must accept a certificate thumbprint when you upgrade from an earlier release to Horizon View 5.1 or later, and a vCenter Server or View Composer certificate is untrusted, or if you replace a trusted certificate with an untrusted certificate.

On the View Administrator dashboard, the vCenter Server or View Composer icon turns red and an Invalid Certificate Detected dialog box appears. You must click **Verify** and follow the procedure shown here.

Similarly, in View Administrator you can configure a SAML 2.0 authenticator for use by a View Connection Server instance. If the SAML 2.0 server certificate is not trusted by View Connection Server, you must determine whether to accept the certificate thumbprint. If you do not accept the thumbprint, you cannot configure the SAML 2.0 authenticator in Horizon View. After a SAML 2.0 authenticator is configured, you can reconfigure it in the Edit View Connection Server dialog box.

**Procedure**

1. When View Administrator displays an Invalid Certificate Detected dialog box, click **View Certificate**.
2. Examine the certificate thumbprint in the Certificate Information window.
Examine the certificate thumbprint that was configured for the vCenter Server or View Composer instance.

a. On the vCenter Server or View Composer host, start the MMC snap-in and open the Windows Certificate Store.

b. Navigate to the vCenter Server or View Composer certificate.

c. Click the Certificate Details tab to display the certificate thumbprint.

Similarly, examine the certificate thumbprint for a SAML 2.0 authenticator. If appropriate, take the preceding steps on the SAML 2.0 authenticator host.

Verify that the thumbprint in the Certificate Information window matches the thumbprint for the vCenter Server or View Composer instance.

Similarly, verify that the thumbprints match for a SAML 2.0 authenticator.

Determine whether to accept the certificate thumbprint.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The thumbprints match.</td>
<td>Click Accept to use the default certificate.</td>
</tr>
<tr>
<td>The thumbprints do not match.</td>
<td>Click Reject. Troubleshoot the mismatched certificates. For example, you might have provided an incorrect IP address for vCenter Server or View Composer.</td>
</tr>
</tbody>
</table>

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 269.

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.

Remove View Composer from View Manager

You can remove the connection between View Manager and the View Composer service that is associated with a 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. View Manager prevents you from removing View Composer if any associated linked clones still exist. After the connection to View Composer is disabled, View Manager cannot provision or manage new linked clones.
**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. If the linked-clone desktops are configured with persistent disks, you can detach or delete the persistent disks.
   c. Click **OK**.
      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.
   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 tab, select the vCenter Server instance with which View Composer is associated.

4. Click **Edit**.

5. Under View Composer Server Settings, click **Edit**, select **Do not use 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.

**What to do next**

If you intend to install View Composer on another host and reconfigure View Manager to connect to the new View Composer service, you must perform certain additional steps. See “Migrate View Composer Without Linked-Clone Desktops,” on page 365.

**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 351.

Configuring Settings for Client Sessions

You can configure global settings that affect the client sessions and connections that are managed by a View Connection Server instance or replicated group. You can set the session timeout length, display prelogin and warning messages, and set security-related 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 and PCoIP Secure Gateway,” on page 31 for information about configuring direct connections.

Prerequisites

Familiarize yourself with the global settings. See “Global Settings for Client Sessions,” on page 28 and “Global Security Settings for Client Sessions and Connections,” on page 29.

Procedure

1. In View Administrator, click View Configuration > Global Settings.
2. Choose whether to configure general settings or security settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General global settings</td>
<td>In the General pane, click Edit.</td>
</tr>
<tr>
<td>Global security settings</td>
<td>In the Security pane, click Edit.</td>
</tr>
</tbody>
</table>

3. Configure the global settings.
4. Click OK.

What to do next

You can change the data recovery password that was provided during installation. See “Change the Data Recovery Password,” on page 26.

Change the Data Recovery Password

You provide a data recovery password when you install View Connection Server version 5.1 or later. After installation, you can change this password in View Administrator. The password is required when you restore the View LDAP configuration from a backup.

When you back up View Connection Server, the View LDAP configuration is exported as encrypted LDIF data. To restore the encrypted backup View configuration, you must provide the data recovery password.

The password must contain between 1 and 128 characters. Follow your organization’s best practices for generating secure passwords.
Procedure

1. In View Administrator, click **View Configuration > Global Settings**.
2. In the Security pane, click **Change data recovery password**.
3. Type and retype the new password.
4. (Optional) Type a password reminder.

**NOTE** You can also change the data recovery password when you schedule your View configuration data to be backed up. See “Schedule View Manager Configuration Backups,” on page 352.

**What to do next**

When you use the `vdmimport` utility to restore a backup View configuration, provide the new password.
Global Settings for Client Sessions

General global settings determine session timeout lengths, SSO enablement and timeout limits, status updates in View Administrator, and whether prelogin and warning messages are displayed.

Table 1-3. General Global Settings for Client Sessions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Session timeout</strong></td>
<td>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. This value determines the amount of time that a single View Client session can stay connected to a desktop. It does not affect the amount of time that a Windows session remains running on a desktop virtual machine.</td>
</tr>
</tbody>
</table>
| **SSO**                        | Determines whether to enable or disable Single Sign-on (SSO) for View users and sets the SSO timeout limit. When SSO is in effect, when a user logs in to View Connection Server from View Client, 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. This setting has the following options:  
  - **Disable after**. Enables SSO until the specified timeout limit is reached. This is the default option. By default, the user’s SSO credentials are no longer valid after 15 minutes. This SSO timeout limit reduces the chance that someone else could start using the desktop session. You can change the SSO timeout limit by typing another value in the **Disable after** text box. 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.  
  - **Always enabled**. Enables SSO with no timeout limit.  
  - **Disabled**. Disables SSO altogether. On remote desktops, a new SSO timeout limit takes effect immediately. You do not need to restart the View Connection Server service or the client computer. For desktops that run in local mode, see “SSO Timeout Limits and Local Mode Desktops,” on page 29. |
| **View Administrator session timeout** | Determines how long an idle View Administrator session continues before the session times out. **Important**: Setting the View Administrator session timeout to a high number of minutes increases the risk of unauthorized use of View Administrator. Use caution when you allow an idle session to persist a long time. By default, the View Administrator session timeout is 30 minutes. You can set a session timeout from 1 to 4320 minutes (72 hours). |
| **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. By default, this setting is not enabled. |
Table 1-3. General Global Settings for Client Sessions (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a pre-login message</td>
<td>Displays a disclaimer or another message to View Client users when they log in.</td>
</tr>
<tr>
<td></td>
<td>Type your information or instructions in the text box in the Global Settings dialog window.</td>
</tr>
<tr>
<td></td>
<td>To display no message, leave the check box unselected.</td>
</tr>
<tr>
<td>Display warning before forced logoff</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Check the box to display a warning message.</td>
</tr>
<tr>
<td></td>
<td>Type the number of minutes to wait after the warning is displayed and before logging off the user. The default is five minutes.</td>
</tr>
<tr>
<td></td>
<td>Type your warning message. You can use the default message:</td>
</tr>
<tr>
<td></td>
<td>Your desktop is scheduled for an important update and will be shut down in 5 minutes. Please save any unsaved work now.</td>
</tr>
</tbody>
</table>

SSO Timeout Limits and Local Mode Desktops

On desktops that run in local mode, a 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.

On View desktops that are used in local mode, a checkout operation might take longer than the SSO timeout limit. In this case, the user's SSO credentials expire before the checkout is completed.

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 and the user then launches the desktop, the user still needs to log in to the desktop manually, even though the user has not yet spent any time in a desktop session. SSO succeeds after the user closes View Client and reconnects to View Connection Server.

A first-time checkout in a low-bandwidth environment might take longer than 15 minutes, the default timeout limit. A user's SSO credentials might expire during the first checkout if the default SSO timeout limit is in effect.

Global Security Settings for Client Sessions and Connections

Global security settings determine whether clients are reauthenticated after interruptions, message security mode is enabled, IPSec is used for security server connections, and SSO is used for local desktop operations.

SSL is required for all View Client connections and View Administrator connections to View. If your View deployment uses load balancers or other client-facing, intermediate servers, you can off-load SSL to them and then configure non-SSL connections on individual View Connection Server instances and security servers. See “Off-load SSL Connections to Intermediate Servers,” on page 33.
Table 1-4. Global Security Settings for Client Sessions and Connections

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate secure tunnel connections after network interruption</td>
<td>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. This setting offers increased security. For example, if a laptop is stolen and moved to a different network, the user cannot automatically gain access to the remote desktop because the network connection was temporarily interrupted. 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.</td>
</tr>
<tr>
<td>Message security mode</td>
<td>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 30. By default, message security mode is enabled.</td>
</tr>
<tr>
<td>Use IPSec for Security Server connections</td>
<td>Determines whether to use Internet Protocol Security (IPSec) for connections between security servers and View Connection Server instances. By default, secure connections (using IPSec) for security server connections is enabled.</td>
</tr>
<tr>
<td>Disable Single Sign-on for Local Mode operations</td>
<td>Determines if single sign-on is enabled when users log in to their local desktops. If you enable 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.</td>
</tr>
</tbody>
</table>

**NOTE** If you upgrade to View 5.1 or later from an earlier View release, the global setting Require SSL for client connections is displayed in View Administrator, but only if the setting was disabled in your View configuration before you upgraded. Because SSL is required for all View Client connections and View Administrator connections to View, this setting is not displayed in fresh installations of View 5.1 or later versions and is not displayed after an upgrade if the setting was already enabled in the previous View configuration.

After an upgrade, if you do not enable the Require SSL for client connections setting, HTTPS connections from View clients will fail, unless they connect to an intermediate device that is configured to make onward connections using HTTP. See “Off-load SSL Connections to Intermediate Servers,” on page 33.

**Message Security Mode for View Components**

You can set message security mode for View components. This setting determines how sender signatures in JMS messages are treated. By default, JMS messages are rejected if the signature is missing or invalid, or if a message was modified after it was signed.

If any component in your View environment predates View Manager 3.0, when message security was introduced, you can change the mode to log a warning if any of these conditions are found, or to not verify signatures at all. These options are not recommended and it is preferable to upgrade older components.

Some JMS messages are encrypted because they carry sensitive information such as user credentials. Consider using IPSec to encrypt all JMS messages between View Connection Server instances, and between View Connection Server instances and security servers.
Table 1-5 shows the options you can select to configure the message security mode. To set an option, select it from the Message security mode list in the Global Settings dialog window.

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

When you first install View on a system, the message security mode is set to Enabled. If you upgrade View, the message security mode remains unchanged from its existing setting.

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 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the secure tunnel</td>
<td>Select Use secure tunnel connection to desktop.</td>
</tr>
<tr>
<td>Disable the secure tunnel</td>
<td>Deselect Use secure tunnel connection to desktop.</td>
</tr>
</tbody>
</table>

The secure tunnel is enabled by default.

4. Configure use of the PCoIP Secure Gateway.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the PCoIP Secure Gateway</td>
<td>Select Use PCoIP Secure Gateway for PCoIP connections to desktop</td>
</tr>
<tr>
<td>Disable the PCoIP Secure Gateway</td>
<td>Deselect Use PCoIP Secure Gateway for PCoIP connections to desktop</td>
</tr>
</tbody>
</table>

The PCoIP Secure Gateway is disabled by default.

5. Click OK to save your changes.

Configure Secure HTML Access

In View Administrator, you can configure the use of the Blast Secure Gateway to provide secure HTML access to View desktops.

You can provide secure connections to external users who use HTML Access to connect to View desktops. The Blast Secure Gateway, enabled by default on View Connection Server and security server hosts, ensures that only authenticated users can communicate with View desktops. With HTML Access, View Client software does not have to be installed on the users’ endpoint devices.

When the Blast Secure Gateway is not enabled, client Web browsers use HTML Access to establish direct connections to View desktop virtual machines, bypassing the Blast Secure Gateway.

**IMPORTANT** A typical network configuration that provides secure connections for external users includes a security server. To enable or disable the Blast Secure Gateway on a security server, you must edit the View Connection Server instance that is paired with the security server. If external users connect directly to a View Connection Server host, you enable or disable the Blast Secure Gateway by editing that View Connection Server instance.

Prerequisites

- If users select View desktops by using the Horizon User Portal, verify that Horizon Workspace is installed and configured for use with View Connection Server and that View Connection Server is paired with a SAML 2.0 Authentication server.
- Verify that the secure tunnel is enabled. If the secure tunnel is disabled, the Blast Secure Gateway cannot be enabled.

Procedure

1. In View Administrator, select View Configuration > Servers.
2. In the View Connection Servers panel, select a View Connection Server instance and click Edit.
3 Configure use of the Blast Secure Gateway.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the Blast Secure Gateway</td>
<td>Select Use Blast Secure Gateway for HTML access to desktop</td>
</tr>
<tr>
<td>Disable the Blast Secure Gateway</td>
<td>Deselect Use Blast Secure Gateway for HTML access to desktop</td>
</tr>
</tbody>
</table>

The Blast Secure Gateway is enabled by default.

4 Click OK to save your changes.

**Open the Port Used by HTML Access on Security Servers**

When you install View Connection Server or security server, the View server installer creates the Windows Firewall rule for the port that is used by HTML Access for client connections, but the installer leaves the rule disabled until it is actually needed. When you later install HTML Access on a View Connection Server instance, the HTML Access installer automatically enables the rule to allow communication to that port. However, on security servers, you must manually enable the rule in the Windows Firewall to allow communication to the port.

By default, HTML Access uses TCP port 8443 for client connections to the Blast Secure Gateway.

**Procedure**

- To open the port used by HTML Access on a View Connection Server computer, install HTML Access on that computer.

  The HTML Access installer enables the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

- To open the port for HTML Access on a security server, manually enable the **VMware View Connection Server (Blast-In)** rule in the Windows Firewall.

**Off-load SSL Connections to Intermediate Servers**

View Clients must use HTTPS to connect to View Manager. If your View Clients connect to load balancers or other intermediate servers that pass on the connections to View Connection Server instances or security servers, you can off-load SSL to the intermediate servers.

**Import SSL Off-loading Servers’ Certificates to View Servers**

If you off-load SSL connections to an intermediate server, you must import the intermediate server’s certificate onto the View Connection Server instances or security servers that it is off-loading. The same SSL server certificate must reside on both the off-loading intermediate server and the off-loaded View servers.

If the intermediate server’s certificate is not installed on the View Connection Server instance or security server, View Clients cannot validate their connections to View. In this situation, the certificate thumbprint sent by the View server does not match the certificate on the intermediate server to which View Clients are connecting.

Do not confuse load balancing with SSL off-loading. The preceding requirement applies to any device that is configured to provide SSL off-loading, including some types of load balancers. However, pure load balancing does not require copying of certificates between devices.

For information about importing certificates to View servers, see "Import a Signed Server Certificate into a Windows Certificate Store" in the **VMware Horizon View Installation** document.
Set View Server External URLs to Point Clients to SSL Off-loading Servers

If SSL is off-loaded to an intermediate server and View Clients use the secure tunnel to connect to View, make sure to set the secure tunnel external URL to an address that clients can use to access the intermediate server. If View Clients use the PCoIP Secure Gateway, set the secure tunnel external URL and PCoIP external URL to addresses that allow clients to connect to the intermediate server.

You configure the external URL settings on the View Connection Server instance or security server that connects to the intermediate server. For more information, see “Configuring External URLs for PCoIP Secure Gateway and Tunnel Connections” in the VMware Horizon View Installation document.

Allow HTTP Connections to Intermediate Servers

When SSL is off-loaded to an intermediate server, you can configure View Connection Server instances or security servers to allow HTTP connections from the client-facing, intermediate devices. The intermediate devices must accept HTTPS for View Client connections.

To allow HTTP connections between View servers and intermediate devices, you must configure the locked.properties file on each View Connection Server instance and security server on which HTTP connections are allowed.

Even when HTTP connections between View servers and intermediate devices are allowed, you cannot disable SSL in View. View servers continue to accept HTTPS connections as well as HTTP connections.

**Note** If your View Clients use smart card authentication, the clients must make HTTPS connections directly to View Connection Server or security server. SSL off-loading is not supported with smart card authentication.

**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. To configure the View server's protocol, add the `serverProtocol` property and set it to `http`.

   The value `http` must be typed in lower case.

3. (Optional) Add properties to configure a non-default HTTP listening port and a network interface on the View server.

   - To change the HTTP listening port from 80, set `serverPortNonSSL` to another port number to which the intermediate device is configured to connect.
   - If the View server has more than one network interface, and you intend the server to listen for HTTP connections on only one interface, set `serverHost` to the IP address of that network interface.

4. Save the locked.properties file.

5. Restart the View Connection Server service or security server service to make your changes take effect.

**Example: locked.properties file**

This file allows non-SSL HTTP connections to a View server. The IP address of the View server’s client-facing network interface is 10.20.30.40. The server uses the default port 80 to listen for HTTP connections. The value `http` must be lower case.

```
serverProtocol=http
serverHost=10.20.30.40
```
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**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Connection Server instance</td>
<td>Select the View Connection Server instance in the View Connection Servers panel and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Security server</td>
<td>Select the security server in the Security Servers panel and click <strong>Edit</strong>.</td>
</tr>
</tbody>
</table>
2 Type the secure tunnel external URL in the **External URL** text box.

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

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

**Note** You can use the IP address if you have to access a View Connection Server instance or security server when the host name is not resolvable. However, the host that you contact will not match the SSL certificate that is configured for the View Connection Server instance or security server, resulting in blocked access or access with reduced security.

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: 10.20.30.40:4172

The URL must contain the IP address and port number that a client system can use to reach this security server 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.

**Join or Withdraw from the Customer Experience Program**

When you install View Connection Server with a new configuration, you can choose to participate in a customer experience improvement program. If you change your mind about participating after the installation, you can join or withdraw from the program by using View Administrator.

If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware’s response to user requirements. No data that identifies your organization is collected.

To review the list of fields from which data is collected, including the fields that are made anonymous, see "Information Collected by the Customer Experience Improvement Program,” on page 368.

**Procedure**

1. In View Administrator, click **View Configuration > Product Licensing and Usage**.
2. In the Customer Experience Program pane, click **Edit Settings**.
3. Decide whether to participate in or withdraw from the program by selecting or deselecting the **Send anonymous data to VMware** checkbox.
4. (Optional) If you participate, you can select the geographic location, type of business, and number of employees in your organization.
5. Click **OK**.

**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 Role-Based Delegated Administration

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,” on page 39
- “Using Folders to Delegate Administration,” on page 40
- “Understanding Permissions,” on page 41
- “Manage Administrators,” on page 42
- “Manage and Review Permissions,” on page 43
- “Manage and Review Folders,” on page 45
- “Manage Custom Roles,” on page 47
- “Predefined Roles and Privileges,” on page 48
- “Required Privileges for Common Tasks,” on page 51
- “Best Practices for Administrator Users and Groups,” on page 53

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.

**NOTE** If you intend to provide access to your desktops through Horizon Workspace, verify that you create the desktop pools as a user with Administrators permissions on the root folder in View. If you give the user Administrators permissions on a folder other than the root folder, Horizon Workspace will not recognize the SAML 2.0 Authenticator you configure in View, and you cannot configure the pool in Horizon Workspace.

- **Different Administrators for Different Folders** on page 40
  You can create a different administrator to manage each folder in your configuration.

- **Different Administrators for the Same Folder** on page 41
  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**

<table>
<thead>
<tr>
<th>Administrator</th>
<th>Role</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>view-domain.com\Admin1</td>
<td>Inventory Administrators</td>
<td>/CorporateDesktops</td>
</tr>
<tr>
<td>view-domain.com\Admin2</td>
<td>Inventory Administrators</td>
<td>/DeveloperDesktops</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Administrator</th>
<th>Role</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>view-domain.com\Admin1</td>
<td>Inventory Administrators</td>
<td>/CorporateDesktops</td>
</tr>
<tr>
<td>view-domain.com\Admin2</td>
<td>Inventory Administrators (Read only)</td>
<td>/CorporateDesktops</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Role</th>
<th>Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory Administrators</td>
<td>MarketingDesktops</td>
</tr>
<tr>
<td>Administrators (Read only)</td>
<td>/</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Admin</th>
<th>Role</th>
<th>Inherited</th>
</tr>
</thead>
<tbody>
<tr>
<td>view-domain.com\Admin1</td>
<td>Inventory Administrators</td>
<td></td>
</tr>
<tr>
<td>view-domain.com\Admin1</td>
<td>Administrators (Read only)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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.
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 View Administrators account are given the Administrators role. You specify the View Administrators account when you install View Connection Server. The View Administrators account can be the local Administrators group (BUILTIN\Administrators) on the View Connection Server computer or a domain user or group account.

**Note** By default, the Domain Admins group is a member of the local Administrators group. If you specified the View Administrators account as the local Administrators group, and 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 42
  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 43
  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 48.
- Familiarize yourself with the best practices for creating administrator users and groups. See “Best Practices for Administrator Users and Groups,” on page 53.
- To assign a custom role to the administrator, create the custom role. See “Add a Custom Role,” on page 47.
- 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 45.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The role you selected applies to folders</td>
<td>Select one or more folders and click Next.</td>
</tr>
<tr>
<td>You want the permission to apply to all folders</td>
<td>Select the root folder and click Next.</td>
</tr>
</tbody>
</table>

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 43
  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 44
  You can delete a permission that includes a specific administrator user or group, a specific role, or a specific folder.

- Review Permissions on page 45
  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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a permission that applies to a specific administrator or group</td>
<td>Select the administrator or group on the Administrators and Groups tab.</td>
</tr>
<tr>
<td>Delete a permission that applies to a specific role</td>
<td>Select the role on the Roles tab.</td>
</tr>
<tr>
<td>Delete a permission that applies to a specific folder</td>
<td>Select the folder on the Folders tab.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the permissions that include a specific administrator or group</td>
<td>Select the administrator or group on the Administrators and Groups tab.</td>
</tr>
<tr>
<td>Review the permissions that include a specific role</td>
<td>Select the role on the Roles tab and click Permissions.</td>
</tr>
<tr>
<td>Review the permissions that include a specific folder</td>
<td>Select the folder on the Folders tab.</td>
</tr>
</tbody>
</table>

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 45
  
  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 46
  
  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 desktop pools from one folder to another.

- **Remove a Folder** on page 46
  
  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 46
  
  You can see all of the desktop pools in a particular folder in View Administrator.

- **Review the Desktops in a Folder** on page 46
  
  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 desktop 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 46.

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 47
  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 47
  You can modify the privileges in a custom role. You cannot modify the predefined administrator roles.

- Remove a Custom Role on page 48
  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 48.

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 48.

Procedure
1 In View Administrator, select View Configuration > Administrators.
2 On the Roles tab, select the role.
3 Click Privileges 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 44.

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 48
  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 49
  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 50
  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 51
  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

<table>
<thead>
<tr>
<th>Role</th>
<th>User Capabilities</th>
<th>Applies to a Folder</th>
</tr>
</thead>
</table>
| 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.                                                                                                                                                           | Yes                 |
|                               | 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.                                                                                                             |                     |
| 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.                                                                                                                                                            | Yes                 |
|                               | 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.                                                                                           |                     |
| Inventory Administrators (Read only) | View, but not modify, inventory objects.                                                                                                                                                                               | Yes                 |
|                               | When administrators have this role on a folder, they can only view the inventory objects in that folder.                                                                                                             |                     |

**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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>User Capabilities</th>
<th>Predefined Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console Interaction</td>
<td>Log in to and use View Administrator.</td>
<td>Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrators (Read only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inventory Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inventory Administrators (Read only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global Configuration and Policy Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Global Configuration and Policy Administrators (Read only)</td>
</tr>
<tr>
<td>Direct Interaction</td>
<td>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.</td>
<td>Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Administrators (Read only)</td>
</tr>
<tr>
<td>Manage Global Configuration and Policies</td>
<td>View and modify global policies and configuration settings except for administrator roles and permissions.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Manage Roles and Permissions</td>
<td>Create, modify, and delete administrator roles and permissions.</td>
<td>Administrators</td>
</tr>
<tr>
<td>Register Agent</td>
<td>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.</td>
<td>Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent Registration Administrators</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>User Capabilities</th>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Pool</td>
<td>Enable and disable desktop pools.</td>
<td>Desktop pool</td>
</tr>
<tr>
<td>Entitle Pool</td>
<td>Add and remove user entitlements.</td>
<td>Desktop pool</td>
</tr>
<tr>
<td>Manage Composer Pool Image</td>
<td>Resync, Refresh, and Rebalance linked-clone pools and change the default pool image.</td>
<td>Desktop pool</td>
</tr>
<tr>
<td>Manage Desktop</td>
<td>Perform all desktop and session-related operations.</td>
<td>Desktop</td>
</tr>
<tr>
<td>Manage Local Sessions</td>
<td>Roll back and initiate replications for local desktops.</td>
<td>Desktop</td>
</tr>
<tr>
<td>Manage Persistent Disks</td>
<td>Perform all View Composer persistent disk operations, including attaching, detaching, and importing persistent disks.</td>
<td>Persistent disk</td>
</tr>
<tr>
<td>Manage Pool</td>
<td>Add, modify, and delete desktop pools and add and remove desktops.</td>
<td>Desktop pool</td>
</tr>
<tr>
<td>Manage Remote Sessions</td>
<td>Disconnect and log off remote sessions and send messages to desktop users.</td>
<td>Desktop</td>
</tr>
<tr>
<td>Manage Reboot Operation</td>
<td>Reset desktops.</td>
<td>Desktop</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Predefined Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full (Read only)</td>
<td>Grants read-only access to all settings.</td>
<td>Administrators (Read only)</td>
</tr>
<tr>
<td>Manage Inventory (Read only)</td>
<td>Grants read-only access to inventory objects.</td>
<td>Inventory Administrators (Read only)</td>
</tr>
<tr>
<td>Manage Global Configuration and Policies (Read only)</td>
<td>Grants read-only access to configuration settings and global policies except for administrators and roles.</td>
<td>Global Configuration and Policy Administrators (Read only)</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable or disable a pool</td>
<td>Enable Pool on the pool.</td>
</tr>
<tr>
<td>Entitle or unentitle users to a pool</td>
<td>Entitle Pool on the pool.</td>
</tr>
</tbody>
</table>
| Add a pool | Manage Pool  

 laborious 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

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

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detach a disk</td>
<td>Manage Persistent Disks on the disk and Manage Pool on the pool.</td>
</tr>
<tr>
<td>Attach a disk</td>
<td>Manage Persistent Disks on the disk and Manage Pool on the desktop.</td>
</tr>
<tr>
<td>Edit a disk</td>
<td>Manage Persistent Disks on the disk and Manage Pool on the selected pool.</td>
</tr>
<tr>
<td>Change folders</td>
<td>Manage Persistent Disks on the source and target folders.</td>
</tr>
<tr>
<td>Recreate desktop</td>
<td>Manage Persistent Disks on the disk and Manage Pool on the last pool.</td>
</tr>
<tr>
<td>Import from vCenter</td>
<td>Manage Persistent Disks on the folder and Manage Pool on the pool.</td>
</tr>
<tr>
<td>Delete a disk</td>
<td>Manage Persistent Disks on the disk.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update general user information</td>
<td>Manage Global Configuration and Policies</td>
</tr>
<tr>
<td>Send messages to desktop users</td>
<td>Manage Remote Sessions on the desktop.</td>
</tr>
<tr>
<td>Add an administrator user or group</td>
<td>Manage Roles and Permissions</td>
</tr>
<tr>
<td>Add, modify, or delete an administrator permission</td>
<td>Manage Roles and Permissions</td>
</tr>
<tr>
<td>Add, modify, or delete an administrator role</td>
<td>Manage Roles and Permissions</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Task</th>
<th>Required Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or delete a folder</td>
<td>Must have the Administrators role on the root folder.</td>
</tr>
<tr>
<td>Manage ThinApp applications and settings in View Administrator</td>
<td>Must have the Administrators role on the root folder.</td>
</tr>
<tr>
<td>View and modify View Transfer Server instances and the Transfer Server repository</td>
<td>Must have the Administrators role on the root folder.</td>
</tr>
<tr>
<td>Install View Agent on an unmanaged desktop source, such as a physical system, standalone virtual machine, or terminal server</td>
<td>Register Agent</td>
</tr>
<tr>
<td>View or modify configuration settings (except for administrators) in View Administrator</td>
<td>Manage Global Configuration and Policies</td>
</tr>
<tr>
<td>Run all PowerShell commands and command line utilities except for vdmadmin and vdmimport.</td>
<td>Direct Interaction</td>
</tr>
<tr>
<td>Use the vdmadmin and vdmimport commands</td>
<td>Must have the Administrators role on the root folder.</td>
</tr>
<tr>
<td>Use the vdmexport command</td>
<td>Must have the Administrators role or the Administrators (Read only) role on the root folder.</td>
</tr>
</tbody>
</table>

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

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,” on page 55
- “Install View Agent on an Unmanaged Desktop Source,” on page 55

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 Horizon 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 55.

Install View Agent on an Unmanaged Desktop Source

You must install View Agent on 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 66.
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 57.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the VMware Horizon 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 xxxx 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate as the currently logged in user</td>
<td>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.</td>
</tr>
<tr>
<td>Specify administrator credentials</td>
<td>You must provide the username and password of a View Connection Server administrator in the Username and Password text boxes.</td>
</tr>
</tbody>
</table>
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 119.
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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Redirection</td>
<td>Gives users access to locally connected USB devices on their desktops. Windows 2003 and Windows 2008 do not support USB redirection. <strong>Note</strong> You can use group policy settings to disable USB redirection for specific users.</td>
</tr>
<tr>
<td>PCoIP Server</td>
<td>Lets users connect to the View desktop with the PCoIP display protocol. <strong>Note</strong> On Windows Vista, if you install the PCoIP Server component, the Windows group policy <strong>Disable or enable software Secure Attention Sequence</strong> is enabled and set to <strong>Services and Ease of Access applications</strong>. If you change this setting, single sign-on does not work correctly.</td>
</tr>
<tr>
<td>PCoIP Smartcard</td>
<td>Lets users authenticate with smart cards when they use the PCoIP display protocol.</td>
</tr>
</tbody>
</table>
Creating and Preparing Virtual Machines

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,” on page 59
- “Install View Agent on a Virtual Machine,” on page 64
- “Install View Agent Silently,” on page 66
- “Configure a Virtual Machine with Multiple NICs for View Agent,” on page 70
- “Optimize Windows Guest Operating System Performance,” on page 70
- “Optimize Windows 7 and Windows 8 Guest Operating System Performance,” on page 71
- “Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops,” on page 73
- “Preparing Virtual Machines for View Composer,” on page 79
- “Creating Virtual Machine Templates,” on page 85
- “Creating Customization Specifications,” on page 86

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 59
   You use vSphere Client to create virtual machines in vCenter Server for View desktops.

2. Install a Guest Operating System on page 61
   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 62
   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 60.

**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>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Location</td>
<td>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.</td>
</tr>
<tr>
<td>Host/Cluster</td>
<td>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.</td>
</tr>
<tr>
<td>Resource Pool</td>
<td>If the physical ESX server resources are divided into resource pools, you can assign them to the virtual machine.</td>
</tr>
<tr>
<td>Datastore</td>
<td>The location of files associated with the virtual machine.</td>
</tr>
<tr>
<td>Hardware Machine Version</td>
<td>If you create the virtual machine on an ESXi 5.1 or later host or cluster, you can select virtual hardware version 9 or 8. Version 9 provides greater virtual machine functionality. If the host or cluster is ESX/ESXi 5.0 or later, you can select virtual hardware version 8 or 7. If the host or cluster is ESX/ESXi 4.0 or later, you can select virtual hardware version 7 only.</td>
</tr>
<tr>
<td>Guest Operating System</td>
<td>The type of operating system that you will install in the virtual machine.</td>
</tr>
</tbody>
</table>
### Table 4-1. Custom Configuration Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description and Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPUs</td>
<td>The number of virtual processors in the virtual machine. For most guest operating systems, a single processor is sufficient.</td>
</tr>
<tr>
<td>Memory</td>
<td>The amount of memory to allocate to the virtual machine. In most cases, 512MB is sufficient.</td>
</tr>
</tbody>
</table>
| 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 70 for more information. **Important** For Windows 8, 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](http://support.microsoft.com/kb/2550978)  
  - For Windows 7 versions previous to SP1: [http://support.microsoft.com/kb/2344941](http://support.microsoft.com/kb/2344941) |
| SCSI Controller| The type of SCSI adapter to use with the virtual machine. For Windows 8, 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 and later. **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 or Windows 8, 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 Horizon 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 Horizon 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 139.
- Verify that you have administrative rights on the guest operating system.
- On Windows Vista operating systems, verify that the Windows Update Service is enabled. If you disable this service on Windows Vista, the View Agent installer fails to install the USB driver.
- If you intend to configure 3D graphics rendering for desktop pools, familiarize yourself with the Enable 3D Support setting for virtual machines.
  This setting is active on Windows 7 and later operating systems. On ESXi 5.1 and later hosts, you can also select options that determine how the 3D renderer is managed on the ESXi host. For details, see the vSphere Virtual Machine Administration document.
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.
   - If you plan to use Horizon Workspace to offer a catalog that includes ThinApp applications, you must install the Horizon Agent.
   - 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 View clients will connect to the virtual machine with the PCoIP display protocol, go to Control Panel > System > Advanced System Settings > Performance Settings and change the setting for Visual Effects to Adjust for best performance.
   - If you instead use the setting called Adjust for best appearance or Let Windows choose what's best for my computer and Windows chooses appearance instead of performance, performance is negatively affected.
10. If a proxy server is used in your network environment, configure network proxy settings.
11. 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.
12. 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.
13. Configure the Windows firewall to allow Remote Desktop connections to the virtual machine.
(Optional) Disable Hot Plug PCI devices. This step prevents users from accidentally disconnecting the virtual network device (vNIC) from the virtual machine.

(Optional) Configure user customization scripts.

What to do next

Install View Agent. See “Install View Agent on a Virtual Machine,” on page 64.

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 66.

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

Prerequisites

- Prepare the guest operating system for View desktop deployment. See “Prepare a Guest Operating System for View Desktop Deployment,” on page 62.
- 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 65.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the VMware Horizon 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 xxxxx 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.
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 70.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Redirection</td>
<td>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.</td>
</tr>
<tr>
<td>View Composer Agent</td>
<td>Lets View Agent run on the linked-clone desktops that are deployed from this virtual machine.</td>
</tr>
<tr>
<td>Virtual Printing</td>
<td>Lets users print to any printer available on their Windows client computers. Users do not have to install additional drivers on their desktops.</td>
</tr>
<tr>
<td>PCoIP Server</td>
<td>Lets users connect to the View desktop using the PCoIP display protocol. Installing the PCoIP Server feature disables sleep mode on Windows 8, 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.</td>
</tr>
<tr>
<td>PCoIP Smartcard</td>
<td>Lets users authenticate with smart cards when they use the PCoIP display protocol.</td>
</tr>
<tr>
<td>View Persona Management</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 62.
- 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 xxxxx 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 65.
- If you select the View Composer Agent custom setup option, verify that you have a license to use View Composer.
- Familiarize yourself with the silent installation properties available with View Agent. See “Silent Installation Properties for View Agent,” on page 68.
- Familiarize yourself with the TCP ports that the View Agent installation program opens on the firewall. See the VMware Horizon 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 70.

**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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/s</code></td>
<td>Disables the bootstrap splash screen and extraction dialog, which prevents the display of interactive dialogs.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code></td>
</tr>
<tr>
<td></td>
<td>The <code>/s</code> option is required to run a silent installation.</td>
</tr>
<tr>
<td><code>/v&quot;MSI_command_line_options&quot;</code></td>
<td>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 <code>/v</code> and at the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;command_line_options&quot;</code></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v&quot;command_line_options INSTALLDIR=&quot;d:\abc\my folder&quot;&quot;&quot;</code></td>
</tr>
<tr>
<td></td>
<td>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 <code>/v&quot;command_line_options&quot;</code> option is required to run a silent installation.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>MSI Option or Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/qn</td>
<td>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: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn&quot;</code> 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.</td>
</tr>
<tr>
<td>INSTALLDIR</td>
<td>Specifies an alternative installation path for the View component. Use the format <code>INSTALLDIR=path</code> 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.</td>
</tr>
<tr>
<td>ADDLOCAL</td>
<td>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 <code>ADDLOCAL=ALL</code>. For example: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=ALL&quot;</code> 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 <code>ADDLOCAL=value,value,value...</code>. For example, you might want to install View Agent in a guest operating system with the View Composer Agent and PCoIP features: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v&quot;/qn ADDLOCAL=Core,SVIAgent,PCoIP&quot;</code> Note: The Core feature is required in View Agent. This MSI property is optional.</td>
</tr>
<tr>
<td>REBOOT</td>
<td>You can use the <code>REBOOT=ReallySuppress</code> option to allow system configuration tasks to complete before the system reboots. This MSI property is optional.</td>
</tr>
<tr>
<td>/l*v log_file</td>
<td>Writes logging information into the specified log file with verbose output. For example: <code>/l*v &quot;&quot;%TEMP%\vmmsi.log&quot;&quot;</code> 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.</td>
</tr>
</tbody>
</table>

**Silent Installation Properties for View Agent**

You can include specific properties when you silently install View Agent 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

<table>
<thead>
<tr>
<th>MSI Property</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALLDIR</td>
<td>The path and folder in which the View Agent software is installed. For example: INSTALLDIR=&quot;D:\abc\my folder&quot; 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.</td>
<td>%ProgramFiles%\VMware\VMware View\Agent</td>
</tr>
<tr>
<td>RDPCHOICE</td>
<td>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.</td>
<td>1</td>
</tr>
<tr>
<td>VDM_VC_MANAGED_AGENT</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_NAME</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_USERNAME</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>VDM_SERVER_PASSWORD</td>
<td>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.</td>
<td>None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Silent Installation Feature</th>
<th>Custom Setup Option in an Interactive Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core.</td>
<td>None.</td>
</tr>
<tr>
<td>If you specify individual features with the MSI property, ADDLOCAL=, you must include Core.</td>
<td>During an interactive installation, the core View Agent functions are installed by default.</td>
</tr>
<tr>
<td>If you specify ADDLOCAL=ALL, all features, including Core, are installed.</td>
<td></td>
</tr>
<tr>
<td>SVIAgent</td>
<td>View Composer Agent</td>
</tr>
<tr>
<td>ThinPrint</td>
<td>Virtual Printing</td>
</tr>
</tbody>
</table>
Table 4-6. View Agent Silent Installation Features and Interactive Custom Setup Options (Continued)

<table>
<thead>
<tr>
<th>Silent Installation Feature</th>
<th>Custom Setup Option in an Interactive Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThinPrintPCoIP</td>
<td>Virtual Printing with PCoIP</td>
</tr>
<tr>
<td>PCoIP</td>
<td>PCoIP Protocol</td>
</tr>
<tr>
<td>USB</td>
<td>USB Redirection</td>
</tr>
<tr>
<td>VPA</td>
<td>View Persona Management</td>
</tr>
<tr>
<td>VmVideo</td>
<td>In an interactive installation, this feature is not a separate custom setup option.</td>
</tr>
<tr>
<td>VmwVAudio</td>
<td>In an interactive installation, this feature is not a separate custom setup option.</td>
</tr>
<tr>
<td>SmartCard</td>
<td>In an interactive installation, the SmartCard feature is not a separate custom setup option.</td>
</tr>
<tr>
<td>VMCI</td>
<td>In an interactive installation, the VMCI feature is not a separate custom setup option.</td>
</tr>
</tbody>
</table>

For details about the custom setup options, see “View Agent Custom Setup Options,” on page 65.

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.
  - Choose a basic theme.
  - Set the background to a solid color.
  - Set the screen saver to None.
  - 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 who 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 as 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.

If users are going to play full-screen videos or run 3D applications on desktops that run in a vSphere 5.1 environment, follow the instructions to modify the registry described in Microsoft KB 235257.

The Microsoft KB is titled “Server Does Not Use All Bandwidth Available When Streaming Files with Bit Rates over 100 Kbps” and is located at [http://support.microsoft.com/kb/235257](http://support.microsoft.com/kb/235257). Restart the virtual machine to enable the modified registry setting to take effect.

Without this optimization, brief freezes can occur, or the videos can stutter.

**Note**  Making this optimization delivers performance improvements in both ESXi 5.x and ESXi 5.1, but it is required for ESXi 5.1.

**What to do next**

For Windows 7 and Windows 8 guest operating systems, perform additional optimization tasks. See “Optimize Windows 7 and Windows 8 Guest Operating System Performance,” on page 71.

**Optimize Windows 7 and Windows 8 Guest Operating System Performance**

You can perform additional steps to optimize Windows 7 and Windows 8 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 70.

- Familiarize yourself with the procedure for disabling the Windows Customer Experience Improvement Program. See “Disable the Windows Customer Experience Improvement Program,” on page 72.
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. Turn off the Windows Customer Experience Improvement Program and disable related tasks from the Task Scheduler.
6. Shut down the guest operating system and power off the virtual machine.
7. Power on the virtual machine.

What to do next

See “Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops,” on page 73 for information on disabling certain Windows 7 and Windows 8 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.

Disable the Windows Customer Experience Improvement Program

Disabling the Windows Customer Experience Improvement Program and the related Task Scheduler tasks that control this program can improve Windows 7 and Windows 8 system performance in large View desktop pools.

Procedure

1. In the Windows 7 or Windows 8 guest operating system, start the control panel and click Action Center > Change Action Center settings.
2. Click Customer Experience Improvement Program settings.
3. Select No, I don’t want to participate in the program and click Save changes.
4. Start the control panel and click Administrative Tools > Task Scheduler.
5. In the Task Scheduler (Local) pane of the Task Scheduler dialog box, expand the Task Scheduler Library > Microsoft > Windows nodes and open the Application Experience folder.
6. Disable the AITAgent and ProgramDataUpdater tasks.
7. In the Task Scheduler Library > Microsoft > Windows node, open the Customer Experience Improvement Program folder.
8. Disable the Consolidator, KernelCEIPTask, and Use CEIP tasks.

What to do next

Perform other Windows 7 or Windows 8 optimization tasks. See “Optimize Windows 7 and Windows 8 Guest Operating System Performance,” on page 71.
Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops

By disabling certain Windows 7 or Windows 8 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 and Windows 8 Services and Tasks

Windows 7 and Windows 8 schedule 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 services.

Windows 7 and Windows 8 introduce 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 or Windows 8 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 and Windows 8 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 and Windows 8 Services and Tasks That Cause Linked-Clone Growth

Certain services and tasks in Windows 7 and Windows 8 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 Windows 7 and Windows 8 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 or Windows 8 services that are shown in `Table 4-7`, verify that you took the optimization steps in “Optimize Windows Guest Operating System Performance,” on page 70 and “Optimize Windows 7 and Windows 8 Guest Operating System Performance,” on page 71.
Table 4-7. Impact of Windows 7 and Windows 8 Services and Tasks on OS Disk Growth and IOPS When OS Is Left Idle

<table>
<thead>
<tr>
<th>Service or Task</th>
<th>Description</th>
<th>Default Occurrence or Startup</th>
<th>Impact on Linked-Clone OS Disks</th>
<th>Impact on IOPS</th>
<th>Turn Off This Service or Task?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Hibernation</td>
<td>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.</td>
<td>Default power-plan settings disable hibernation.</td>
<td>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.</td>
<td>High. When hibernation is triggered, the system writes a hiberfil.sys file the size of the installed RAM.</td>
<td>Yes Hibernation provides no benefit in a virtual environment. For instructions, see “Disable Windows Hibernation in the Parent Virtual Machine,” on page 82..</td>
</tr>
<tr>
<td>Windows Scheduled Disk Defragmentation</td>
<td>Disk defragmentation is scheduled as a background process.</td>
<td>Once a week</td>
<td>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.</td>
<td>High</td>
<td>Yes</td>
</tr>
<tr>
<td>Windows Update Service</td>
<td>Detects, downloads, and installs updates for Windows and other programs.</td>
<td>Automatic startup</td>
<td>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.</td>
<td>Medium to high</td>
<td>Yes, if you use View Composer recompose to install Windows updates and refresh to return OS disks to their original snapshots.</td>
</tr>
<tr>
<td>Windows Diagnostic Policy Service</td>
<td>Detects, troubleshoots, and resolves problems in Windows components. If you stop this service, diagnostics no longer function.</td>
<td>Automatic startup</td>
<td>Medium to high. The service is triggered on demand. The write frequency varies, depending on demand.</td>
<td>Small to medium</td>
<td>Yes, if you do not need the diagnostic tools to function on the desktops.</td>
</tr>
<tr>
<td>Prefetch/Superfetch</td>
<td>Stores specific information about applications that you run to help them start faster. This feature was introduced in Windows XP.</td>
<td>Always on, unless it is disabled.</td>
<td>Medium</td>
<td>Causes periodic updates to its layout and database information and individual prefetch files, which are generated on demand.</td>
<td>Medium</td>
</tr>
<tr>
<td>Service or Task</td>
<td>Description</td>
<td>Default Occurrence or Startup</td>
<td>Impact on Linked-Clone OS Disks</td>
<td>Impact on IOPS</td>
<td>Turn Off This Service or Task?</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------------------------</td>
<td>--------------------------------</td>
<td>---------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Windows Registry Backup (RegIdleBackup)</td>
<td>Automatically backs up the Windows registry when the system is idle.</td>
<td>Every 10 days at 12:00 am</td>
<td>Medium. Each time this task runs, it generates registry backup files.</td>
<td>Medium.</td>
<td>Yes. There is no need for Windows Registry Backup. To restore registry data, you can use the View Composer refresh operation.</td>
</tr>
<tr>
<td>System Restore</td>
<td>Reverts the Windows system to a previous, healthy state.</td>
<td>When Windows starts up and once a day thereafter.</td>
<td>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.</td>
<td>No major impact.</td>
<td>Although its impact is small, this task is redundant if you use View Composer refresh to return OS disks to their original snapshots.</td>
</tr>
<tr>
<td>Windows Defender</td>
<td>Provides anti-spyware features.</td>
<td>When Windows starts up. Performs a quick scan once a day. Checks for updates before each scan.</td>
<td>Medium to high. Performs definition updates, scheduled scans, and scans that are started on demand.</td>
<td>Medium to high.</td>
<td>Yes, if other anti-spyware software is installed.</td>
</tr>
<tr>
<td>Microsoft Feeds Synchronization task (msfeedssync.exe)</td>
<td>Periodically updates RSS feeds in Windows Internet Explorer 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 is running.</td>
<td>Once a day.</td>
<td>Medium. Affects OS-disk growth if persistent disks are not configured. If persistent disks are configured, the impact is diverted to the persistent disks.</td>
<td>Medium</td>
<td>Yes, if your users do not require automatic RSS feed updates on their desktops.</td>
</tr>
</tbody>
</table>

### Disable Scheduled Disk Defragmentation on Windows 7 and Windows 8 Parent Virtual Machines

Before you create linked clones, you must disable scheduled defragmentations on Windows 7 and Windows 8 parent virtual machines. Windows 7 and Windows 8 schedule 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 or Windows 8 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**. 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 and Windows 8 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 or Windows 8 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 and Windows 8 Virtual Machines

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

Do not 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 or Windows 8 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 and Windows 8 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 and Windows 8.

**Procedure**

1. Start the Windows Registry Editor on the local Windows 7 or Windows 8 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 and Windows 8 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 or Windows 8 guest operating system as an administrator.
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 and Windows 8 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 or Windows 8 guest operating system as an administrator.
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 and Windows 8 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 or Windows 8 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 and Windows 8 Virtual Machines**

Windows Internet Explorer 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 or Windows 8 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 80
  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 on Linked-Clone Desktops** on page 82
  To make sure that View Composer properly activates Windows 8, 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 82
  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 83
  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 84
  
  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 84
  
  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 59.

  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.

  **IMPORTANT** Linked clones and virtual machines that were converted from linked clones are not supported as parent virtual machines.


  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 64.

  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 8, 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 on Linked-Clone Desktops,” on page 82.
If the parent virtual machine runs Windows 7 or Windows 8, verify that you followed the best practices for optimizing the operating system. See “Optimizing Windows 7 and Windows 8 for Linked-Clone Desktops,” on page 73.


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.

**NOTE** If the parent virtual machine contains multiple virtual disks, when you create a desktop pool, do not select a drive letter for the View Composer persistent disk or disposable data disk that already exists on the parent virtual machine or that conflicts with a drive letter that is used for a network-mounted drive.

- Verify that the virtual machine does not contain an independent disk.

An independent disk is excluded when you take a snapshot of the virtual machine. Linked clones that are created or recomposed from the virtual machine will not contain the independent disk.

- If you plan to configure disposable data disks when you create linked-clone desktops, remove default user `TEMP` and `TMP` variables from the parent virtual machine.

You can also remove the `pagefile.sys` file to avoid duplicating the file on all the linked clones. If you leave the `pagefile.sys` file on the parent virtual machine, a read-only version of the file is inherited by the linked clones, while a second version of the file is used on the disposable data disk.

- Disable the hibernation option to reduce the size of linked-clone OS disks that are created from the parent virtual machine.

- Before you take a snapshot of the parent virtual machine, disable searching Windows Update for device drivers.

  This Windows feature can interfere with the customization of linked-clone desktops. As each linked clone is customized, Windows might search for the best drivers on the Internet for that clone, resulting in repeated searches and customization delays.

- 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 on Linked-Clone Desktops

To make sure that View Composer properly activates Windows 8, 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 8, 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 or Windows 8 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 8, 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.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Action</th>
</tr>
</thead>
</table>
| Windows 8, 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 92.

**Prerequisites**

Prepare the parent virtual machine to meet the requirements of the View Composer service. See “Prepare a Parent Virtual Machine,” on page 80.

**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.

As a best practice, you can remove the pagefile.sys file from the parent virtual machine before you take a snapshot, to avoid duplicating the file on all the linked clones. See “Prepare a Parent Virtual Machine,” on page 80.

NOTE  This feature is not the same as configuring local storage for the virtual-machine swap files. See “Configure a Parent Virtual Machine to Use Local Storage,” on page 83.

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 80.

**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 88 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 8, Windows 7 or Vista. Sysprep tools are built into these operating systems.

When you use a Sysprep customization specification to join a Windows 8 or 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

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 88
  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 92
  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 119
  To create a manual desktop pool, View Manager provisions desktops from existing desktop sources. You select a separate desktop source for each desktop in the pool.

- **Microsoft Terminal Services Pools** on page 123
  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 125
  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 140
  You can configure a power policy for the virtual machines in a desktop pool if the virtual machines are managed by vCenter Server.

- **Configure View Storage Accelerator for Desktop Pools** on page 145
  You can configure desktop pools to enable ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator can reduce IOPS and improve performance during boot storms, when many desktops start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. To use this feature, you must make sure that View Storage Accelerator is enabled for individual desktop pools.
Deploying Large Desktop Pools on page 147

When many users require the same desktop image, you can create one large automated pool from a single template or parent virtual machine. By using a single base image and pool name, you can avoid dividing the desktops arbitrarily into smaller groups that must be managed separately. This strategy simplifies your View deployment and administration tasks.

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 92.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>User assignment</td>
<td>Choose the type of user assignment:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- In a dedicated-assignment pool, each user is assigned to a desktop. Users receive the same desktop each time they log in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- In a floating-assignment pool, users receive different desktops each time they log in.</td>
<td>For details, see “User Assignment in Desktop Pools,” on page 126.</td>
</tr>
<tr>
<td>Enable automatic assignment</td>
<td>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.</td>
<td>If you do not enable automatic assignment, you must explicitly assign a desktop to each user.</td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Select the vCenter Server that manages the virtual machines in the pool.</td>
<td></td>
</tr>
<tr>
<td>Pool ID</td>
<td>The unique name that identifies the pool in View Administrator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If multiple vCenter Servers are running in your environment, make sure that another vCenter Server is not using the same pool ID.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Display name</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Folder</td>
<td>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 40. 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.</td>
<td></td>
</tr>
<tr>
<td>Delete desktop after logoff</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Pool Settings</td>
<td>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 132. For a list of the settings that apply to automated pools, see “Desktop Settings for Automated Pools That Contain Full Virtual Machines,” on page 91. For more information about power policies and automated pools, see “Setting Power Policies for Desktop Pools,” on page 140.</td>
<td></td>
</tr>
<tr>
<td>Virtual machine naming</td>
<td>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 126.</td>
<td></td>
</tr>
<tr>
<td>List of desktop names</td>
<td>If you specify names manually, prepare a list of desktop names and, optionally, the associated user names.</td>
<td></td>
</tr>
<tr>
<td>Naming pattern</td>
<td>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 129.</td>
<td></td>
</tr>
<tr>
<td>Maximum number of desktops</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Number of spare (powered on) desktops</td>
<td>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 126. When you specify names manually, this option is called # Unassigned desktops kept powered on.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-1. Worksheet: Configuration Options for Creating an Automated Pool That Contains Full Virtual Machines (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum number of desktops</td>
<td>If you use a naming pattern and provision desktops on demand, specify a minimum number of desktops in the pool. View Manager creates the minimum number of desktops when you create the pool. If you provision desktops on demand, View Manager dynamically creates additional desktops as users connect to the pool for the first time or as you assign desktops to users.</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>Select the virtual machine template that View Manager uses to create the pool.</td>
<td></td>
</tr>
<tr>
<td>vCenter Server folder</td>
<td>Select the folder in vCenter Server in which the desktop pool resides.</td>
<td></td>
</tr>
<tr>
<td>Host or cluster</td>
<td>Select the ESX host or cluster on which the desktop virtual machines run. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts.</td>
<td></td>
</tr>
<tr>
<td>Resource pool</td>
<td>Select the vCenter Server resource pool in which the desktop pool resides.</td>
<td></td>
</tr>
<tr>
<td>Datastores</td>
<td>Select one or more datastores on which to store the desktop pool. For clusters, you can use shared or local datastores.</td>
<td></td>
</tr>
<tr>
<td>Use View Storage Accelerator</td>
<td>Determine whether ESXi hosts cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. For details, see “Configure View Storage Accelerator for Desktop Pools,” on page 145.</td>
<td></td>
</tr>
<tr>
<td>Guest customization</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>

### 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 92.

### 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 59.
- 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 88.

Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See “Desktop and Pool Settings,” on page 132.

If you intend to provide access to your desktops through Horizon Workspace, verify that you create the desktop pools as a user with Administrators permissions on the root folder in View. If you give the user Administrators permissions on a folder other than the root folder, Horizon Workspace will not recognize the SAML Authenticator you configure in View, and you cannot configure the pool in Horizon Workspace.

Procedure
1. In View Administrator, click Inventory > Pools.
2. Click Add.
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 149.

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 132.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Automated Pool, Dedicated Assignment</th>
<th>Automated Pool, Floating Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection Server restrictions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote desktop power policy</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic logoff after disconnect</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow users to reset their desktops</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow multiple sessions per user</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Delete desktop after logout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Default display protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 5-2. Settings for Automated Pools That Contain Full Virtual Machines (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Automated Pool, Dedicated Assignment</th>
<th>Automated Pool, Floating Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to choose protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3D Renderer</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Max number of monitors</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Max resolution of any one monitor</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Adobe Flash quality</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Adobe Flash throttling</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>User assignment</td>
<td>Choose the type of user assignment:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In a dedicated-assignment pool, each user is assigned to a desktop. Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>receive the same desktop each time they log in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ In a floating-assignment pool, users receive different desktops each time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>they log in.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For details, see “User Assignment in Desktop Pools,” on page 126.</td>
<td></td>
</tr>
<tr>
<td>Enable automatic assignment</td>
<td>In a dedicated-assignment pool, a desktop is assigned to a user when the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user first logs in to the pool. You can also explicitly assign desktops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>to users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you do not enable automatic assignment, you must explicitly assign a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>desktop to each user.</td>
<td></td>
</tr>
<tr>
<td>vCenter Server</td>
<td>Select the vCenter Server that manages the virtual machines in the pool.</td>
<td></td>
</tr>
</tbody>
</table>
**Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool ID</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Display name</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>View Folder</td>
<td>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 40. 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.</td>
<td></td>
</tr>
<tr>
<td>Delete or refresh desktop on logoff</td>
<td>If you select floating user assignment, choose whether to refresh desktops, delete desktops, or do nothing after users log off. For details, see “Using Folders to Delegate Administration,” on page 40. Note: You set this option on the Pool Settings page.</td>
<td></td>
</tr>
<tr>
<td>Pool Settings</td>
<td>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 132. For a list of the settings that apply to linked-clone pools, see “Desktop Settings for Linked-Clone Desktop Pools,” on page 102. For more information about power policies and automated pools, see “Setting Power Policies for Desktop Pools,” on page 140.</td>
<td></td>
</tr>
<tr>
<td>Virtual machine naming</td>
<td>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 126.</td>
<td></td>
</tr>
<tr>
<td>List of desktop names</td>
<td>If you specify names manually, prepare a list of desktop names and, optionally, the associated user names.</td>
<td></td>
</tr>
<tr>
<td>Naming pattern</td>
<td>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 129.</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Max number of desktops</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Number of spare (powered on) desktops</td>
<td>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 126. When you specify names manually, this option is called # Unassigned desktops kept powered on.</td>
<td></td>
</tr>
<tr>
<td>Minimum number of ready (provisioned) desktops during View Composer maintenance operations</td>
<td>If you specify names manually or use a naming pattern, specify a minimum number of desktops that are ready and provisioned while View Composer operations take place. This setting lets you keep desktops provisioned and ready to accept connection requests from users while View Composer refreshes, recomposes, or rebalances the desktops in the pool. This value must be smaller than the Min number of desktops, which you specify if you provision desktops on demand. See “Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations,” on page 117.</td>
<td></td>
</tr>
</tbody>
</table>
| Provision desktops on demand or Provision all desktops up front | If you use a naming pattern, choose whether to provision all desktops when the pool is created or provision desktops as they are needed.  
• Provision all desktops up front. When the pool is created, View Manager provisions the number of desktops you specify in Max number of desktops.  
• Provision desktops on demand. When the pool is created, View Manager creates the number of desktops that you specify in Min number of desktops. View Manager dynamically creates additional desktops as users connect to the pool for the first time or as you assign desktops to users. |
| Min number of desktops                      | If you use a naming pattern and provision desktops on demand, specify a minimum number of desktops in the pool. View Manager creates the minimum number of desktops when you create the pool. View Manager maintains the minimum number of desktops even when other settings such as Delete or refresh desktop on logoff cause desktops to be deleted. |
### Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect Windows profile to persistent disks</td>
<td>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 recreate the linked-clone desktop from the detached disk. For example, when a desktop or pool is deleted, you can detach the persistent disk and recreate the desktop, preserving the original user data and settings. If you store the Windows profile in the OS disk, user data and settings are removed during refresh, recompose, and rebalance operations.</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>Disk size and drive letter for persistent disk</td>
<td>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.</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>Disposable File Redirection</td>
<td>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.</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>Disk size and drive letter for disposable file disk</td>
<td>If you redirect disposable files to a nonpersistent disk, provide the disk size in megabytes and the drive letter. The disk size should be larger than page-file size of the guest OS. To determine the page-file size, see &quot;Keep a Record of the Parent Virtual Machine’s Paging-File Size,&quot; on page 84. 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. You can select a drive letter for the disposable file disk. The default value, Auto, directs View to assign 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.</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>Select separate datastores for persistent and OS disks</td>
<td>If you redirect user profiles to separate persistent disks, you can store the persistent disks and OS disks on different datastores.</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Fill In Your Value Here</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Select separate datastores for replica and OS disks</td>
<td>You can store the replica (master) virtual machine disk on a high performance datastore and the linked clones on separate datastores. For details, see “Storing View Composer Replicas and Linked Clones on Separate Datastores,” on page 113. If you store replicas and OS disks on separate datastores, native NFS snapshots cannot be used. Native cloning on a NAS device can only take place if the replica and OS disks are stored on the same datastores.</td>
<td></td>
</tr>
<tr>
<td>Parent virtual machine</td>
<td>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. <strong>Note</strong>: You cannot use View Composer to deploy desktops that run Windows Vista Ultimate Edition or Windows XP Professional SP1.</td>
<td></td>
</tr>
<tr>
<td>Default image (snapshot)</td>
<td>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 linked clones in the pool use the default image, and 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. The parent virtual machine and snapshot are also required for View Composer maintenance operations.</td>
<td></td>
</tr>
<tr>
<td>Publish base image to the Transfer Server repository.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>vCenter Server folder</td>
<td>Select the folder in vCenter Server in which the desktop pool resides.</td>
<td></td>
</tr>
<tr>
<td>Host or cluster</td>
<td>Select the ESX host or cluster on which the desktop virtual machines run. In vSphere 5.1 or later, you can select a cluster with up to 32 ESXi hosts if the replicas are stored on VMFS5 or later datastores or NFS datastores. If you store replicas on a VMFS version earlier than VMFS5, a cluster can have at most eight hosts. In vSphere 5.0, you can select a cluster with more than eight ESXi hosts if the replicas are stored on NFS datastores. If you store replicas on VMFS datastores, a cluster can have at most eight hosts. See “Configuring Pools on Clusters With More Than Eight Hosts,” on page 147.</td>
<td></td>
</tr>
<tr>
<td>Resource pool</td>
<td>Select the vCenter Server resource pool in which the desktop pool resides.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Datastores</td>
<td>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 106. You can use shared or local datastores for an individual ESXi host or for ESXi clusters. If you use local datastores in an ESXi cluster, you must consider the vSphere infrastructure constraints that are imposed on your desktop deployment. See “Storing Linked-Clone Desktops on Local Datastores,” on page 112. In vSphere 5.1 or later, a cluster can have more than eight ESXi hosts if the replicas are stored on datastores that are VMFS5 or later or NFS. In vSphere 5.0, a cluster can have more than eight ESXi hosts only if the replicas are stored on NFS datastores. See “Configuring Pools on Clusters With More Than Eight Hosts,” on page 147. For more information about the disks that are created for linked clones, see “Linked-Clone Desktop Data Disks,” on page 119.</td>
<td></td>
</tr>
<tr>
<td>Storage Overcommit</td>
<td>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 110.</td>
<td></td>
</tr>
<tr>
<td>Use View Storage Accelerator</td>
<td>Determine whether to use View Storage Accelerator, which allows ESXi hosts to cache common virtual machine disk data. View Storage Accelerator can improve performance and reduce the need for extra storage I/O bandwidth to manage boot storms and anti-virus scanning I/O storms. This feature is supported on vSphere 5.0 and later. This feature is enabled by default. For details, see “Configure View Storage Accelerator for Desktop Pools,” on page 145.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
</table>
| Use native NFS snapshots (VAAI) - Tech Preview | If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can use native snapshot technology to clone virtual machines.  
**Note**: Native NFS snapshot technology (VAAI) is a Tech Preview feature. The feature is available for you to try out, but it is not recommended for production use and no support is provided.  
You can use this feature only if you select datastores that reside on NAS devices that support native cloning operations through VAAI.  
You cannot use this feature if you store replicas and OS disks on separate datastores. You cannot use this feature in a pool that is enabled for View Storage Accelerator or virtual machine disk space reclamation.  
This feature is supported on vSphere 5.0 and later.  
For details, see “Using View Composer Array Integration with Native NFS Snapshot Technology (VAAI),” on page 114. |                                                                        |
| Reclaim VM disk space                      | Determine whether to allow ESXi hosts to reclaim unused disk space on linked clones that are created in space-efficient disk format. The space reclamation feature reduces the total storage space required for linked-clone desktops.  
This feature is supported on vSphere 5.1 and later.  
The linked-clone virtual machines must be virtual hardware version 9 or later.  
For details, see “Reclaim Disk Space on Linked-Clone Desktops,” on page 115. |                                                                        |
| Initiate reclamation when unused space on VM exceeds: | Type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk to trigger space reclamation. When the unused disk space exceeds this threshold, View initiates the operation that directs the ESXi host to reclaim space on the OS disk.  
This value is measured per virtual machine. The unused disk space must exceed the specified threshold on an individual virtual machine before View starts the space reclamation process on that machine.  
For example: 2 GB.  
The default value is 1 GB. |                                                                        |
| Blackout Times                             | Configure days and times during which View Storage Accelerator regeneration and the reclamation of virtual machine disk space do not take place.  
To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.  
For details, see “Set Blackout Times for ESXi Operations on View Desktops,” on page 116. |                                                                        |
### Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory domain</strong></td>
<td>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 15. You specify this user when you configure View Composer settings for vCenter Server. For details, see “Configure View Composer Settings,” on page 17. 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Active Directory container</strong></td>
<td>Provide the Active Directory container relative distinguished name. For example: <strong>CN=Computers</strong> When you run the Add Pool wizard, you can browse your Active Directory tree for the container.</td>
<td></td>
</tr>
<tr>
<td><strong>Use QuickPrep or a customization specification (Sysprep)</strong></td>
<td>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. 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 103.</td>
<td></td>
</tr>
<tr>
<td><strong>Power-off script</strong></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-3. Worksheet: Configuration Options for Creating a Linked-Clone Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Fill In Your Value Here</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post synchronization script</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
| Allow reuse of pre-existing computer accounts | Select this option to use existing computer accounts in Active Directory for linked clones that are provisioned by View Composer. This option lets you control the computer accounts that are created in Active Directory.  
When a linked clone is provisioned, if an existing AD computer account name matches the linked clone desktop name, View Composer uses the existing computer account. Otherwise, a new computer account is created.  
The existing computer accounts must be located in the Active Directory container that you specify with the Active Directory container setting.  
When this option is disabled, a new AD computer account is created when View Composer provisions a linked clone. This option is disabled by default.  
For details, see “Use Existing Active Directory Computer Accounts for Linked Clones,” on page 117. |                         |

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 88.

Prerequisites

- Verify that the View Composer service is installed, either on the same host as vCenter Server or on a separate host, and that a View Composer database is configured. See the VMware Horizon View Installation document.
- Verify that View Composer settings for vCenter Server are configured in View Administrator. See “Configure View Composer Settings,” on page 17.
- 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 59.
- 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 92.

Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See “Desktop and Pool Settings,” on page 132.

If you intend to provide access to your desktops through Horizon Workspace, verify that you create the desktop pools as a user with Administrators permissions on the root folder in View. If you give the user Administrators permissions on a folder other than the root folder, Horizon Workspace will not recognize the SAML Authenticator you configure in View, and you cannot configure the pool in Horizon Workspace.

**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. Parent VM
     b. Snapshot
     c. VM folder location
     d. Host or cluster
     e. Resource pool
     f. 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. If a linked clone is in an error state, the View automatic recovery mechanism attempts to power on, or shut down and restart, the linked clone. If repeated recovery attempts fail, the linked clone is deleted.

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 149.

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 132.

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

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 103.

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 106.

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

<table>
<thead>
<tr>
<th>Support for SIDs or GUIDs</th>
<th>Clone Creation</th>
<th>Refresh</th>
<th>Recompose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sysprep: Unique SIDs for linked clones</td>
<td>With Sysprep customization, unique SIDs are generated for linked clones.</td>
<td>Unique SIDs are preserved.</td>
<td>Unique SIDs are not preserved.</td>
</tr>
<tr>
<td>QuickPrep: Common SIDs for linked clones</td>
<td>With QuickPrep customization, a common SID is generated for all clones in a pool.</td>
<td>Common SID is preserved.</td>
<td>Common SID is preserved.</td>
</tr>
<tr>
<td>Third-party application GUIDs</td>
<td>Each application behaves differently.</td>
<td>The GUID is preserved if an application generates the GUID before the initial snapshot is taken.</td>
<td>Recompose operations do not preserve an application GUID unless the application writes the GUID on the drive specified as a View Composer persistent disk.</td>
</tr>
</tbody>
</table>

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 desktops on vSphere 4.0 software.
Comparing QuickPrep and Microsoft Sysprep

<table>
<thead>
<tr>
<th>QuickPrep</th>
<th>Customization Specification (Sysprep)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed to work with View Composer. For details, see “Customizing Linked-Clone Desktops with QuickPrep,” on page 104.</td>
<td>Can be created with the standard Microsoft Sysprep tools.</td>
</tr>
<tr>
<td>Uses the same local computer security identifier (SID) for all linked clones in the pool.</td>
<td>Generates a unique local computer SID for each linked clone in the pool.</td>
</tr>
<tr>
<td>Can run additional customization scripts before linked clones are powered off and after linked clones are created, refreshed, or recomposed.</td>
<td>Can run an additional script when the user first logs in.</td>
</tr>
<tr>
<td>Joins the linked clone computer to the Active Directory domain.</td>
<td>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.</td>
</tr>
<tr>
<td>For each linked clone, adds a unique ID to the Active Directory domain account.</td>
<td>For each linked clone, adds a unique ID to the Active Directory domain account.</td>
</tr>
<tr>
<td>Does not generate a new SID after linked clones are refreshed. The common SID is preserved.</td>
<td>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.</td>
</tr>
<tr>
<td>Does not generate a new SID after linked clones are recomposed. The common SID is preserved.</td>
<td>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 106.</td>
</tr>
<tr>
<td>Runs faster than Sysprep.</td>
<td>Can take longer than QuickPrep.</td>
</tr>
</tbody>
</table>

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 8, Windows 7, and Windows Vista linked-clone desktops. For details, see “Activating Windows on Linked-Clone Desktops,” on page 82.

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 105.

**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 15.

### 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
```

**IMPORTANT** Protect QuickPrep customization scripts from access by ordinary users. Place the scripts in a secure folder.

#### 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 84.

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 Process Privileges

For security reasons, certain Windows operating system privileges are removed from the View Composer Guest Agent process that invokes QuickPrep customization scripts.

A QuickPrep customization script cannot perform any action that requires a privilege that is removed from the View Composer Guest Agent process.

The following privileges are removed from the process that invokes QuickPrep scripts:
- SeCreateTokenPrivilege
- SeTakeOwnershipPrivilege
- SeSecurityPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeSystemtimePrivilege
- SeUndockPrivilege
- SeManageVolumePrivilege
- SeLockMemoryPrivilege
- SeIncreaseBasePriorityPrivilege
- SeCreatePermanentPrivilege
- SeDebugPrivilege
- SeAuditPrivilege

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 Horizon 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**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Selected Free Space (GB)</th>
<th>Min Recommended (GB)</th>
<th>50% Utilization (GB)</th>
<th>Max Recommended (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS disks</td>
<td>184.23</td>
<td>40.00</td>
<td>80.00</td>
<td>130.00</td>
</tr>
<tr>
<td>Persistent disks</td>
<td>28.56</td>
<td>4.00</td>
<td>10.00</td>
<td>20.00</td>
</tr>
</tbody>
</table>

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 109.

**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 110.
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 109.

Table 5-8. Storage Sizing Formulas for Linked-Clone Disks on Selected Datastores

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Selected Free Space (GB)</th>
<th>Min Recommended (GB)</th>
<th>50% Utilization (GB)</th>
<th>Max Recommended (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS disks</td>
<td>Free space on the selected datastores</td>
<td>Number of VMs * (2 * memory of VM) + (2 * replica disk)</td>
<td>Number of VMs * (50% of replica disk + memory of VM) + (2 * replica disk)</td>
<td>Number of VMs * (100% of replica disk + memory of VM) + (2 * replica disk)</td>
</tr>
<tr>
<td>Persistent disks</td>
<td>Free space on the selected datastores</td>
<td>Number of VMs * 20% of persistent disk</td>
<td>Number of VMs * 50% of persistent disk</td>
<td>Number of VMs * 100% of persistent disk</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Selected Free Space (GB)</th>
<th>Min Recommended (GB)</th>
<th>50% Utilization (GB)</th>
<th>Max Recommended (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS disks</td>
<td>184.23</td>
<td>10 * (2<em>1GB) + (2</em>10GB) = 40.00</td>
<td>10 * (50% of 10GB + 1GB) + (2*10GB) = 80.00</td>
<td>10 * (100% of 10GB + 1GB) + (2*10GB) = 130.00</td>
</tr>
<tr>
<td>Persistent disks</td>
<td>28.56</td>
<td>10 * (20% of 2GB) = 4.00</td>
<td>10 * (50% of 2GB) = 10.00</td>
<td>10 * (100% of 2GB) = 20.00</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Selected Free Space (GB)</th>
<th>Min Recommended (GB)</th>
<th>50% Utilization (GB)</th>
<th>Max Recommended (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS disks</td>
<td>Free space on the selected datastores</td>
<td>Number of VMs * (2 * memory of VM)</td>
<td>Number of VMs * (50% of replica disk + memory of VM)</td>
<td>Number of VMs * (100% of replica disk + memory of VM)</td>
</tr>
<tr>
<td>Persistent disks</td>
<td>Free space on the selected datastores</td>
<td>Number of VMs * 20% of persistent disk</td>
<td>Number of VMs * 50% of persistent disk</td>
<td>Number of VMs * 100% of persistent disk</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Selected Free Space (GB)</th>
<th>Min Recommended (GB)</th>
<th>50% Utilization (GB)</th>
<th>Max Recommended (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS disks</td>
<td>184.23</td>
<td>10 * (2*1GB) = 20.00</td>
<td>10 * (50% of 10GB + 1GB) = 60.00</td>
<td>10 * (100% of 10GB + 1GB) = 110.00</td>
</tr>
<tr>
<td>Persistent disks</td>
<td>28.56</td>
<td>10 * (20% of 2GB) = 4.00</td>
<td>10 * (50% of 2GB) = 10.00</td>
<td>10 * (100% of 2GB) = 20.00</td>
</tr>
</tbody>
</table>

**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 111.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>New desktop pool</td>
<td>a Click Add.</td>
</tr>
<tr>
<td></td>
<td>b Proceed through the Add Pool wizard until the Select Datastores page</td>
</tr>
<tr>
<td></td>
<td>is displayed.</td>
</tr>
<tr>
<td>Existing desktop pool</td>
<td>a Select the linked-clone pool and click Edit.</td>
</tr>
<tr>
<td></td>
<td>b Click the vCenter Settings tab.</td>
</tr>
</tbody>
</table>

3 On the Select Datastores page, select the storage overcommit level.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Storage is not overcommitted.</td>
</tr>
<tr>
<td>Conservative</td>
<td>4 times the size of the datastore. This is the default level.</td>
</tr>
<tr>
<td>Moderate</td>
<td>7 times the size of the datastore.</td>
</tr>
<tr>
<td>Aggressive</td>
<td>15 times the size of the datastore.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Storage Overcommit Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Storage is not overcommitted.</td>
</tr>
<tr>
<td>Conservative</td>
<td>4 times the size of the datastore. This is the default level.</td>
</tr>
<tr>
<td>Moderate</td>
<td>7 times the size of the datastore.</td>
</tr>
<tr>
<td>Aggressive</td>
<td>15 times the size of the datastore.</td>
</tr>
</tbody>
</table>

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 Linked-Clone Desktops on Local Datastores**

Linked-clone desktops can be stored on local datastores, which are internal spare disks on ESXi hosts. Local storage offers advantages such as inexpensive hardware, fast virtual-machine provisioning, high performance power operations, and simple management. However, using local storage limits the vSphere infrastructure configuration options that are available to you. Using local storage is beneficial in certain View environments but not appropriate in others.

Using local datastores is most likely to work well if the View desktops in your environment are stateless. For example, you might use local datastores if you deploy stateless kiosks or classroom and training stations.

Consider using local datastores if your desktops have floating assignments, are not dedicated to individual end users, do not require persistent disks for user data, and can be deleted or refreshed at regular intervals such as on user logoff. This approach lets you control the disk usage on each local datastore without having to move or load-balance the virtual machines across datastores.

However, you must consider the restrictions that using local datastores imposes on your View desktop deployment:

- You cannot use VMotion to manage volumes.
- You cannot load-balance virtual machines across a resource pool. For example, you cannot use the View Composer rebalance operation with linked-clones that are stored on local datastores.
- You cannot use VMware High Availability.
- You cannot use the vSphere Distributed Resource Scheduler (DRS).
- You cannot store a View Composer replica and linked clones on separate datastores if the replica is on a local datastore.

When you store linked clones on local datastores, VMware strongly recommends that you store the replica on the same volume as the linked clones. Although it is possible to store linked clones on local datastores and the replica on a shared datastore if all ESXi hosts in the cluster can access the replica, VMware does not recommend this configuration.

- If you select local spinning-disk drives, performance might not match that of a commercially available storage array. Local spinning-disk drives and a storage array might have similar capacity, but local spinning-disk drives do not have the same throughput as a storage array. Throughput increases as the number of spindles grows.

If you select direct attached solid-state disks (SSDs), performance is likely to exceed that of many storage arrays.

You can store linked clones on a local datastore without constraints if you configure the desktop pool on a single ESXi host or a cluster that contains a single ESXi host. However, using a single ESXi host limits the size of the desktop pool that you can configure.

To configure a large desktop pool, you must select a cluster that contains multiple ESXi hosts with the collective capacity to support a large number of virtual machines.

If you intend to take advantage of the benefits of local storage, you must carefully consider the consequences of not having VMotion, HA, DRS, and other features available. If you manage local disk usage by controlling the number and disk growth of the virtual machines, if you use floating assignments and perform regular refresh and delete operations, you can successfully deploy linked clones to local datastores.
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 ESXi cluster, so replicas do not require much storage space. A solid-state disk can improve the speed at which ESXi 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. ESXi 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 ESXi hosts in the cluster.
- If the linked-clone datastores are shared, the replica datastore must be shared. The replica cannot reside on a local datastore.
  
  If the linked-clone datastores are local, VMware strongly recommends that you store the replica on the same volume as the linked clones. Although it is possible to store linked clones on local datastores and the replica on a shared datastore if all ESXi hosts in the cluster can access the replica, VMware does not recommend this configuration.

**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.
Using View Composer Array Integration with Native NFS Snapshot Technology (VAAI)

If your deployment includes NAS devices that support the vStorage APIs for Array Integration (VAAI), you can enable the View Composer Array Integration feature on linked-clone pools. This feature uses native NFS snapshot technology to clone virtual machines.

**Note** Native NFS snapshot technology (VAAI) is a Tech Preview feature. The feature is available for you to try out, but it is not recommended for production use and no support is provided.

With this technology, the NFS disk array clones the virtual machine files without having the ESXi host read and write the data. This operation might reduce the time and network load when virtual machines are cloned.

Apply these guidelines for using native NFS snapshot technology:

- You can use this feature only if you configure desktop pools on datastores that reside on NAS devices that support native cloning operations through VAAI.
- You can use View Composer features to manage linked clones that are created by native NFS snapshot technology. For example, you can refresh, recompose, rebalance, create persistent disks, and run QuickPrep customization scripts on these clones.
- You cannot use this feature if you store replicas and OS disks on separate datastores.
- This feature is supported on vSphere 5.0 and later.
- You can use NAS device-cloned virtual machines in local mode. However, when users check out their desktops, the View Composer base image in the Transfer Server repository is not used in the checkout operation. Instead, View Transfer Server mounts and downloads the whole virtual machine to the client computer.

After a user checks in a desktop, native NFS cloning is not used again for that desktop. View manages the desktop as a full virtual machine. This constraint applies only to desktops that were used in local mode. Remote desktops in the pool continue to benefit from native NFS cloning.

- If you edit a pool and select or deselect the native NFS cloning feature, existing virtual machines are not affected.

To change existing virtual machines from native NFS clones to traditional redo log clones, you must deselect the native NFS cloning feature and recompose the pool to a new base image. To change the cloning method for all virtual machines in a pool and use a different datastore, you must select the new datastore, deselect the native NFS cloning feature, rebalance the pool to the new datastore, and recompose the pool to a new base image.

Similarly, to change virtual machines from traditional redo log clones to native NFS clones, you must select a NAS datastore that supports VAAI, select the native NFS cloning feature, rebalance the pool to the NAS datastore, and recompose the pool.

- On an ESXi cluster, to configure native cloning on a selected NFS datastore in View Administrator, you might have to install vendor-specific NAS plug-ins that support native cloning operations on VAAI on all ESXi hosts in the cluster. See your storage vendor documentation for guidance on configuration requirements.
- Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator or virtual machine disk space reclamation.

**Important** NAS storage vendors might provide additional settings that can affect the performance and operation of VAAI. You should follow the vendor’s recommendations and configure the appropriate settings on both the NAS storage array and ESXi. See your storage vendor documentation for guidance on configuring vendor-recommended settings.
Reclaim Disk Space on Linked-Clone Desktops

In vSphere 5.1 and later, you can configure the disk space reclamation feature for linked-clone desktop pools. Starting in vSphere 5.1, View creates linked-clone virtual machines in an efficient disk format that allows ESXi hosts to reclaim unused disk space on the linked clones, reducing the total storage space required for linked clones.

As users interact with linked-clone desktops, the clones' OS disks grow and can eventually use almost as much disk space as full-clone desktops. Disk space reclamation reduces the size of the OS disks without requiring you to refresh or recompose the linked clones. Space can be reclaimed while the virtual machines are powered on and users are interacting with their desktops.

In View Administrator, you cannot directly initiate disk space reclamation for a pool. You determine when View initiates disk space reclamation by specifying the minimum amount of unused disk space that must accumulate on a linked-clone OS disk to trigger the operation. When the unused disk space exceeds the specified threshold, View directs the ESXi host to reclaim space on that OS disk. View applies the threshold to each virtual machine in the pool.

You can use the `vdmadmin -M` option to initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes. See “Reclaiming Disk Space on Virtual Machines Using the -M Option,” on page 420.

You can configure disk space reclamation on linked clones when you create a new pool or edit an existing pool. For an existing pool, see “Upgrade Desktop Pools for Space Reclamation” in the VMware Horizon View Upgrades document.

If a View Composer is refreshing, recomposing, or rebalancing linked clones, disk space reclamation does not take place on those linked clones.

Disk space reclamation operates only on OS disks in linked clones. The feature does not affect View Composer persistent disks and does not operate on full-clone virtual machines.

Native NFS snapshot technology (VAAI) is not supported in pools that contain virtual machines with space-efficient disks.

**Prerequisites**

- Verify that your vCenter Server and ESXi hosts are version 5.1 with ESXi 5.1 download patch ESXi510-201212001 or later.
  - In an ESXi cluster, verify that all the hosts are version 5.1 with download patch ESXi510-201212001 or later.
- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on all the linked-clone virtual machines in the pool.
- Verify that all the linked-clone virtual machines in the pool are virtual hardware version 9 or later.
- Verify that the virtual machines use SCSI controllers. Disk space reclamation is not supported on virtual machines with IDE controllers.
- Verify that the linked-clone desktops run Windows XP or Windows 7. Disk space reclamation is not supported on Windows 8 desktops.
- Verify that disk space reclamation is enabled in vCenter Server. This option ensures that the virtual machines in the pool are created in the efficient disk format that is required to reclaim disk space. See “Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines,” on page 19.
Procedure

1. In View Administrator, display the Advanced Storage Options page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New desktop pool</td>
<td>Start the Add Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the Advanced Storage Options page.</td>
</tr>
<tr>
<td>Existing desktop pool</td>
<td>Select the existing pool, click Edit, and click the Advanced Storage Options tab. To upgrade a pool to support space reclamation, see “Upgrade Desktop Pools for Space Reclamation” in the VMware Horizon View Upgrades document.</td>
</tr>
</tbody>
</table>

2. Select the Reclaim VM disk space check box.

3. In the Initiate reclamation when unused space exceeds text box, type the minimum amount of unused disk space, in gigabytes, that must accumulate on a linked-clone OS disk before ESXi starts reclaiming space on that disk.

   For example: 2 GB.

   The default value is 1 GB.

What to do next

You can configure blackout days and times during which disk space reclamation and regeneration for View Storage Accelerator do not take place. See “Set Blackout Times for ESXi Operations on View Desktops,” on page 116.

In View Administrator, you can click Inventory > Desktops and select a desktop to display the last time space reclamation occurred and the last amount of space reclaimed on the desktop.

Set Blackout Times for ESXi Operations on View Desktops

Regenerating digest files for View Storage Accelerator and reclaiming virtual machine disk space can use ESXi resources. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.

For example, you can specify a blackout period during weekday morning hours when users start work, and boot storms and anti-virus scanning I/O storms take place. You can specify different blackout times on different days.

Disk space reclamation and View Storage Accelerator digest file regeneration do not occur during blackout times that you set. You cannot set separate blackout times for each operation.

View allows View Storage Accelerator digest files to be created for new desktops during the provisioning stage, even when a blackout time is in effect.

Prerequisites

- Verify that Enable View Storage Accelerator, Enable space reclamation, or both features are selected for vCenter Server.
- Verify that Use View Storage Accelerator, Reclaim VM disk space, or both features are selected for the desktop pool.

Procedure

1. On the Advanced Storage Options page in the Add Pool wizard, go to Blackout Times and click Add.

   If you are editing an existing pool, click the Advanced Storage Options tab.
2. Check the blackout days and specify the starting and ending times. The time selector uses a 24-hour clock. For example, 10:00 is 10:00 a.m., and 22:00 is 10:00 p.m.

3. Click OK.

4. To add another blackout period, click Add and specify another period.

5. To modify or remove a blackout period, select the period from the Blackout times list and click Edit or Remove.

**Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations**

If your users must be able to access View desktops at all times, you must maintain a certain number of desktops that stay provisioned and ready to accept connection requests from your users even when View Composer maintenance operations take place. You can set a minimum number of provisioned, ready desktops while View Composer refreshes, recomposes, or rebalances the linked-clone virtual machines in a pool.

When you specify a **Minimum number of ready (provisioned) desktops during View Composer maintenance operations**, View Manager ensures that the specified number of desktops stays provisioned and ready while View Composer proceeds through the operation. You can specify the minimum number of ready desktops when you create or edit a linked-clone pool.

The following guidelines apply to this setting:

- If you use a naming pattern to provision desktops and provision desktops on demand, set the number of ready desktops during View Composer operations to a smaller value than the specified **Min number of desktops**. If the minimum number were smaller, your pool could end up with fewer total desktops than the minimum number you want to keep provisioned and ready during View Composer operations. In this case, View Composer maintenance operations could not take place.

- If you provision desktops by manually specifying a list of desktop names, do not reduce the total pool size (by removing desktop names) to a lower number than the minimum number of ready desktops. In this case, View Composer maintenance operations could not take place.

- If you set a large minimum number of ready desktops in relation to the pool size, View Composer maintenance operations might take longer to complete. While View Manager maintains the minimum number of ready desktops during a maintenance operation, the operation might not reach the concurrency limit that is specified in the **Max concurrent View Composer maintenance operations** setting.

For example, if a pool contains 20 desktops and the minimum number of ready desktops is 15, View Composer can operate on at most five desktops at a time. If the concurrency limit for View Composer maintenance operations is 12, the concurrency limit is never reached.

- The term “ready” applies to the state of the linked-clone virtual machine, not the desktop status that is displayed in View Administrator. A virtual machine is ready when it is provisioned and ready to be powered on. The desktop status reflects the View-managed condition of the desktop. For example, a desktop can have a status of Connected, Disconnected, Agent Unreachable, Deleting, and so on.

**Use Existing Active Directory Computer Accounts for Linked Clones**

When you create or edit a desktop pool, you can configure View Composer to use existing computer accounts in Active Directory for newly provisioned linked clones.

By default, View Composer generates a new Active Directory computer account for each linked clone that it provisions. The **Allow reuse of pre-existing computer accounts** option lets you control the computer accounts that are created in Active Directory by ensuring that View Composer uses existing AD computer accounts.
With this option enabled, when a linked clone is provisioned, View Composer checks if an existing AD computer account name matches the linked clone desktop name. If a match exists, View Composer uses the existing AD computer account. If View Composer does not find a matching AD computer account name, View Composer generates a new AD computer account for the linked clone.

You can set the **Allow reuse of pre-existing computer accounts** option when you create a new desktop pool or edit an existing pool. If you edit a pool and set this option, the setting affects linked-clone desktops that are provisioned in the future. Linked clones that are already provisioned are not affected.

When you set the **Allow reuse of pre-existing computer accounts** option, you can limit the Active Directory permissions assigned to the View Composer user account that generates the desktop pool. Only the following Active Directory permissions are required:

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

You can only limit the Active Directory permissions if you are sure that all desktops you intend to provision have existing computer accounts allocated in Active Directory. View Composer generates a new AD computer account if no matching name is found. Additional permissions such as Create Computer Objects are required to create new computer accounts. For a complete list of permissions required for the View Composer user account, see “Create a User Account for View Composer,” on page 15.

This option cannot be disabled if View Composer is currently using at least one existing AD computer account.

**Prerequisites**

Verify that the existing computer accounts are located in the Active Directory container that you specify with the **Active Directory container** setting. If the existing accounts are located in a different container, provisioning fails for linked clones with those account names, and an error message states that the existing computer accounts already exist in Active Directory.

For example, if you select the **Allow reuse of pre-existing computer accounts** option and specify that the **Active Directory container** is the default value, **CN=Computers**, and the existing computer accounts are located in **OU=mydesktops**, provisioning fails for those accounts.

**Procedure**

1. In Active Directory, create the computer accounts to use for the linked-clone desktops.
   
   For example: `desktop1`, `desktop2`, `desktop3`

   The computer account names must use consecutive integers so that they match the View desktop names that are generated during desktop provisioning.

2. In View Administrator, create a pool with the Add Pool wizard or edit the pool in the Edit Pool dialog.

3. On the Provisioning Settings page or tab, select **Use a naming pattern**.

4. In the Naming pattern text box, type a desktop name that matches the Active Directory computer account name.

   For example: `desktop`

   View appends unique numbers to the pattern to provide a unique name for each desktop.

   For example: `desktop1`, `desktop2`, `desktop3`

5. On the Guest Customization page or tab, select the **Allow reuse of pre-existing computer accounts** option.
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. You select a separate desktop source for each desktop in the pool.

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 126.     |
| 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    |
|                  |     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 132.            |
|                  | For a list of the settings that apply to manual pools, see            |
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 on 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 59.
  - To prepare unmanaged virtual machines, physical computers, and Blade PCs, see Chapter 3, “Preparing Unmanaged Desktop Sources,” on page 55.
- Gather the configuration information that you must provide to create the pool. See “Worksheet for Creating a Manual Desktop Pool,” on page 120.
- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See “Desktop and Pool Settings,” on page 132.

Procedure

1. In View Administrator, click Inventory > Pools.
2. Click Add.
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 149.

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 59.

  To prepare an unmanaged virtual machine, physical computer, or Blade PC, see Chapter 3, “Preparing Unmanaged Desktop Sources,” on page 55.

- Gather the configuration information you must provide to create the manual pool. See “Worksheet for Creating a Manual Desktop Pool,” on page 120.

- Decide how to configure power settings, display protocol, Adobe Flash quality, and other settings. See “Desktop and Pool Settings,” on page 132.

Procedure

1. In View Administrator, click **Inventory > Pools**.
2. Click **Add**.
3. Select **Manual Pool**.
4. Select the type of user assignment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated Assignment</td>
<td>The desktop is assigned to one user. Only that user can log in to the desktop.</td>
</tr>
<tr>
<td>Floating Assignment</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 149.

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 132.
### Table 5-14. Settings for Manual Desktop Pools

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Connection Server restrictions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote desktop power policy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic logoff after disconnect</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow users to reset their desktop</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow multiple sessions per user</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Default display protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Allow users to choose protocol</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3D Renderer</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max number of monitors</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max resolution of any one monitor</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adobe Flash quality</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Adobe Flash throttling</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

To use PCoIP with a desktop source that is not managed by vCenter Server, you must install Teradici hardware on the desktop source.

**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 pool 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 55.
- 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 124. For descriptions of each desktop setting, see “Desktop and Pool Settings,” on page 132.
- 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 Terminal Services 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 149.

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 132.

<table>
<thead>
<tr>
<th>Table 5-15. Settings for Terminal Services Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Setting</strong></td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Connection Server restrictions</td>
</tr>
<tr>
<td>Automatic logoff after disconnect</td>
</tr>
<tr>
<td>Default display protocol</td>
</tr>
</tbody>
</table>
**Table 5-15. Settings for Terminal Services Pools (Continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Microsoft Terminal Services Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Flash quality</td>
<td>Yes</td>
</tr>
<tr>
<td>Adobe Flash throttling</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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 126
  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 126
  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 131
  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 132
  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 or Later Desktops** on page 136
  When you create or edit a Windows 7 or later desktop pool, you can configure 3D graphics rendering for your desktops. Desktops can take advantage of Virtual Shared Graphics Acceleration (vSGA), a vSphere feature that uses physical graphics cards installed on the ESXi hosts and manages the graphics processing unit (GPU) resources amongst the desktops.

- **Prevent Access to View Desktops Through RDP** on page 139
  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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Providing a Desktop-Naming Pattern</th>
<th>Naming Desktops Manually</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop names</td>
<td>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 129.</td>
<td>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 128.</td>
</tr>
<tr>
<td>Pool size</td>
<td>You specify a maximum number of desktops.</td>
<td>Your list of desktop names determines the number of desktops.</td>
</tr>
<tr>
<td>To add desktops to the pool</td>
<td>You can increase the maximum pool size.</td>
<td>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 268.</td>
</tr>
</tbody>
</table>
Table 5-16. Naming Desktops Manually or Providing a Desktop-Naming Pattern (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Providing a Desktop-Naming Pattern</th>
<th>Naming Desktops Manually</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-demand provisioning</td>
<td>Available. View Manager dynamically creates and provisions the specified minimum and spare number of desktops as users first log in or as you assign desktops to users. View Manager can also create and provision all the desktops when you create the pool.</td>
<td>Not available. View Manager creates and provisions all the desktops that you specify in your list when the pool is created.</td>
</tr>
<tr>
<td>Initial customization</td>
<td>Available. When a desktop is provisioned, View Manager can run a customization specification that you select.</td>
<td>Available. When a desktop is provisioned, View Manager can run a customization specification that you select.</td>
</tr>
<tr>
<td>Manual customization of dedicated desktops</td>
<td>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.</td>
<td>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 131.</td>
</tr>
<tr>
<td>Dynamic or fixed pool size</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Spare desktops</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>User assignment</td>
<td>You can use a naming pattern for dedicated-assignment and floating-assignment pools.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 !.

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>
<thead>
<tr>
<th>If You Set This Number of Desktops in the Pool</th>
<th>This Is the Maximum Prefix Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-99</td>
<td>13 characters</td>
</tr>
<tr>
<td>100-999</td>
<td>12 characters</td>
</tr>
<tr>
<td>1,000 or more</td>
<td>11 characters</td>
</tr>
</tbody>
</table>

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 129.

**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>
<thead>
<tr>
<th>Fixed-Length Token</th>
<th>Maximum Length of the Naming Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{n:fixed=1}</code></td>
<td>14 characters</td>
</tr>
<tr>
<td><code>{n:fixed=2}</code></td>
<td>13 characters</td>
</tr>
<tr>
<td><code>{n:fixed=3}</code></td>
<td>12 characters</td>
</tr>
</tbody>
</table>
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 128.

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 129.

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 131
  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 131
  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 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
</table>
| 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.  
When this state is in effect, remote desktops are unavailable for use. In addition, active local desktop sessions are suspended and local desktops are unavailable. |
| 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.  
If you intend to provide access to your desktops through Horizon Workspace, and you configure View Connection Server restrictions, the Horizon User Portal might display desktops to users when those desktops are actually restricted. Horizon users will be unable to launch these desktops. |
| 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 140.  
For more information about how power policies affect automated pools, see “Setting Power Policies for Desktop Pools,” on page 140. |
| 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. |
<table>
<thead>
<tr>
<th><strong>Setting</strong></th>
<th><strong>Options</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to reset their desktops</td>
<td>Allow users to reset their own desktops without administrative assistance.</td>
</tr>
<tr>
<td>Allow multiple sessions per user</td>
<td>Allow a user to connect to multiple desktops in the pool at the same time.</td>
</tr>
<tr>
<td>Delete desktop after logoff</td>
<td>Select whether to delete floating-assignment, full virtual machine desktops.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>No.</strong> Virtual machines remain in the desktop pool after users log off.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Yes.</strong> Virtual machines are powered off and deleted as soon as users log off.</td>
</tr>
<tr>
<td>Delete or refresh desktop on logoff</td>
<td>Select whether to delete, refresh, or leave alone floating-assignment, linked-clone desktops.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Never.</strong> Virtual machines remain in the pool and are not refreshed after users log off.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Delete immediately.</strong> 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 <strong>Deleting</strong> state.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Refresh immediately.</strong> 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.</td>
</tr>
<tr>
<td>Refresh OS disk after logoff</td>
<td>Select whether and when to refresh the OS disks for dedicated-assignment, linked-clone desktops.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Never.</strong> The OS disk is never refreshed.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Always.</strong> The OS disk is refreshed every time the user logs off.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>Every.</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>▪ <strong>At.</strong> 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 <strong>At</strong> 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.</td>
</tr>
</tbody>
</table>
### Table 5-19. Desktop and Pool Setting Descriptions (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default display protocol</td>
<td>Select the display protocol that you want View Connection Server to use to communicate with View clients.</td>
</tr>
<tr>
<td></td>
<td><strong>PCoIP</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Microsoft RDP</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Allow users to choose protocol</td>
<td>Allow users to override the default display protocol for their desktops by using View Client.</td>
</tr>
<tr>
<td>3D Renderer</td>
<td>You can select whether to enable 3D graphics rendering if your pool comprises Windows 7 or later desktops. You can configure the 3D Renderer to use software rendering or hardware rendering based on physical GPU graphics cards installed on ESXi 5.1 or later hosts. To enable this feature, you must select PCoIP as the protocol and disable the Allow users to choose protocol setting (select No). With the hardware-based 3D Renderer options, users can take advantage of graphics applications for design, modelling, and multimedia. The desktops must run on vSphere 5.1 or later. Windows 7 desktops must be virtual hardware version 8 or later. Windows 8 desktops must be virtual hardware version 9 or later. With the software 3D Renderer option, users can take advantage of graphics enhancements in less demanding applications such as AERO, Microsoft Office 2010, and Google Earth. The desktops must run on vSphere 5.0 or later and be virtual hardware version 8 or later. 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. <strong>Note</strong> 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 or Later Desktops,” on page 136, “3D Rendering Options,” on page 137, and “Best Practices for Configuring 3D Rendering,” on page 138.</td>
</tr>
</tbody>
</table>
Table 5-19. Desktop and Pool Setting Descriptions (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max number of monitors</td>
<td>If you use PCoIP as the display protocol, you can select the <strong>Maximum number of monitors</strong> on which users can display the desktop.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>3D Renderer</strong> 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 ESXi hosts.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>3D Renderer</strong> setting is selected, you can select at most two monitors.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>Max resolution of any one monitor</td>
<td>If you use PCoIP as the display protocol and you do not select the <strong>3D Renderer</strong> setting, you should specify the <strong>Maximum resolution of any one monitor</strong>.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>3D Renderer</strong> 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 ESXi hosts.</td>
</tr>
<tr>
<td></td>
<td>When the <strong>3D Renderer</strong> setting is selected, you cannot change the <strong>Maximum resolution of any one monitor</strong>. The resolution is set to 1920x1200 pixels.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>HTML Access</td>
<td>Determines whether to allow users to connect to View desktops by using HTML from their Web browsers. Select <strong>Enabled</strong> to allow Horizon users to connect to View desktops in this pool over HTML.</td>
</tr>
<tr>
<td></td>
<td>When a user logs in to the View Portal or Horizon User Portal and selects a View desktop, the Blast Agent enables the user to connect to the desktop over HTTPS. The desktop is displayed in the user's browser. Other display protocols, such as PCoIP or RDP, are not used. View Client software does not have to be installed on the client devices.</td>
</tr>
<tr>
<td></td>
<td>To use HTML access, you must install the HTML Desktop Access feature pack in your View deployment. The Blast Agent must be installed on the View desktops in the pool.</td>
</tr>
<tr>
<td></td>
<td>To use HTML Access with Horizon Workspace, you must pair View Connection Server with a SAML 2.0 Authentication server. Horizon Workspace must be installed and configured for use with View Connection Server.</td>
</tr>
</tbody>
</table>
### Table 5-19. Desktop and Pool Setting Descriptions (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adobe Flash quality</strong></td>
<td>Determines the quality of Adobe Flash content that is displayed on Web pages.</td>
</tr>
<tr>
<td></td>
<td>- Do not control. Quality is determined by Web page settings.</td>
</tr>
<tr>
<td></td>
<td>- Low. This setting results in the most bandwidth savings. If no quality level is specified, the system defaults to Low.</td>
</tr>
<tr>
<td></td>
<td>- Medium. This setting results in moderate bandwidth savings.</td>
</tr>
<tr>
<td></td>
<td>- High. This setting results in the least bandwidth savings.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Adobe Flash Quality and Throttling,” on page 271.</td>
</tr>
<tr>
<td><strong>Adobe Flash throttling</strong></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- Disabled. No throttling is performed. The timer interval is not modified.</td>
</tr>
<tr>
<td></td>
<td>- Conservative. Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.</td>
</tr>
<tr>
<td></td>
<td>- Moderate. Timer interval is 500 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>- Aggressive. Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Adobe Flash Quality and Throttling,” on page 271.</td>
</tr>
</tbody>
</table>

**NOTE** Properties set for local desktops do not take effect until the desktops are checked back in.

### Configuring 3D Rendering on Windows 7 or Later Desktops

When you create or edit a Windows 7 or later desktop pool, you can configure 3D graphics rendering for your desktops. Desktops can take advantage of Virtual Shared Graphics Acceleration (vSGA), a vSphere feature that uses physical graphics cards installed on the ESXi hosts and manages the graphics processing unit (GPU) resources amongst the desktops.

When you select the **3D Renderer** hardware-based options, users can take advantage of 3D applications for design, modeling, and multimedia, which typically require GPU hardware to perform well. The **3D Renderer** setting also offers a software option, which provides graphics enhancements that can support less demanding applications such as Windows AERO, Microsoft Office 2010, and Google Earth.

### Requirements for 3D Rendering

To enable hardware or software 3D graphics rendering, your pool deployment must meet the following requirements:

- The desktops must be Windows 7 or later
- The pool must use the PCoIP as the default display protocol
- Users must not be allowed to choose their own protocol

To support hardware-based 3D rendering, a pool must meet these additional requirements:

- The desktops must run on ESXi 5.1 or later hosts and be managed by vCenter Server 5.1 or later software
GPU graphics cards and the associated vSphere Installation Bundles (VIBs) must be installed on the ESXi hosts. For a list of supported GPU hardware, see the VMware Hardware Compatibility List at http://www.vmware.com/resources/compatibility/search.php.

Windows 7 desktops must be virtual hardware version 8 or later. Windows 8 desktops must be virtual hardware version 9 or later.

To support software 3D rendering, a pool must meet these additional 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 virtual hardware version 8 or later

You must power off and on existing virtual machines for the 3D Renderer setting to take effect. Restarting a virtual machine does not cause the setting to take effect.

### Configuring 3D Rendering

You select options to determine the way View manages 3D rendering. For details, see “3D Rendering Options,” on page 137.

When you enable the 3D Renderer 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 minimum VRAM size is 64MB. For virtual hardware version 9 virtual machines, the default VRAM size is 96MB, and you can configure a maximum size of 512MB. For virtual hardware version 8 virtual machines, the default VRAM size is 64MB, and you can configure a maximum size 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 or vSphere Web Client, unless you select the Manage using vSphere Client option.

When you enable the 3D Renderer 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.

### 3D Rendering Options

The 3D Renderer setting for desktop pools provides options that let you configure graphics rendering in different ways.

#### Table 5-20. 3D Renderer Options for Pools Running on vSphere 5.1 or Later

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Manage using vSphere Client     | The 3D Renderer option that is set in vSphere Web Client for a virtual machine determines the type of 3D graphics rendering that takes place. View does not control 3D rendering.  
In the vSphere Web Client, you can configure the Automatic, Software, or Hardware options. These options have the same effect as they do when you set them in View Administrator.  
When you select the Manage using vSphere Client option, the Configure VRAM for 3D Guests, Max number of monitors, and Max resolution of any one monitor settings are inactive in View Administrator. You can configure these settings for a virtual machine in the vSphere Web Client. |
| Automatic                       | 3D rendering is enabled. The ESXi host controls the type of 3D rendering that takes place. For example, the ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on. If all GPU hardware resources are already reserved when a virtual machine is powered on, ESXi uses the software renderer for that machine.  
When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see “Examining GPU Resources on an ESXi Host,” on page 139. |
| Software                        | 3D rendering is enabled. The ESXi host uses software 3D graphics rendering. If a GPU graphics card is installed on the ESXi host, this pool will not use it.  
In the Configure VRAM for 3D Guests dialog box, you can use the slider to increase the amount of VRAM that is reserved. |
Table 5-20. 3D Renderer Options for Pools Running on vSphere 5.1 or Later (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>3D rendering is enabled. The ESXi host reserves GPU hardware resources on a first-come, first-served basis as virtual machines are powered on.</td>
</tr>
<tr>
<td></td>
<td>The ESXi host allocates VRAM to a virtual machine based on the value that is set in the Configure VRAM for 3D Guests dialog box.</td>
</tr>
<tr>
<td>IMPORTANT</td>
<td>If you configure the Hardware option, consider these potential constraints:</td>
</tr>
<tr>
<td>n</td>
<td>If a user tries to connect to a desktop when all GPU hardware resources are reserved, the virtual machine will not power on, and the user will receive an error message.</td>
</tr>
<tr>
<td>n</td>
<td>A desktop cannot be moved by vMotion to an ESXi host that does not have GPU hardware configured.</td>
</tr>
<tr>
<td>n</td>
<td>All ESXi hosts in the cluster must be version 5.1 or later. If a desktop is created on an ESXi 5.0 host in a mixed cluster, the virtual machine will not power on.</td>
</tr>
</tbody>
</table>
|            | When you configure hardware-based 3D rendering, you can examine the GPU resources that are allocated to each virtual machine on an ESXi host. For details, see “Examining GPU Resources on an ESXi Host,” on page 139.
| Disabled   | 3D rendering is inactive.                                                                                                                   |

Table 5-21. 3D Renderer Options for Pools Running on vSphere 5.0

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>The 3D Renderer option is enabled. The ESXi host uses software 3D graphics rendering. When software rendering is configured, the default VRAM size is 64MB, the minimum size. In the Configure VRAM for 3D Guests dialog box, you can use the slider to increase the amount of VRAM that is reserved. With software rendering, the ESXi host allocates up to a maximum of 128MB per virtual machine. If you set a higher VRAM size, it is ignored.</td>
</tr>
<tr>
<td>Disabled</td>
<td>3D rendering is inactive.</td>
</tr>
</tbody>
</table>

If a desktop pool is running on earlier vSphere version than 5.0, the 3D Renderer setting is inactive and is not available in View Administrator.

Best Practices for Configuring 3D Rendering

The 3D rendering options and other pool settings offer various advantages and drawbacks. Select the option that best supports your vSphere hardware infrastructure and your users’ requirements for graphics rendering.

The Automatic option is the best choice for many View deployments that require 3D rendering. This option ensures that some type of 3D rendering takes place even when GPU resources are completely reserved. In a mixed cluster of ESXi 5.1 and ESXi 5.0 hosts, this option ensures that a virtual machine is powered on successfully and uses 3D rendering even if, for example, vMotion moved the virtual machine to an ESXi 5.0 host.

The only drawback with the Automatic option is that you cannot easily tell whether a virtual machine is using hardware or software 3D rendering.

The Hardware option guarantees that every virtual machine in the pool uses hardware 3D rendering, provided that GPU resources are available on the ESXi hosts. This option might be the best choice when all your users run graphically intensive applications.

With the Hardware option, you must strictly control your vSphere environment. All ESXi hosts must be version 5.1 or later and must have GPU graphics cards installed. When all GPU resources on an ESXi host are reserved, View cannot power on a virtual machine for the next user who tries to log in to a desktop. You must manage the allocation of GPU resources and the use of vMotion to ensure that resources are available for your desktops.

Select the Manage using vSphere Client option to support a mixed configuration of 3D rendering and VRAM sizes for virtual machines in a pool. In vSphere Web Client, you can configure individual virtual machines with different options and VRAM values.
Select the **Software** option if you have ESXi 5.0 hosts only, or the ESXi 5.1 hosts do not have GPU graphics cards, or your users only run applications, such as AERO and Microsoft Office, that do not require hardware graphics acceleration.

**Configuring Desktop Settings to Manage GPU Resources**

You can configure other desktop settings to ensure that GPU resources are not wasted when users are not actively using them.

For floating pools, set a session timeout so that GPU resources are freed up for other users when a user is not using the desktop.

For dedicated pools, you can configure the **Automatically logoff after disconnect** setting to **Immediately** and a **Suspend** power policy if these settings are appropriate for your users. For example, do not use these settings for a pool of researchers who execute long-running simulations.

**Examining GPU Resources on an ESXi Host**

To better manage the GPU resources that are available on an ESXi host, you can examine the current GPU resource reservation. The ESXi command-line query utility, `gpuvm`, lists the GPUs that are installed on an ESXi host and displays the amount of GPU memory that is reserved for each virtual machine on the host. Note that this GPU memory reservation is not the same as virtual machine VRAM size.

To run the utility, type `gpuvm` from a shell prompt on the ESXi host. You can use a console on the host or an SSH connection.

For example, the utility might display the following output:

```
# gpuvm
Xserver unix:0, GPU maximum memory 2076672KB
    pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
    pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
GPU memory left 1684480KB.
```

**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.

By default, while a user is logged in to a View desktop session, you can use RDP to connect to the desktop virtual machine from outside of View. The RDP connection terminates the View desktop session, and the View user's unsaved data and settings might be lost. The View user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the `AllowDirectRDP` 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 View Agent Configuration Administrative Template file is installed in Active Directory. See “Using the View Group Policy Administrative Template Files,” on page 180.
Procedure

1. Select PCoIP as the display protocol that you want View Connection Server to use to communicate with View clients.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 87 or “Managing Desktop Pools,” on page 265 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 5-22 describes the available power policies.
<table>
<thead>
<tr>
<th>Power Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Take no power action</td>
<td>View Manager does not enforce any power policy after a user logs off. This setting has two consequences.</td>
</tr>
<tr>
<td></td>
<td>■ View Manager does not change the power state of the virtual machine after a user logs off.</td>
</tr>
<tr>
<td></td>
<td>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. When a user reconnects to the desktop, the virtual machine restarts if it was powered off.</td>
</tr>
<tr>
<td></td>
<td>■ View Manager does not enforce any power state after an administrative task is completed.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Ensure desktops are always powered on</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Ensure desktops are always powered on</strong> if you run batch processes or system management tools that must contact the virtual machines at scheduled times.</td>
</tr>
<tr>
<td>Suspend</td>
<td>The virtual machine enters a suspended state when a user logs off, but not when a user disconnects.</td>
</tr>
<tr>
<td></td>
<td>You can also configure desktops in a dedicated pool to be suspended when a user disconnects without logging off. To configure this policy, you must set an attribute in View LDAP. See “Configure Dedicated Desktops To Be Suspended After Users Disconnect,” on page 142.</td>
</tr>
<tr>
<td></td>
<td>When multiple virtual machines are resumed from a suspended state, some virtual machines might have delays in powering on. Whether any delays occur depends on the ESXi host hardware and the number of virtual machines that are configured on an ESXi host. Users connecting to their desktops from View Client might temporarily see a desktop-not-available message. To access their desktops, users can connect again.</td>
</tr>
<tr>
<td>Power off</td>
<td>The virtual machine shuts down when a user logs off, but not when a user disconnects.</td>
</tr>
</tbody>
</table>

**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 5-23 describes when View Manager applies the configured power policy.
Table 5-23. When View Manager Applies the Power Policy

<table>
<thead>
<tr>
<th>Desktop Pool Type</th>
<th>The power policy is applied ...</th>
</tr>
</thead>
</table>
| 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 143 for more information.

**Configure Dedicated Desktops To Be Suspended After Users Disconnect**

The **Suspend** power policy causes virtual machines to be suspended when a user logs off, but not when a user disconnects. You can also configure desktops in a dedicated pool to be suspended when a user disconnects from a desktop without logging off. Using suspend when users disconnect helps to conserve resources.

To enable suspend on disconnect for dedicated desktops, you must set an attribute in View LDAP.

**Procedure**

1. Start the ADSI Edit utility on your View Connection Server host.
2. In the console tree, select **Connect to**.
3. In the **Select or type a domain or server** field, type the server name as **localhost:389**.
4. Under **Connection point**, click **Select or type a distinguished name or naming context**, type the distinguished name as **DC=vdi, DC=vmware, DC=int**, and click **OK**.
   
   The ADAM ADSI Edit main window appears.
5. Expand the ADAM ADSI tree and expand **OU=Properties**.
6 Select OU=Global and select CN=Common in the right pane
7 Select Action > Properties, and under the pae-NameValuePair attribute, add the new entry suspendOnDisconnect=1.
8 Restart View Connection Server.

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 5-24 describes the floating-assignment, automated pool in this example. The pool uses a desktop-naming pattern to provision and name the desktops.

<table>
<thead>
<tr>
<th>Desktop Pool Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of desktops (minimum)</td>
<td>10</td>
</tr>
<tr>
<td>Number of desktops (maximum)</td>
<td>20</td>
</tr>
<tr>
<td>Number of spare, powered-on desktops</td>
<td>2</td>
</tr>
<tr>
<td>Remote desktop power policy</td>
<td>Power off</td>
</tr>
</tbody>
</table>

When this desktop pool is provisioned, 10 desktops are created, two desktops are powered on and immediately available, and eight desktops are powered off.

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 powered off according to the power policy.

Power Policy Example 2

Table 5-25 describes the floating-assignment, automated pool in this example. The pool uses a desktop-naming pattern to provision and name the desktops.
Table 5-25. Desktop Pool Settings for Automated Pool with Floating Assignments Example 2

<table>
<thead>
<tr>
<th>Desktop Pool Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of desktops (minimum)</td>
<td>5</td>
</tr>
<tr>
<td>Number of desktops (maximum)</td>
<td>5</td>
</tr>
<tr>
<td>Number of spare, powered-on desktops</td>
<td>2</td>
</tr>
<tr>
<td>Remote desktop power policy</td>
<td>Power off</td>
</tr>
</tbody>
</table>

When this desktop pool is provisioned, five desktops are created, two desktops are powered on and immediately available, and three desktops are powered off.

If a fourth desktop in this pool is powered off, one of the existing desktops is powered on. 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 5-26 describes the dedicated-assignment, automated pool in this example.

Table 5-26. Desktop Pool Settings for Automated Pool with Dedicated Assignments Example

<table>
<thead>
<tr>
<th>Desktop Pool Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of desktops (minimum)</td>
<td>3</td>
</tr>
<tr>
<td>Number of desktops (maximum)</td>
<td>5</td>
</tr>
<tr>
<td>Number of spare, powered-on desktops</td>
<td>2</td>
</tr>
<tr>
<td>Remote desktop power policy</td>
<td>Ensure desktops are always powered on</td>
</tr>
</tbody>
</table>

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.

Configure View Storage Accelerator for Desktop Pools

You can configure desktop pools to enable ESXi hosts to cache virtual machine disk data. This feature, called View Storage Accelerator, uses the Content Based Read Cache (CBRC) feature in ESXi hosts. View Storage Accelerator can reduce IOPS and improve performance during boot storms, when many desktops start up or run anti-virus scans at once. The feature is also beneficial when administrators or users load applications or data frequently. To use this feature, you must make sure that View Storage Accelerator is enabled for individual desktop pools.

View Storage Accelerator is enabled for a pool by default. You can enable or disable View Storage Accelerator when you create or edit a pool.

You can enable View Storage Accelerator on pools that contain linked clones and pools that contain full virtual machines.

View Storage Accelerator is also supported with local mode. Users can check out desktops in pools that are enabled for View Storage Accelerator. The feature is disabled while a desktop is checked out and reenabled after the desktop is checked in.

Native NFS snapshot technology (VAAI) is not supported in pools that are enabled for View Storage Accelerator.

View Storage Accelerator is now qualified to work in configurations that use View replica tiering, in which replicas are stored on a separate datastore than linked clones. Although the performance benefits of using View Storage Accelerator with View replica tiering are not materially significant, certain capacity-related benefits might be realized by storing the replicas on a separate datastore. Hence, this combination is tested and supported.

When a virtual machine is created, View indexes the contents of each virtual disk file. The indexes are stored in a virtual machine digest file. At runtime, the ESXi host reads the digest files and caches common blocks of data in memory. To keep the ESXi host cache up to date, View regenerates the digest files at specified intervals and when the virtual machine is recomposed. You can modify the regeneration interval.

Prerequisites

- Verify that your vCenter Server and ESXi hosts are version 5.0 or later.
  - In an ESXi cluster, verify that all the hosts are version 5.0 or later.
- Verify that the vCenter Server user was assigned the **Global > Act as vCenter Server** privilege in vCenter Server. See the topics in the *VMware Horizon View Installation* documentation that describe View Manager and View Composer privileges required for the vCenter Server user.
- Verify that View Storage Accelerator is enabled in vCenter Server. See “Configure View Storage Accelerator for vCenter Server,” on page 20.
**Procedure**

1. In View Administrator, display the Advanced Storage Options page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New desktop pool</strong></td>
<td>Start the Add Pool wizard to begin creating an automated desktop pool. Follow the wizard configuration prompts until you reach the Advanced Storage Options page.</td>
</tr>
<tr>
<td><strong>Existing desktop pool</strong></td>
<td>Select the existing pool, click <strong>Edit</strong>, and click the <strong>Advanced Storage Options</strong> tab. In an existing pool, View Storage Accelerator digest files are not configured for virtual machines until they are powered off.</td>
</tr>
</tbody>
</table>

2. To enable View Storage Accelerator for the pool, make sure that the **Use View Storage Accelerator** check box is selected.

   This setting is selected by default. To disable the setting, uncheck the **Use View Storage Accelerator** box.

3. (Optional) Specify which disk types to cache by selecting **OS disks** only or **OS and persistent disks** from the menu.

   **OS disks** are selected by default.

   If you configure View Storage Accelerator for full virtual machines, you cannot select a disk type. View Storage Accelerator is performed on the whole virtual machine.

4. (Optional) In the **Regenerate storage accelerator after** text box, specify the interval, in days, after which the regeneration for View Storage Accelerator digest files take place.

   The default regeneration interval is seven days.

**What to do next**

You can configure blackout days and times during which disk space reclamation and View Storage Accelerator regeneration do not take place. See “Set Blackout Times for ESXi Operations on View Desktops,” on page 116.

**Set Blackout Times for ESXi Operations on View Desktops**

Regenerating digest files for View Storage Accelerator and reclaiming virtual machine disk space can use ESXi resources. To ensure that ESXi resources are dedicated to foreground tasks when necessary, you can prevent the ESXi hosts from performing these operations during specified periods of time on specified days.

For example, you can specify a blackout period during weekday morning hours when users start work, and boot storms and anti-virus scanning I/O storms take place. You can specify different blackout times on different days.

Disk space reclamation and View Storage Accelerator digest file regeneration do not occur during blackout times that you set. You cannot set separate blackout times for each operation.

View allows View Storage Accelerator digest files to be created for new desktops during the provisioning stage, even when a blackout time is in effect.

**Prerequisites**

- Verify that **Enable View Storage Accelerator, Enable space reclamation**, or both features are selected for vCenter Server.
- Verify that **Use View Storage Accelerator, Reclaim VM disk space**, or both features are selected for the desktop pool.
Procedure

1. On the Advanced Storage Options page in the Add Pool wizard, go to **Blackout Times** and click **Add**. If you are editing an existing pool, click the **Advanced Storage Options** tab.

2. Check the blackout days and specify the starting and ending times. The time selector uses a 24-hour clock. For example, 10:00 is 10:00 a.m., and 22:00 is 10:00 p.m.

3. Click **OK**.

4. To add another blackout period, click **Add** and specify another period.

5. To modify or remove a blackout period, select the period from the Blackout times list and click **Edit** or **Remove**.

**Deploying Large Desktop Pools**

When many users require the same desktop image, you can create one large automated pool from a single template or parent virtual machine. By using a single base image and pool name, you can avoid dividing the desktops arbitrarily into smaller groups that must be managed separately. This strategy simplifies your View deployment and administration tasks.

To support large pools, you can create pools on ESXi clusters that contain up to 32 ESXi hosts. You can also configure a pool to use multiple network labels, making the IP addresses of multiple port groups available for the desktop virtual machines.

**Configuring Pools on Clusters With More Than Eight Hosts**

In vSphere 5.1 and later, you can deploy a linked clone desktop pool on a cluster that contains up to 32 ESXi hosts. All ESXi hosts in the cluster must be version 5.1 or later. The hosts can use VMFS or NFS datastores. VMFS datastores must be VMFS5 or later.

In vSphere 5.0, you can deploy linked clones on a cluster that contains more than eight ESXi hosts, but you must store the replica disks on NFS datastores. You can store replica disks on VMFS datastores only with clusters that contain eight or fewer hosts.

In vSphere 5.0, the following rules apply when you configure a linked clone pool on a cluster that contains more than eight hosts:

- If you store replica disks on the same datastores as OS disks, you must store the replica and OS disks on NFS datastores.
- If you store replica disks on separate datastores than OS disks, the replica disks must be stored on NFS datastores. The OS disks can be stored on NFS or VMFS datastores.
- If you store View Composer persistent disks on separate datastores, the persistent disks can be configured on NFS or VMFS datastores.

In vSphere 4.1 and earlier releases, you can deploy desktop pools only with clusters that contain eight or fewer hosts.

**Assigning Multiple Network Labels to a Desktop Pool**

In View 5.2 and later releases, you can configure an automated pool to use multiple network labels. You can assign multiple network labels to a linked-clone pool or an automated pool that contains full virtual machines.

In past releases, virtual machines in the pool inherited the network labels that were used by the NICs on the parent virtual machine or template. A typical parent virtual machine or template contains one NIC and one network label. A network label defines a port group and VLAN. The netmask of one VLAN typically provides a limited range of available IP addresses.
In View 5.2 and later releases, you can assign network labels that are available in vCenter Server for all the ESXi hosts in the cluster where the desktop pool is deployed. By configuring multiple network labels for the pool, you greatly expand the number of IP addresses that can be assigned to the virtual machines in the pool.

You must use View PowerCLI cmdlets to assign multiple network labels to a pool. You cannot perform this task in View Administrator.

For details about using View PowerCLI to perform this task, see “Assign Multiple Network Labels to a Desktop Pool” in the chapter “Using View PowerCLI” in the VMware Horizon View Integration document.
Entitling Users and Groups

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,” on page 149
- “Remove Entitlements from a Desktop Pool,” on page 149
- “Review Desktop Pool Entitlements,” on page 150
- “Restricting View Desktop Access,” on page 150

Add Entitlements to Desktop Pools

Before users can access a View desktop, they must be entitled to use a desktop pool.

Prerequisites


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 150
  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 151
  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 152
  Before implementing restricted entitlements, you must be aware of certain considerations and limitations.

- **Assign a Tag to a View Connection Server Instance** on page 152
  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 153
  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>
<thead>
<tr>
<th>View Connection Server</th>
<th>Desktop Pool</th>
<th>Access Permitted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>No tags</td>
<td>No tags</td>
<td>Yes</td>
</tr>
<tr>
<td>No tags</td>
<td>One or more tags</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 6-1. Tag Matching Rules (Continued)

<table>
<thead>
<tr>
<th>View Connection Server</th>
<th>Desktop Pool</th>
<th>Access Permitted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more tags</td>
<td>No tags</td>
<td>Yes</td>
</tr>
<tr>
<td>One or more tags</td>
<td>One or more tags</td>
<td>Only when tags match</td>
</tr>
</tbody>
</table>

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.
- If you intend to provide access to your desktops through Horizon Workspace, and you configure View Connection Server restrictions, the Horizon User Portal might display desktops to users when those desktops are actually restricted. When a Horizon user attempts to log in to a desktop, it will not launch if the desktop pool’s tag does not match the tag assigned to the View Connection Server instance that the user is 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a tag to a new pool</td>
<td>Click Add to start the Add Pool wizard and define and identify the pool.</td>
</tr>
<tr>
<td>Assign a tag to an existing pool</td>
<td>Select the pool and click Edit.</td>
</tr>
</tbody>
</table>

3. Go to the Pool Settings page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool settings for a new pool</td>
<td>Click Pool Settings in the Add Pool wizard.</td>
</tr>
<tr>
<td>Pool settings for an existing pool</td>
<td>Select the Pool Settings tab.</td>
</tr>
</tbody>
</table>

4. Click Browse next to Connection Server restrictions and configure the View Connection Server instances that can access the desktop pool.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make the pool accessible to any View Connection Server instance</td>
<td>Select No Restrictions.</td>
</tr>
<tr>
<td>Make the pool accessible only to View Connection Server instances that have those tags</td>
<td>Select Restrict to these tags and select one or more tags. You can use the check boxes to select multiple tags.</td>
</tr>
</tbody>
</table>

5. Click OK to save your changes.
Setting Up User Authentication

View uses your existing Active Directory infrastructure for user authentication and management. For added security, you can integrate View with smart card authentication and two-factor authentication solutions such as RSA SecurID and RADIUS.

This chapter includes the following topics:

- “Using SAML 2.0 Authentication,” on page 155
- “Using Smart Card Authentication,” on page 157
- “Using Smart Card Certificate Revocation Checking,” on page 165
- “Using Two-Factor Authentication,” on page 168
- “Using the Log In as Current User Feature Available with Windows-Based View Client,” on page 172
- “Allow Users to Save Credentials,” on page 173

Using SAML 2.0 Authentication

Security Assertion Markup Language (SAML) server authentication allows View to exchange authentication information with other services such as the Horizon Web service. After a user signs in to Horizon Workspace, the SAML server authentication enables the user to initiate a View session and begin using the virtual desktop without being prompted again for log in credentials.

Authentication to View is handled by the Horizon service through the SAML 2.0 authenticator. When authentication delegation is enabled, and a user is verified by SAML, the SAML identity provider performs all authentication, with the exception of the disclaimer.

When you select a View desktop icon in the Horizon User Portal, a SAML artifact is generated. The View client sends the artifact to the View Connection Server. When the View Connection Server validates the artifact, it connects with Horizon Workspace.

The View Connection Server sends the artifact to Horizon, where it is validated. Horizon Workspace then sends a SAML assertion to the View Connection Server, which is validated and authenticates the user with View. This authentication is then used to launch the View desktop after validation. The assertion is generated by Horizon Workspace after receiving the artifact from the View Connection Server. The View Connection Server validates the assertion received from Horizon Workspace.

You must associate the View Connection Server with a SAML authentication service such as Horizon Workspace to facilitate this process.

**Note** If you intend to provide access to your desktops through Horizon Workspace, verify that you create the desktop pools as a user with Administrators permissions on the root folder in View. If you give the user Administrators permissions on a folder other than the root folder, Horizon Workspace will not recognize the SAML 2.0 Authenticator you configure in View, and you cannot configure the pool in Horizon Workspace.
Configure SAML 2.0 Authenticators in View Administrator

To configure a SAML Server to perform authentication tasks, you must add a SAML authenticator and specify a label, Metadata URL, Administration URL, and other settings.

Prerequisites

- Verify that the SAML 2.0 Authenticator is installed and available for inclusion in the Horizon service and View Connection Server. For installation and configuration information, see https://www.vmware.com/support/pubs/horizon_pubs.html.
- Make a note of the name of the Horizon server. You must enter this name in the metadata URL string during configuration.
- Make a note of the URL for accessing the administration console of the SAML identity provider. You specify this URL during configuration.

Procedure

1. In View Administrator, navigate to View Configuration > Servers.
2. Click the Connection Servers tab.
3. Select a server and click Edit.
4. Click the Authentication tab in the Edit View Connection Server Settings dialog box.
5. On the Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator) drop-down menu, select the appropriate authentication setting.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>SAML authentication is disabled.</td>
</tr>
<tr>
<td>Allowed</td>
<td>SAML authentication is allowed. You can login to View manually from the View Client, or you can log in by using Horizon.</td>
</tr>
<tr>
<td>Required</td>
<td>SAML authentication is required. You can log in to View only from Horizon. You cannot log in manually.</td>
</tr>
</tbody>
</table>

6. From the SAML Authenticator drop down menu, select Create New Authenticator.

If a SAML 2.0 authenticator has already been added, click Manage Authenticators > Add SAML 2.0 Authenticator.

7. Complete the information in the Add SAML 2.0 Authenticator dialog box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Label</td>
<td>Used to identify the SAML 2.0 authenticator in the Select Authenticator drop-down menu on the Authenticators tab of the Edit View Connection Server Settings dialog box.</td>
</tr>
<tr>
<td>Description</td>
<td>This is optional. This a brief description of the authenticator.</td>
</tr>
<tr>
<td>Metadata URL</td>
<td>Used to retrieve all the information required to exchange SAML information between the SAML identity provider and a connection server. The URL has the following format: <a href="https://YOUR">https://YOUR</a> HORIZON SERVER NAME/SAAS/API/1.0/GET/metadata/idp.xml.</td>
</tr>
<tr>
<td>Administration URL</td>
<td>This is optional. This URL is a link to the administration console for the SAML identity provider.</td>
</tr>
</tbody>
</table>

8. Click OK.

If you do not have valid trusted certificates installed, you will be prompted to verify the certificate.

9. Navigate to Dashboard in the Inventory section of View Administrator.
10 Click **SAML 2.0 Authenticators**.

11 Select the SAML server that you modified or added, verify the details, and click **OK**.

The View dashboard now displays the SAML 2.0 authenticator in a Healthy condition, which is indicated by a green icon.

You can configure each View Connection Server instance with a **Required**, **Allowed**, or **Disabled** authentication setting, depending on specific customer requirements.

### 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 Horizon 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 Horizon 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 system, 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 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 158
   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 159
   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 159
   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 160
   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 161
   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 159.

**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 159.

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 158.
- Verify that the keytool utility is added to the system path on your View Connection Server or security
  server host. See the VMware Horizon 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. Settings that are configured on a View Connection Server instance are also applied to a paired security server.
Configure Smart Card Settings in View Administrator

You can use View Administrator to specify settings to accommodate different smart card authentication scenarios.

When you configure these settings on a View Connection Server instance, the settings are also applied to paired security servers.

Prerequisites

- Modify View Connection Server configuration properties on your View Connection Server host.
- Verify that View clients make HTTPS connections directly to your View Connection Server or security server host. Smart card authentication is not supported if you off-load SSL to an intermediate device that makes HTTP connections to the View Connection Server or security server host.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Allowed</td>
<td>Smart card authentication is disabled on the View Connection Server instance.</td>
</tr>
<tr>
<td>Optional</td>
<td>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.</td>
</tr>
<tr>
<td>Required</td>
<td>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.</td>
</tr>
</tbody>
</table>

*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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect users from View Connection Server when they remove their smart cards</td>
<td>Select the Disconnect user sessions on smart card removal check box.</td>
</tr>
<tr>
<td>Keep users connected to View Connection Server when they remove their smart cards and let them start new desktop sessions without reauthenticating</td>
<td>Deselect the Disconnect user sessions on smart card removal check box.</td>
</tr>
</tbody>
</table>

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 162.

Verify your smart card authentication configuration. See “Verify Your Smart Card Authentication Configuration,” on page 164.

**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 162
  
  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 163
  
  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 163
  
  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 164
  
  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 the Active Directory server, navigate to the Group Policy Management plug-in.

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

2. Expand the **Computer Configuration** section and open **Windows Settings\Security Settings\Public Key**.
3. Right-click **Trusted Root Certification Authorities** and select **Import**.
4. Follow the prompts in the wizard to import the root certificate (for example, **rootCA.cer**) and click **OK**.
5. Close the Group Policy window.
All of the systems in the domain now have a copy of the root certificate in their trusted root store.

What to do next

If an intermediate certification authority (CA) issues your smart card login or domain controller certificates, add the intermediate certificate to the Intermediate Certification Authorities group policy in Active Directory. See “Add an Intermediate Certificate to Intermediate Certification Authorities,” on page 164.

Add an Intermediate Certificate to Intermediate Certification Authorities

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

Procedure

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

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

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

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

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

5. Close the Group Policy window.

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

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 166

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 166

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 166

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 167

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 168

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


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**


**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

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enableRevocationChecking</td>
<td>Set this property to <strong>true</strong> to enable certificate revocation checking.</td>
</tr>
<tr>
<td></td>
<td>When this property is set to <strong>false</strong>, certificate revocation checking is</td>
</tr>
<tr>
<td></td>
<td>disabled and all other certificate revocation checking properties are</td>
</tr>
<tr>
<td></td>
<td>ignored. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>crlLocation</td>
<td>Specifies the location of the CRL, which can be either a URL or a file path.</td>
</tr>
<tr>
<td></td>
<td>If you do not specify a URL, or if the specified URL is invalid, View</td>
</tr>
<tr>
<td></td>
<td>uses the list of CRLs on the user certificate if <strong>allowCertCRLs</strong> is set to</td>
</tr>
<tr>
<td></td>
<td><strong>true</strong> or is not specified. If View cannot access a CRL, CRL checking</td>
</tr>
<tr>
<td></td>
<td>fails.</td>
</tr>
<tr>
<td>allowCertCRLs</td>
<td>When this property is set to <strong>true</strong>, View extracts a list of CRLs</td>
</tr>
<tr>
<td></td>
<td>from the user certificate. The default value is <strong>true</strong>.</td>
</tr>
<tr>
<td>enableOCSP</td>
<td>Set this property to <strong>true</strong> to enable OCSP certificate revocation checking.</td>
</tr>
<tr>
<td></td>
<td>The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>ocspURL</td>
<td>Specifies the URL of an OCSP Responder.</td>
</tr>
<tr>
<td>ocspResponderCert</td>
<td>Specifies the file that contains the OCSP Responder’s signing certificate.</td>
</tr>
<tr>
<td></td>
<td>View uses this certificate to verify that the OCSP Responder’s responses</td>
</tr>
<tr>
<td></td>
<td>are genuine.</td>
</tr>
<tr>
<td>ocspSendNonce</td>
<td>When this property is set to <strong>true</strong>, a nonce is sent with OCSP requests</td>
</tr>
<tr>
<td></td>
<td>to prevent repeated responses. The default value is <strong>false</strong>.</td>
</tr>
<tr>
<td>ocspCRLFailover</td>
<td>When this property is set to <strong>true</strong>, View uses CRL checking if OCSP</td>
</tr>
<tr>
<td></td>
<td>certificate revocation checking fails. The default value is <strong>true</strong>.</td>
</tr>
</tbody>
</table>

Using Two-Factor Authentication

You can configure a View Connection Server instance so that users are required to use RSA SecurID authentication or RADIUS (Remote Authentication Dial-In User Service) authentication.

With Horizon View 5.1 and later releases, RADIUS support has been added to the two-factor authentication feature included with Horizon View:

- RADIUS support offers a wide range of alternative two-factor token-based authentication options.
- Horizon View now provides an open standard extension interface to allow third-party solution providers to integrate advanced authentication extensions into Horizon View.

Because two-factor authentication solutions such as RSA SecurID and RADIUS work with authentication managers, installed on separate servers, you must have those servers configured and accessible to the View Connection Server host. For example, if you use RSA SecurID, the authentication manager would be RSA Authentication Manager. If you have RADIUS, the authentication manager would be a RADIUS server.
To use two-factor authentication, each user must have a token, such as an RSA SecurID token, that is registered with its authentication manager. A two-factor authentication token is a piece of hardware or software that generates an authentication code at fixed intervals. Often authentication requires knowledge of both a PIN and an authentication code.

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

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 Using Two-Factor Authentication** on page 169
  When a user connects to a View Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in View Client.

- **Enable Two-Factor Authentication in View Administrator** on page 170
  You enable a View Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying View Connection Server settings in View Administrator.

- **Troubleshooting RSA SecurID Access Denial** on page 171
  Access is denied when View Client connects with RSA SecurID authentication.

- **Troubleshooting RADIUS Access Denial** on page 172
  Access is denied when View Client connects with RADIUS two-factor authentication.

### Logging in Using Two-Factor Authentication

When a user connects to a View Connection Server instance that has RSA SecurID authentication or RADIUS authentication enabled, a special login dialog box appears in View Client.

Users enter their RSA SecurID or RADIUS authentication user name and passcode in the a special login dialog box. A two-factor authentication 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.

- When logging in to View, RADIUS authentication works much like RSA SecurID. If the RADIUS server issues an access challenge, View Client displays a dialog box similar to the RSA SecurID prompt for the next token code. Currently support for RADIUS challenges is limited to prompting for text input. Any challenge text sent from the RADIUS server is not displayed. More complex forms of challenge, such as multiple choice and image selection, are currently not supported.

  After a user enters credentials in View Client, the RADIUS server can send an SMS text message or email, or text using some other out-of-band mechanism, to the user's cell phone with a code. The user can enter this text and code into View client to complete the authentication.

- Because some RADIUS vendors provide the ability to import users from Active Directory, end users might first be prompted to supply Active Directory credentials before being prompted for a RADIUS authentication user name and passcode.
Enable Two-Factor Authentication in View Administrator

You enable a View Connection Server instance for RSA SecurID authentication or RADIUS authentication by modifying View Connection Server settings in View Administrator.

Prerequisites

Install and configure the two-factor authentication software, such as the RSA SecurID software or the RADIUS software, on an authentication manager server.

- For RSA SecurID authentication, export the sdconf.rec file for the View Connection Server instance from RSA Authentication Manager. See the RSA Authentication Manager documentation.
- For RADIUS authentication, follow the vendor's configuration documentation. Make a note of the RADIUS server's host name or IP address, the port number on which it is listening for RADIUS authentication (usually 1812), the authentication type (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2) and the shared secret. You will enter these values in View Administrator. You can enter values for a primary and a secondary RADIUS authenticator.

Procedure

1. In View Administrator, select View Configuration > Servers.
2. On the Connection Servers tab, select the server and click Edit.
3. On the Authentication tab, from the 2-factor authentication drop-down list in the Advanced Authentication section, select RSA SecureID or RADIUS.
4. To force RSA SecurID or RADIUS user names to match user names in Active Directory, select Enforce SecurID and Windows user name matching or Enforce 2-factor and Windows user name matching.
   If you select this option, users must use the same RSA SecurID or RADIUS user name for Active Directory authentication. If you do not select this option, the names can be different.
5. For RSA SecurID, click Upload File, type the location of the sdconf.rec file, or click Browse to search for the file.
6 For RADIUS authentication, complete the rest of the fields:
   a Select **Use the same username and password for RADIUS and Windows authentication** if the initial RADIUS authentication uses Windows authentication that triggers an out-of-band transmission of a token code, and this token code is used as part of a RADIUS challenge.

   If you select this check box, users will not be prompted for Windows credentials after RADIUS authentication if the RADIUS authentication uses the Windows username and password. Users do not have to reenter the Windows username and password after RADIUS authentication.

   b From the **Authenticator** drop-down list, select **Create New Authenticator** and complete the page.

   - Set **Accounting port** to 0 unless you want to enable RADIUS accounting. Set this port to a non-zero number only if your RADIUS server supports collecting accounting data. If the RADIUS server does not support accounting messages and you set this port to a nonzero number, the messages will be sent and ignored and retried a number of times, resulting in a delay in authentication.

   Accounting data can be used in order to bill users based on usage time and data. Accounting data can also be used for statistical purposes and for general network monitoring.

   - If you specify a realm prefix string, the string is placed at the beginning of the username when it is sent to the RADIUS server. For example, if the username entered in the View Client is `jdoe` and the realm prefix `DOMAIN-A\` is specified, the username `DOMAIN-A\jdoe` is sent to the RADIUS server. Similarly if you use the realm suffix, or postfix, string `@mycorp.com`, the username `jdoe@mycorp.com` is sent to the RADIUS server.

7 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 configuration settings take effect immediately.

When users open View Client and authenticate to View Connection Server, they are prompted for two-factor authentication. For RADIUS authentication, the login dialog box displays text prompts that contain the token label you specified.

**What to do next**

If you have a replicated group of View Connection Server instances and you want to also set up RADIUS authentication on them, you can re-use an existing RADIUS authenticator configuration.

**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.

Troubleshooting RADIUS Access Denial

Access is denied when View Client connects with RADIUS two-factor authentication.

Problem

A View Client connection using RADIUS two-factor authentication displays Access Denied.

Cause

RADIUS does not receive a reply from the RADIUS server, causing View to time out.

Solution

The following common configuration mistakes most often lead to this situation:

- The RADIUS server has not been configured to accept the View Connection Server instance as a RADIUS client. Each View Connection Server instance using RADIUS must be set up as a client on the RADIUS server. See the documentation for your RADIUS two-factor authentication product.
- The shared secret values on the View Connection Server instance and the RADIUS server do not match.

Using the Log In as Current User Feature Available with Windows-Based View Client

With View Client for Windows, when 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:

- When smart card authentication is set to Required on a View Connection Server instance, 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.

- 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.

---

**Allow Users to Save Credentials**

Administrators can configure View Connection Server to allow View Client mobile devices to remember a user’s user name, password, and domain information. If users choose to have their credentials saved, the credentials are added to the login fields in View Client on subsequent connections.

On Windows-based View Clients, the feature for logging in as the current user avoids requiring users to supply credentials multiple times. With View Client for mobile devices, such as Android and iPad, you can configure a feature that allows a **Save Password** check box to appear on the login dialog boxes.

You configure a timeout limit that indicates how long to save credential information by setting a value in View LDAP. The timeout limit is set in minutes. 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. In the Connection Settings dialog box, select or connect to `DC=vdi,DC=vmware,DC=int`.
3. In the Computer pane, select or type `localhost:389` or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.
   
   For example: `localhost:389` or `mycomputer.mydomain.com:389`
4. On the object `CN=Common, OU=Global, OU=Properties`, set the `pae-ClientCredentialCacheTimeout` attribute.

   When this attribute is not set or is set to 0, the feature is disabled. To enable this feature, you can set the number of minutes to retain the credential information, or set a value of -1, meaning that there is no timeout.

   On View Connection Server, the new setting takes effect immediately. You do not need to restart the View Connection Server service or the client computer.
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,” on page 175
- “Using Active Directory Group Policies,” on page 179
- “Using the View Group Policy Administrative Template Files,” on page 180
- “Setting Up Location-Based Printing,” on page 218
- “Using Terminal Services Group Policies,” on page 221
- “Active Directory Group Policy Example,” on page 222

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.

- Configure Global Policy Settings on page 176
  You can configure global policies to control the behavior of all client sessions users.

- Configure Policies for Desktop Pools on page 176
  You can configure desktop-level policies to affect specific desktop pools. Desktop-level policy settings take precedence over their equivalent global policy settings.

- Configure Policies for Desktop Users on page 177
  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.
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 177
- “Local Mode Policies,” on page 178

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 177
- “Local Mode Policies,” on page 178

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 177.

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>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia redirection (MMR)</td>
<td>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.</td>
</tr>
<tr>
<td>USB Access</td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 8-1. View Policies (Continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote mode</td>
<td>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.</td>
</tr>
<tr>
<td>PCoIP hardware acceleration</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 Deny.  
If you change this value from Allow 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)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target replication frequency</td>
<td>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 <strong>No replication</strong> setting. If you select <strong>At a specified interval</strong>, the default replication interval is 12 hours. You can prohibit scheduled replications by selecting <strong>No replication</strong>. The <strong>No replication</strong> policy does not prohibit explicit replication requests. You can initiate replications in View Administrator, and users can request replications if the <strong>User initiated replication</strong> policy is set to <strong>Allow</strong>. If a replication takes longer than the interval that is specified in the <strong>Target replication frequency</strong> policy, the next scheduled replication starts after the previous one is completed. The pending replication does not cancel the previous one. For example, the <strong>Target replication frequency</strong> 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.</td>
</tr>
<tr>
<td>User deferred replication</td>
<td>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 <strong>Deny</strong>. When the value is set to <strong>Allow</strong>, the deferment period is two hours.</td>
</tr>
<tr>
<td>Disks replicated</td>
<td>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 <strong>Persistent disks</strong>.</td>
</tr>
<tr>
<td>User-initiated check in</td>
<td>Determines whether users are allowed to check in desktops that are running in local mode. The default value is <strong>Allow</strong>.</td>
</tr>
<tr>
<td>User-initiated replication</td>
<td>Determines whether users are allowed to initiate replications from their desktops when they run in local mode. The default value is <strong>Allow</strong>.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Template Name</th>
<th>Template File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware View Agent Configuration</td>
<td>vdm_agent.adm</td>
<td>Contains policy settings related to the authentication and environmental components of View Agent.</td>
</tr>
<tr>
<td>VMware View Client Configuration</td>
<td>vdm_client.adm</td>
<td>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.</td>
</tr>
<tr>
<td>VMware View Server Configuration</td>
<td>vdm_server.adm</td>
<td>Contains policy settings related to View Connection Server.</td>
</tr>
<tr>
<td>VMware View Common Configuration</td>
<td>vdm_common.adm</td>
<td>Contains policy settings that are common to all View components.</td>
</tr>
<tr>
<td>VMware View PCoIP Session Variables</td>
<td>pcoip.adm</td>
<td>Contains policy settings related to the PCoIP display protocol.</td>
</tr>
</tbody>
</table>

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 policy settings in the View Agent Configuration ADM template file other than those settings that are used with USB devices. 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
By default, while a user is logged in to a View desktop session, you can use RDP to connect to the desktop virtual machine from outside of View. The RDP connection terminates the View desktop session, and the View user's unsaved data and settings might be lost. The View user cannot log in to the desktop until the external RDP connection is closed. To avoid this situation, disable the AllowDirectRDP setting.  
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. |
| 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 185 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 185 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. |
Table 8-4. View Agent Configuration Template Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Time Zone Synchronization</td>
<td>X</td>
<td>X</td>
<td>Determines whether the time zone of the View desktop is synchronized with</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the time zone of the connected client. An enabled setting applies only if</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the Disable time zone forwarding setting of the View Client Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>policy is not set to disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This setting is disabled by default.</td>
</tr>
<tr>
<td>Enable multi-media acceleration</td>
<td>X</td>
<td></td>
<td>Determines whether multimedia redirection (MMR) is enabled on the View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>desktop. MMR is a Microsoft DirectShow filter that forwards multimedia data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>from specific codecs on the remote system directly through a TCP socket to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the client. The data is then decoded directly on the client, where it is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>played. You can disable MMR if the client has insufficient resources to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>handle local multimedia decoding. MMR does not work correctly if the View</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Client video display hardware does not have overlay support. MMR policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>does not apply to local desktop sessions. This setting is enabled by default.</td>
</tr>
<tr>
<td>Force MMR to use software overlay</td>
<td>X</td>
<td></td>
<td>Determines whether the multimedia redirection (MMR) feature uses a software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>overlay instead of a hardware overlay. MMR uses video display hardware with</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>overlay support for better performance. Because hardware overlays typically</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>exist only on the primary monitor in a multi-monitor system, video is not</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>displayed when it is dragged from the primary monitor to a secondary monitor.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enabling this setting forces MMR to use a software overlay on all monitors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This setting is disabled by default.</td>
</tr>
<tr>
<td>ShowDiskActivityIcon</td>
<td>X</td>
<td></td>
<td>This setting is not supported in this release.</td>
</tr>
<tr>
<td>Toggle Display Settings Control</td>
<td>X</td>
<td></td>
<td>Determines whether to disable the Settings tab in the Display control panel</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>when a client session uses the PCoIP display protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This setting is enabled by default.</td>
</tr>
</tbody>
</table>

**USB Settings for the View Agent**

You can define USB policy settings for both View Agent and View Client for Windows. On connection, View Client downloads the USB policy settings from View Agent and uses them in conjunction with the View Client USB policy settings to decide which devices it will allow to be available for redirection from the client computer.

The settings apply at computer level. View Agent preferentially reads the settings from the GPO at computer level, and otherwise from the registry at HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB

Table 8-5 describes each policy setting for splitting composite USB devices in the View Agent Configuration ADM template file. View Agent does not enforce these settings. View Agent passes the settings to View Client for interpretation and enforcement according to whether you specify the merge (m) or override (o) modifier. View Client uses the settings to decide whether to split composite USB devices into their component devices, and whether to exclude the component devices from being available for redirection. For a description of how View applies the policies for splitting composite USB devices, see “Configuring Device Splitting Policy Settings for Composite USB Devices,” on page 199.
**Table 8-5. View Agent Configuration Template: Device-Splitting Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Auto Device Splitting</td>
<td>Allows the automatic splitting of composite USB devices.</td>
</tr>
<tr>
<td></td>
<td>The default value is undefined.</td>
</tr>
<tr>
<td>Exclude Vid/Pid Device From Split</td>
<td>Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is `{m</td>
</tr>
<tr>
<td>Split Vid/Pid Device</td>
<td>Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is `{m</td>
</tr>
</tbody>
</table>

Table 8-6 describes each agent-enforced policy setting for USB in the View Agent Configuration ADM template file. View Agent uses the settings to decide if a USB device can be forwarded to the host machine. View Agent also passes the settings to View Client for interpretation and enforcement according to whether you specify the merge (m) or override (o) modifier. View Client uses the settings to decide if a USB device is available for redirection. As View Agent always enforces an agent-enforced policy setting that you specify, the effect might be to counteract the policy that you have set for View Client. For a description of how View applies the policies for filtering USB devices, see “Configuring Filter Policy Settings for USB Devices,” on page 201.

**Table 8-6. View Agent Configuration Template: Agent-Enforced Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude All Devices</td>
<td>Excludes all USB devices from being forwarded. If set to <code>true</code>, you can use other policy settings to allow specific devices or families of devices to be forwarded. If set to <code>false</code>, you can use other policy settings to prevent specific devices or families of devices from being forwarded. If set to <code>true</code> and passed to View Client, this setting always overrides the setting on View Client. You cannot use the <code>merge</code> (m) or <code>override</code> (o) modifier with this setting. The default value is undefined, which equates to <code>false</code>.</td>
</tr>
<tr>
<td>Exclude Device Family</td>
<td>Excludes families of devices from being forwarded. The format of the setting is `{m</td>
</tr>
</tbody>
</table>

VMware Horizon View Administration 184 VMware, Inc.
<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Vid/Pid Device</td>
<td>Excludes devices with specified vendor and product IDs from being forwarded. The format of the setting is {m</td>
</tr>
<tr>
<td>Include Device Family</td>
<td>Includes families of devices that can be forwarded. The format of the setting is {m</td>
</tr>
<tr>
<td>Include Vid/Pid Device</td>
<td>Includes devices with specified vendor and product IDs that can be forwarded. The format of the setting is {m</td>
</tr>
</tbody>
</table>

Table 8-7 describes each client-interpreted policy setting in the View Agent Configuration ADM template file. View Agent does not enforce these settings. View Agent passes the settings to View Client for interpretation and enforcement. View Client uses the settings to decide if a USB device is available for redirection.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Audio Input Devices</td>
<td>Allows audio input devices to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow Audio Output Devices</td>
<td>Allows audio output devices to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow HIDBootable</td>
<td>Allows input devices other than keyboards or mice that are available at boot time (also known as hid-bootable devices) to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow Other Input Devices</td>
<td>Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow Keyboard and Mouse Devices</td>
<td>Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow Smart Cards</td>
<td>Allows smart-card devices to be forwarded. The default value is undefined.</td>
</tr>
<tr>
<td>Allow Video Devices</td>
<td>Allows video devices to be forwarded. The default value is undefined.</td>
</tr>
</tbody>
</table>

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:\proexp.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 185 for more information.

Table 8-8 describes the registry keys that contain client system information and lists the types of client systems that support them.

**Table 8-8. Client System Information**

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Description</th>
<th>Client Systems Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewClient_IP_Address</td>
<td>The IP address of the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_MAC_Address</td>
<td>The MAC address of the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Machine_Name</td>
<td>The machine name of the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Machine_Domain</td>
<td>The domain of the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_LoggedOn_Username</td>
<td>The user name that was used to log in to the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_LoggedOn_Domainname</td>
<td>The domain name that was used to log in to the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Type</td>
<td>The thin client name or operating system type of the client system.</td>
<td>Windows, Linux, Mac</td>
</tr>
</tbody>
</table>

*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.
### Table 8-8. Client System Information (Continued)

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Description</th>
<th>Client Systems Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewClient_Broker_DNS_Name</td>
<td>The DNS name of the View Connection Server instance.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Broker_URL</td>
<td>The URL of the View Connection Server instance.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Broker_Tunneled</td>
<td>The status of the tunnel connection for the View Connection Server, which can be either true (enabled) or false (disabled).</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Broker_Tunnel_URL</td>
<td>The URL of the View Connection Server tunnel connection, if the tunnel connection is enabled.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Broker_Remote_IP_Address</td>
<td>The IP address of the client system that is seen by the View Connection Server instance.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_TZID</td>
<td>The Olson time zone ID. To disable time zone synchronization, enable the View Agent Disable Time Zone Synchronization group policy setting.</td>
<td>Windows, Linux, Mac</td>
</tr>
<tr>
<td>ViewClient_Windows_Timezone</td>
<td>The GMT standard time. To disable time zone synchronization, enable the View Agent Disable Time Zone Synchronization group policy setting.</td>
<td>Windows</td>
</tr>
</tbody>
</table>

### 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 8-9 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 8-9. View Client Configuration Template: Scripting Definitions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect all USB devices to the desktop on launch</td>
<td>Determines whether all of the available USB devices on the client system are connected to the desktop when the desktop is launched.</td>
</tr>
<tr>
<td>Connect all USB devices to the desktop when they are plugged in</td>
<td>Determines whether USB devices are connected to the desktop when they are plugged in to the client system.</td>
</tr>
</tbody>
</table>
Table 8-9. View Client Configuration Template: Scripting Definitions (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DesktopLayout</td>
<td>Specifies the layout of the View Client window that a user sees when logging into a View desktop. The layout choices are as follows:</td>
</tr>
<tr>
<td></td>
<td>- Full Screen</td>
</tr>
<tr>
<td></td>
<td>- Multimonitor</td>
</tr>
<tr>
<td></td>
<td>- Window – Large</td>
</tr>
<tr>
<td></td>
<td>- Window – Small</td>
</tr>
<tr>
<td></td>
<td>This setting is available only when the DesktopName to select setting is also set.</td>
</tr>
<tr>
<td>DesktopName to select</td>
<td>Specifies the default desktop that View Client uses during login.</td>
</tr>
<tr>
<td>Disable 3rd-party Terminal Services plugins</td>
<td>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.</td>
</tr>
<tr>
<td>Logon DomainName</td>
<td>Specifies the NetBIOS domain that View Client uses during login.</td>
</tr>
<tr>
<td>Logon Password</td>
<td>Specifies the password that View Client uses during login. The password is stored in plain text by Active Directory.</td>
</tr>
<tr>
<td>Logon UserName</td>
<td>Specifies the username that View Client uses during login.</td>
</tr>
<tr>
<td>Server URL</td>
<td>Specifies the URL that View Client uses during login, for example, <a href="http://view1.example.com">http://view1.example.com</a>.</td>
</tr>
<tr>
<td>Suppress error messages (when fully scripted only)</td>
<td>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.</td>
</tr>
</tbody>
</table>

Security Settings

Table 8-10 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 8-10. View Client Configuration Template: Security Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow command line</td>
<td>X</td>
<td>User</td>
<td>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.</td>
</tr>
</tbody>
</table>
| credentials           |          |      | 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 8-10. View Client Configuration Template: Security Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate verification mode</td>
<td>X</td>
<td></td>
<td>Configures the level of certificate checking that is performed by View Client. You can select one of these modes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>No Security.</strong> View does not perform certificate checking.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>Warn But Allow.</strong> When the following server certificate issues occur, a warning is displayed, but the user can continue to connect to View Connection Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- A verifiable certificate that was configured in your deployment has expired or is not yet valid.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If any other certificate error condition occurs, View displays an error dialog and prevents the user from connecting to View Connection Server. <strong>Warn But Allow</strong> is the default value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>Full Security.</strong> If any type of certificate error occurs, the user cannot connect to View Connection Server. View displays certificate errors to the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When this setting is not configured or disabled, View Client users can select a certificate verification mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To allow a View server to perform checking of certificates provided by a View Client, the View Client must make HTTPS connections to the View Connection Server or security server host. Certificate checking is not supported if you off-load SSL to an intermediate device that makes HTTP connections to the View Connection Server or security server host.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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 <strong>CertCheckMode</strong> value name to one of the following registry keys on the client computer:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- For 32-bit Windows: \HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- For 64-bit Windows: \HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use the following values in the registry key:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>0</strong> implements <strong>No Security.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>1</strong> implements <strong>Warn But Allow.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>2</strong> implements <strong>Full Security.</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you configure both the group policy setting and the <strong>CertCheckMode</strong> setting in the registry key, the group policy setting takes precedence over the registry key value.</td>
</tr>
</tbody>
</table>
### Table 8-10. View Client Configuration Template: Security Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default value of the 'Log in as current user' checkbox</td>
<td>X</td>
<td>X</td>
<td>Specifies the default value of the <strong>Log in as current user</strong> 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 <code>logInAsCurrentUser</code> option, that value overrides this setting. When the <strong>Log in as current user</strong> 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.</td>
</tr>
<tr>
<td>Display option to Log in as current user</td>
<td>X</td>
<td>X</td>
<td>Determines whether the <strong>Log in as current user</strong> 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 <strong>Log in as current user</strong> check box by using the policy setting <strong>Default value of the 'Log in as current user' checkbox</strong>. This setting is enabled by default.</td>
</tr>
<tr>
<td>Enable jump list integration</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Enable Single Sign-On for smart card authentication</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Ignore bad SSL certificate date received from the server</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Ignore certificate revocation problems</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>
Table 8-10. View Client Configuration Template: Security Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore incorrect SSL certificate common name (host name field)</td>
<td>X</td>
<td></td>
<td>Determines whether errors that are associated with incorrect server certificate common names are ignored. These errors occur when the certificate does not match the hostname of the server that sends it. This setting applies to View 4.6 and earlier releases only.</td>
</tr>
<tr>
<td>Ignore incorrect usage problems</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Ignore unknown certificate authority problems</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

RDP Settings

Table 8-11 describes the Remote Desktop Protocol (RDP) settings in the View Client Configuration ADM template file. All RDP settings are User Configuration settings.

Table 8-11. View Client Configuration Administrative Template: RDP Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio redirection</td>
<td>Determines whether audio information played on the View desktop is redirected. Select one of the following settings:</td>
</tr>
<tr>
<td>Disable Audio</td>
<td>Audio is disabled.</td>
</tr>
<tr>
<td>Play VM (needed for VoIP USB Support)</td>
<td>Audio plays within the View desktop. This setting requires a shared USB audio device to provide sound on the client.</td>
</tr>
<tr>
<td>Redirect to client</td>
<td>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.</td>
</tr>
<tr>
<td>Audio capture redirection</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Table 8-11. View Client Configuration Administrative Template: RDP Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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/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. Tunneld connections are not supported with NLA. |
| **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. |
Table 8-11. View Client Configuration Administrative Template: RDP Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Font smoothing</td>
<td>(Windows Vista or later) Determines whether antialiasing is applied to the fonts on the View desktop.</td>
</tr>
<tr>
<td>Menu and window animation</td>
<td>Determines whether animation for menus and windows is enabled when clients connect to a View desktop.</td>
</tr>
<tr>
<td>Redirect clipboard</td>
<td>Determines whether the local clipboard information is redirected when clients connect to the View desktop.</td>
</tr>
<tr>
<td>Redirect drives</td>
<td>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.</td>
</tr>
<tr>
<td>Redirect printers</td>
<td>Determines whether local printers are redirected when clients connect to the View desktop.</td>
</tr>
<tr>
<td>Redirect serial ports</td>
<td>Determines whether local COM ports are redirected when clients connect to the View desktop.</td>
</tr>
<tr>
<td>Redirect smart cards</td>
<td>Determines whether local smart cards are redirected when clients connect to the View desktop.</td>
</tr>
<tr>
<td>Redirect supported plug-and-play devices</td>
<td>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.</td>
</tr>
<tr>
<td>Shadow bitmaps</td>
<td>Determines whether bitmaps are shadowed. This setting has no effect in full-screen mode.</td>
</tr>
<tr>
<td>Show contents of window while dragging</td>
<td>Determines whether the folder contents appear when users drag a folder to a new location.</td>
</tr>
<tr>
<td>Themes</td>
<td>Determines whether themes appear when clients connect to a View desktop.</td>
</tr>
<tr>
<td>Windows key combination redirection</td>
<td>Determines where Windows key combinations are applied. This setting lets you send key combinations to the remote virtual machine or apply key combinations locally. If this setting is not configured, key combinations are applied locally.</td>
</tr>
</tbody>
</table>

**General Settings**

Table 8-12 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 8-12. View Client Configuration Template: General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Always on top</strong></td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Default Exit Behavior For Local Mode Desktops</strong></td>
<td>X</td>
<td></td>
<td>Controls the default exit behavior of desktops that are running in local mode. The default setting is <strong>Shutdown</strong>, which causes the guest operating system to shut down.</td>
</tr>
<tr>
<td><strong>Delay the start of replications when starting the View Client with Local Mode</strong></td>
<td>X</td>
<td></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Determine if the VMware View Client should use proxy.pac file</strong></td>
<td>X</td>
<td></td>
<td>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. <strong>Note</strong> This setting applies to direct connections only. It does not affect tunnel connections. This setting applies to View 4.6 and earlier releases only.</td>
</tr>
<tr>
<td><strong>Disable time zone forwarding</strong></td>
<td>X</td>
<td></td>
<td>Determines whether time zone synchronization between the View desktop and the connected client is disabled.</td>
</tr>
<tr>
<td><strong>Disable toast notifications</strong></td>
<td></td>
<td></td>
<td>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. <strong>Note</strong> If you enable this setting, the user does not see a 5-minute warning when the Session Timeout function is active.</td>
</tr>
<tr>
<td><strong>Don't check monitor alignment on spanning</strong></td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable multi-media acceleration</strong></td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable the shade</strong></td>
<td>X</td>
<td></td>
<td>Determines whether the shade menu bar at the top of the View Client window is visible. This setting is enabled by default. <strong>Note</strong> The shade menu bar is disabled by default for kiosk mode.</td>
</tr>
</tbody>
</table>
Table 8-12. View Client Configuration Template: General Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Computer</th>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redirect smart card readers in Local Mode</td>
<td>X</td>
<td></td>
<td>Determines whether smart card readers are redirected to local desktops. The readers are shared with the client system. This setting is enabled by default.</td>
</tr>
<tr>
<td>Tunnel proxy bypass address list</td>
<td>X</td>
<td></td>
<td>Specifies a list of tunnel addresses. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries.</td>
</tr>
<tr>
<td>URL for View Client online help</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Pin the shade</td>
<td>X</td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

USB Settings for the View Client

You can define USB policy settings for both View Agent and View Client for Windows. On connection, View Client downloads the USB policy settings from View Agent and uses them in conjunction with the View Client USB policy settings to decide which devices it will allow to be available for redirection from the host machine.

Table 8-13 describes each policy setting for splitting composite USB in the View Client Configuration ADM template file. The settings apply at computer level. View Client preferentially reads the settings from the GPO at computer level, and otherwise from the registry at HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB. For a description of how View applies the policies for splitting composite USB devices, see “Configuring Device Splitting Policy Settings for Composite USB Devices,” on page 199.

Table 8-13. View Client Configuration Template: USB Splitting Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Auto Device Splitting</td>
<td>Allow the automatic splitting of composite USB devices. The default value is undefined, which equates to false.</td>
</tr>
<tr>
<td>Exclude Vid/Pid Device From Split</td>
<td>Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is &lt;vid-xxxx_pid-yyyy&gt;[;vid-xxxx_pid-yyyy][;...]. You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: vid-0781_pid-55**</td>
</tr>
<tr>
<td>Split Vid/Pid Device</td>
<td>Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]). You can use the exintf keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (*) in place of individual digits in an ID. For example: vid-0781_pid-554c(exintf:01;exintf:02)</td>
</tr>
</tbody>
</table>

NOTE View does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as Include Vid/Pid Device to include those components. The default value is undefined.
Table 8-14 describes each policy setting for filtering USB devices in the View Client Configuration ADM template file. The settings apply at computer level. View Client preferentially reads the settings from the GPO at computer level, and otherwise from the registry at HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB. For a description of how View applies the policies for filtering USB devices, see “Configuring Filter Policy Settings for USB Devices,” on page 201.

Table 8-14. View Client Configuration Template: USB Filtering Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Audio Input Devices</td>
<td>Allows audio input devices to be redirected. The default value is undefined, which equates to <strong>true</strong>.</td>
</tr>
<tr>
<td>Allow Audio Output Devices</td>
<td>Allows audio output devices to be redirected. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Allow HIDBootable</td>
<td>Allows input devices other than keyboards or mice that are available at boot time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to <strong>true</strong>.</td>
</tr>
<tr>
<td>Allow Device Descriptor Failsafe Behavior</td>
<td>Allows devices to be redirected even if the View client fails to get the config/device descriptors. To allow a device even if it fails the config/desc, include it in the Include filters, such as <code>IncludeVidPid</code> or <code>IncludePath</code>. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Allow Other Input Devices</td>
<td>Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be redirected. The default value is undefined, which equates to <strong>true</strong>.</td>
</tr>
<tr>
<td>Allow Keyboard and Mouse Devices</td>
<td>Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be redirected. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Allow Smart Cards</td>
<td>Allows smart-card devices to be redirected. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Allow Video Devices</td>
<td>Allows video devices to be redirected. The default value is undefined, which equates to <strong>true</strong>.</td>
</tr>
<tr>
<td>Disable Remote Configuration</td>
<td>Disables the use of View Agent settings when performing USB device filtering. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Exclude All Devices</td>
<td>Excludes all USB devices from being redirected. If set to <strong>true</strong>, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to <strong>false</strong>, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of <strong>Exclude All Devices</strong> to <strong>true</strong> on View Agent, and this setting is passed to View Client, the View Agent setting overrides the View Client setting. The default value is undefined, which equates to <strong>false</strong>.</td>
</tr>
<tr>
<td>Exclude Device Family</td>
<td>Excludes families of devices from being redirected. The format of the setting is <code>family_name_1;family_name_2;...</code> For example: <code>bluetooth;smart-card</code> If you have enabled automatic device splitting, View examines the device family of each interface of a composite USB device to decide which interfaces should be excluded. If you have disabled automatic device splitting, View examines the device family of the whole composite USB device. The default value is undefined.</td>
</tr>
</tbody>
</table>
### Using Policies to Control USB Redirection

You can configure USB policies for both View Agent and View Client for Windows to specify whether View Client should split composite USB devices into separate components for redirection, to restrict the types of USB devices that View Client makes available for redirection, and to make View Agent prevent certain USB devices from being forwarded from a client computer. You cannot use USB policies to control which USB devices can be used with a checked-out remote desktop.

If you have older versions of View Agent or View Client installed, not all the features of the USB redirection policies are available. Table 8-15 shows how View applies the policies for different combinations of View Agent and View Client for Windows.

---

**Table 8-14. View Client Configuration Template: USB Filtering Settings (Continued)**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Vid/Pid Device</td>
<td>Excludes devices with specified vendor and product IDs from being redirected. The format of the setting is vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... You must specify ID numbers in hexadecimal. You can use the wildcard character (<em>) in place of individual digits in an ID. For example: **vid-0781_pid-</em>*<strong>;vid-0561_pid-554c</strong> The default value is undefined.</td>
</tr>
<tr>
<td>Exclude Path</td>
<td>Exclude devices at specified hub or port paths from being redirected. The format of the setting is bus-x1[;/y1].../port-z1[;bus-x2[;/y2].../port-z2]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: <strong>bus-1/2/3_port-02;bus-1/1/1/4_port-ff</strong> The default value is undefined.</td>
</tr>
<tr>
<td>Include Device Family</td>
<td>Includes families of devices that can be redirected. The format of the setting is family_name_1[;family_name_2]... For example: <strong>storage</strong> The default value is undefined.</td>
</tr>
<tr>
<td>Include Path</td>
<td>Include devices at a specified hub or port paths that can be redirected. The format of the setting is bus-x1[;/y1].../port-z1[;bus-x2[;/y2].../port-z2]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: <strong>bus-1/2_port-02;bus-1/7/1/4_port-0f</strong> The default value is undefined.</td>
</tr>
<tr>
<td>Include Vid/Pid Device</td>
<td>Includes devices with specified vendor and product IDs that can be redirected. The format of the setting is vid-xxx1_pid-yyy2[;vid-xxx2_pid-yyy2]... You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: <strong>vid-0561_pid-554c</strong> The default value is undefined.</td>
</tr>
</tbody>
</table>
### Table 8-15. Compatibility of USB Policy Settings

<table>
<thead>
<tr>
<th>View Agent Version</th>
<th>View Client Version</th>
<th>Effect of USB Policy Settings on USBRedirection</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 or later</td>
<td>5.1 or later</td>
<td>USB policy settings are applicable to both View Agent and View Client. You can use View Agent USB policy settings to block USB devices from being forwarded to a desktop. View Agent can send device splitting and filtering policy settings to View Client. You can use View Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop.</td>
</tr>
<tr>
<td>5.1 or later</td>
<td>5.0.x or earlier</td>
<td>USB policy settings apply only to View Agent. You can use View Agent USB policy settings to block USB devices from being forwarded to a desktop. You cannot use View Client USB policy settings to control which devices can be redirected from a client computer to a desktop. View Client cannot receive device splitting and filtering policy settings from View Agent. Existing registry settings for USB redirection by View Client remain valid.</td>
</tr>
<tr>
<td>5.0.x or earlier</td>
<td>5.1 or later</td>
<td>USB policy settings apply only to View Client. You can use View Client USB policy settings to prevent USB devices from being redirected from a client computer to a desktop. You cannot use View Agent USB policy settings to block USB devices from being forwarded to a desktop. View Agent cannot send device splitting and filtering policy settings to View Client.</td>
</tr>
<tr>
<td>5.0.x or earlier</td>
<td>5.0.x or earlier</td>
<td>USB policy settings do not apply. Existing registry settings for USB redirection by View Client remain valid.</td>
</tr>
</tbody>
</table>

If you upgrade View Client, any existing registry settings for USB redirection, such as `HardwareIdFilters`, remain valid until you define USB policies for View Client.

The Linux client does not support USB policies. You can use the USB policies for View Agent to control which USB devices are allowed to be forwarded from a Linux client to a desktop.

### Configuring Device Splitting Policy Settings for Composite USB Devices

Composite USB devices consist of a combination of two or more different devices, such as a pointing device and an audio input device, a video input device and a storage device, or a communications device and a storage device. If you want to allow one or more of the components to be available for redirection, you can split the composite device into its component interfaces, exclude certain interfaces from redirection, and create a separate filter for each interface.

**Table 8-16 shows how the value of the Allow Auto Device Splitting setting determines whether View Client attempts to split composite USB devices automatically. By default, automatic splitting is disabled.**

### Table 8-16. Effect of Combining Disable Automatic Splitting Policies

<table>
<thead>
<tr>
<th>Allow Auto Device Splitting Policy on View Agent</th>
<th>Allow Auto Device Splitting Policy on View Client</th>
<th>Combined Effective Allow Auto Device Splitting Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow - Default Client Setting</td>
<td><code>false</code> (automatic splitting disabled)</td>
<td>Automatic splitting disabled</td>
</tr>
<tr>
<td>Allow - Default Client Setting</td>
<td><code>true</code> (automatic splitting enabled)</td>
<td>Automatic splitting enabled</td>
</tr>
<tr>
<td>Allow - Default Client Setting</td>
<td>Not defined</td>
<td>Automatic splitting enabled</td>
</tr>
<tr>
<td>Allow - Override Client Setting</td>
<td>Any or not defined</td>
<td>Automatic splitting enabled</td>
</tr>
<tr>
<td>Not defined</td>
<td>Not defined</td>
<td>Automatic splitting disabled</td>
</tr>
</tbody>
</table>

By default, View disables automatic splitting, and excludes any audio-output, keyboard, mouse, or smart-card components of a composite USB device from redirection.
View applies the device splitting policy settings before it applies any filter policy settings. If you have enabled automatic splitting and do not explicitly exclude a composite USB device from being split by specifying its vendor and product IDs, View examines each interface of the composite USB device to decide which interfaces should be excluded or included according to the filter policy settings. If you have disabled automatic device splitting and do not explicitly specify the vendor and product IDs of a composite USB device that you want to split, View applies the filter policy settings to the entire device.

If you enable automatic splitting, you can use the `Exclude Vid/Pid Device From Split` policy to specify the composite USB devices that you want to exclude from splitting.

You can use the `Split Vid/Pid Device` policy to specify the vendor and product IDs of a composite USB device that you want to split. You can also specify the interfaces of the components of a composite USB device that you want to exclude from redirection. View does not apply any filter policy settings to components that you exclude in this way.

**IMPORTANT** If you use the `Split Vid/Pid Device` policy, View does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as `Include Vid/Pid Device` to include those components.

Table 8-17 shows the modifiers that specify how View Client handles a View Agent device splitting policy setting if there is an equivalent device splitting policy setting for View Client. These modifiers apply to all device-splitting policy settings.

**Table 8-17.** Splitting Modifiers for Device-Splitting Policy Settings on View Agent

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>m</code> (merge)</td>
<td>View Client applies the View Agent device splitting policy setting in addition to the View Client device splitting policy setting.</td>
</tr>
<tr>
<td><code>o</code> (override)</td>
<td>View Client uses the View Agent device splitting policy setting instead of the View Client device splitting policy setting.</td>
</tr>
</tbody>
</table>

Table 8-18 shows examples of how View Client processes the settings for `Exclude Device From Split by Vendor/Product ID` on View Agent when you specify different splitting modifiers.

**Table 8-18.** Examples of Applying Splitting Modifiers to Device-Splitting Policy Settings

<table>
<thead>
<tr>
<th>Exclude Device From Split by Vendor/Product ID on View Agent</th>
<th>Exclude Device From Split by Vendor/Product ID on View Client</th>
<th>Effective Exclude Device From Split by Vendor/Product ID Policy Setting Used by View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>m:vid-XXXX_pid-XXXX</code></td>
<td><code>vid-YYYY_pid-YYYY</code></td>
<td><code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code></td>
</tr>
<tr>
<td><code>o:vid-XXXX_pid-XXXX</code></td>
<td><code>vid-YYYY_pid-YYYY</code></td>
<td><code>vid-XXXX_pid-XXXX</code></td>
</tr>
<tr>
<td><code>m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code></td>
<td><code>vid-YYYY_pid-YYYY</code></td>
<td><code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code></td>
</tr>
<tr>
<td><code>o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code></td>
<td><code>vid-YYYY_pid-YYYY</code></td>
<td><code>vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY</code></td>
</tr>
</tbody>
</table>

View Agent does not apply the device splitting policy settings on its side of the connection.

View Client evaluates the device splitting policy settings in the following order of precedence:

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

A device splitting policy setting that excludes a device from being split takes precedence over any policy setting to split the device. If you define any interfaces or devices to be excluded from splitting, View Client excludes the matching component devices from being available for redirection.
Examples of Setting Policies to Split Composite USB Devices

Set splitting policies for desktops to exclude devices with a specific vendor and product IDs from redirection after automatic splitting and pass these policies to client computers.

Table 8-19. Use View Agent Policies to Specify Device Splitting Policy Settings

<table>
<thead>
<tr>
<th>USB Splitting Policies on View Agent</th>
<th>USB Splitting Policies on View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude Vid/Pid From Split set to o:vid-xxxx_pid-yyyy.</td>
<td>Any settings for Allow Auto Device Splitting and Exclude Vid/Pid From Split on View Client are overridden by View Agent.</td>
</tr>
<tr>
<td>Allow Auto Device Splitting set to Allow - Override Client Setting.</td>
<td></td>
</tr>
</tbody>
</table>

Allow Auto Device splitting for desktops and specify policies for splitting specified devices on client computers.

Table 8-20. Use View Agent and View Client Policies to Specify Device Splitting Policy Settings

<table>
<thead>
<tr>
<th>USB Splitting Policies on View Agent</th>
<th>USB Splitting Policies on View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Auto Device Splitting set to Allow - Override Client Setting.</td>
<td>The setting for Allow Auto Device Splitting on View Client is overridden by View Agent.</td>
</tr>
<tr>
<td></td>
<td>Split Vid/Pid Device set to vid-0781_pid-554c(exintf:00;exintf:01) to split a specified composite USB device and exclude interface 00 and interface 01 from redirection.</td>
</tr>
<tr>
<td></td>
<td>Note: You must also specify a filter policy such as Include Vid/Pid Device set to vid-0781_pid-554c, which allows View Client to redirect the other components of the device.</td>
</tr>
</tbody>
</table>

Configuring Filter Policy Settings for USB Devices

Filter policy settings that you configure for View Agent and View Client establish which USB devices can be redirected from a client computer to a desktop.

You can configure USB device filter policy settings in the policy settings for View Agent and View Client. When you connect to a desktop, View Client downloads the View Agent USB policy settings and uses them in conjunction with the View Client USB policy settings to decide which USB devices it will allow you to redirect from the client computer.

View applies any device splitting policy settings before it applies the filter policy settings. If you have split a composite USB device, View examines each of the device’s interfaces to decide which should be excluded or included according to the filter policy settings. If you have not split a composite USB device, View applies the filter policy settings to the entire device.

Table 8-21 shows the modifiers that specify how View Client handles a View Agent filter policy setting for an agent-enforceable setting if an equivalent filter policy setting exists for View Client.

Table 8-21. Filter Modifiers for Agent-Enforceable Settings

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>m (merge)</td>
<td>View Client applies the View Agent filter policy setting in addition to the View Client filter policy setting.</td>
</tr>
<tr>
<td>o (override)</td>
<td>View Client uses the View Agent filter policy setting instead of the View Client filter policy setting.</td>
</tr>
</tbody>
</table>

Table 8-22 shows examples of how View Client processes the settings for Exclude Vid/Pid Device when you specify different filter modifiers.
Table 8-22. Examples of Applying Filter Modifiers to Agent-Enforceable Settings

<table>
<thead>
<tr>
<th>Exclude Vid/Pid Device Setting on View Agent</th>
<th>Exclude Vid/Pid Device Setting on View Client</th>
<th>Effective Exclude Vid/Pid Device Policy Setting Used by View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>o:vid-0a34_pid-****</td>
<td>vid-0122_pid-5cce</td>
<td>vid-0a34_pid-****</td>
</tr>
<tr>
<td>m:vid-0a34_pid-****</td>
<td>vid-0122_pid-5cce</td>
<td>vid-0a34_pid-****;vid-0122_pid-5cce</td>
</tr>
</tbody>
</table>

Table 8-23 shows the modifiers that specify how View Client handles a View Agent filter policy setting for a client-interpreted setting.

Table 8-23. Filter Modifiers for Client-Interpreted Settings

<table>
<thead>
<tr>
<th>Modifier</th>
<th>Description</th>
</tr>
</thead>
</table>
| Default (d in the registry setting) | If a View Client filter policy setting does not exist, View Client uses the View Agent filter policy setting.  
If a View Client filter policy setting exists, View Client applies that policy setting and ignores the View Agent filter policy setting. |
| Override (o in the registry setting) | View Client uses the View Agent filter policy setting instead of any equivalent View Client filter policy setting. |

View Agent does not apply the filter policy settings for client-interpreted settings on its side of the connection.

Table 8-24 shows examples of how View Client processes the settings for Allow Smart Cards when you specify different filter modifiers.

Table 8-24. Examples of Applying Filter Modifiers to Client-Interpreted Settings

<table>
<thead>
<tr>
<th>Allow Smart Cards Setting on View Agent</th>
<th>Allow Smart Cards Setting on View Client</th>
<th>Effective Allow Smart Cards Policy Setting Used by View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable – Default Client Setting (d:false in the registry setting)</td>
<td>true (Allow)</td>
<td>true (Allow)</td>
</tr>
<tr>
<td>Disable – Override Client Setting (o:false in the registry setting)</td>
<td>true (Allow)</td>
<td>false (Disable)</td>
</tr>
</tbody>
</table>

If you set the Disable Remote Configuration Download policy to true, View Client ignores any filter policy settings that it receives from View Agent.

View Agent always applies the filter policy settings in agent-enforceable settings on its side of the connection even if you configure View Client to use a different filter policy setting or disable View Client from downloading filter policy settings from View Agent. View Client does not report that View Agent is blocking a device from being forwarded.

If you set the Exclude All Devices policy to true, View Client prevents all USB devices from being redirected. You can use other policy settings to allow specific devices or families of devices to be redirected. If you set the policy to false, View Client allows all USB devices to be redirected except those that are blocked by other policy settings. You can set the policy on both View Agent and View Client. Table 8-25 shows how the Exclude All Devices policy that you can set for View Agent and View Client combine to produce an effective policy for the client computer. By default, all USB devices are allowed to be redirected unless otherwise blocked.
Table 8-25. Effect of Combining Exclude All Devices Policies

<table>
<thead>
<tr>
<th>Exclude All Devices Policy on View Agent</th>
<th>Exclude All Devices Policy on View Client</th>
<th>Combined Effective Exclude All Devices Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>false or not defined (include all USB devices)</td>
<td>false or not defined (include all USB devices)</td>
<td>Include all USB devices</td>
</tr>
<tr>
<td>false (include all USB devices)</td>
<td>true (exclude all USB devices)</td>
<td>Exclude all USB devices</td>
</tr>
<tr>
<td>true (exclude all USB devices)</td>
<td>Any or not defined</td>
<td>Exclude all USB devices</td>
</tr>
</tbody>
</table>

If you have set Disable Remote Configuration Download policy to true, the value of Exclude All Devices on View Agent is not passed to View Client, but View Agent and View Client enforce the local value of Exclude All Devices.

View Client evaluates the filter policy settings according to an order of precedence. A filter policy setting that excludes a matching device from being redirected takes precedence over the equivalent filter policy setting that includes the device. If View Client does not encounter a filter policy setting to exclude a device, View Client allows the device to be redirected unless you have set the Exclude All Devices policy to true. However, if you have configured a filter policy setting on View Agent to exclude the device, the desktop blocks any attempt to redirect the device to it.

View Client evaluates the filter policy settings in the following order of precedence taking into account the View Client settings and the View Agent settings together with the modifier values that you apply to the View Agent settings.

- Exclude Path
- Include Path
- Exclude Vid/Pid Device
- Include Vid/Pid Device
- Exclude Device Family
- Include Device Family
- Allow Audio Input Devices, Allow Audio Output Devices, Allow HIDBootable, Allow HID (Non Bootable and Not Mouse Keyboard), Allow Keyboard and Mouse Devices, Allow Smart Cards, and Allow Video Devices
- Combined effective Exclude All Devices policy evaluated to exclude or include all USB devices

You can set Exclude Path and Include Path filter policy settings only for View Client. The Allow filter policy settings that refer to separate device families have equal precedence.

If you configure a policy setting to exclude devices based on vendor and product ID values, View Client excludes a device whose vendor and product ID values match this policy setting even though you might have configured an Allow policy setting for the family to which the device belongs.

The order of precedence for policy settings resolves conflicts between policy settings. If you configure Allow Smart Cards to allow the redirection of smart cards, any higher precedence exclusion policy setting overrides this policy. For example, you might have configured an Exclude Vid/Pid Device policy setting to exclude smart-card devices with matching path or vendor and product ID values, or you might have configured an Exclude Device Family policy setting that also excludes the smart-card device family entirely.

If you have configured any View Agent filter policy settings, View Agent evaluates and enforces the filter policy settings in the following order of precedence on the desktop.

- Exclude Vid/Pid Device
- Include Vid/Pid Device
- Exclude Device Family
include device family

agent-enforced exclude all devices policy set to exclude or include all USB devices

view agent enforces this limited set of filter policy settings on its side of the connection.

by defining filter policy settings for view agent, you can create a filtering policy for non-managed client computers. the feature also allows you to block devices from being forwarded from client computers, even if the filter policy settings for view client permit the redirection.

for example, if you configure a policy that permits view client to allow a device to be redirected, view agent blocks the device if you configure a policy for view agent to exclude the device.

examples of setting policies to filter USB devices

restrict desktops so that they allow client computers to forward only storage devices.

Table 8-26. Block All USB Devices except Storage Devices

<table>
<thead>
<tr>
<th>USB Filtering Policies on View Agent</th>
<th>USB Filtering Policies on View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Device Family set to o:storage.</td>
<td>Any setting of Include Device Family or Exclude All Devices on View Client is overridden.</td>
</tr>
<tr>
<td>Exclude All Devices set to true.</td>
<td></td>
</tr>
</tbody>
</table>

restrict desktops so that they allow client computers to forward only those devices with vendor and product ID values that match a specified pattern.

Table 8-27. Block All USB Devices except Devices with Specified Vendor and Product ID Values

<table>
<thead>
<tr>
<th>USB Filtering Policies on View Agent</th>
<th>USB Filtering Policies on View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Vid/Pid Device set to o:vid-0561_pid-554c;vid-0781_pid-****. Exclude All Devices set to true.</td>
<td>Any setting of Include Vid/Pid Device or Exclude All Devices on View Client is overridden.</td>
</tr>
</tbody>
</table>

allow client computers to redirect any devices except smart cards and HID-bootable devices.

Table 8-28. Allow All USB Devices To Be Redirected Except Smart Cards and HID-bootable devices

<table>
<thead>
<tr>
<th>USB Policies on View Agent</th>
<th>USB Policies on View Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude All Devices set to false.</td>
<td>Allow Smartcard set to false.</td>
</tr>
<tr>
<td>Allow HIDBootable set to false.</td>
<td></td>
</tr>
</tbody>
</table>

USB Device Families

You can specify a family when you are creating USB filtering rules for view client or view agent.

Table 8-29. USB Device Families

<table>
<thead>
<tr>
<th>Device Family Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audio</td>
<td>Any audio-input or audio-output device.</td>
</tr>
<tr>
<td>audio-in</td>
<td>Audio-input devices such as microphones.</td>
</tr>
<tr>
<td>audio-out</td>
<td>Audio-output devices such as loudspeakers and headphones.</td>
</tr>
<tr>
<td>bluetooth</td>
<td>Bluetooth-connected devices.</td>
</tr>
<tr>
<td>comm</td>
<td>Communications devices such as modems and wired networking adapters.</td>
</tr>
<tr>
<td>hid</td>
<td>Human interface devices excluding keyboards and pointing devices.</td>
</tr>
<tr>
<td>hid-bootable</td>
<td>Human interface devices that are available at boot time excluding keyboards and pointing devices.</td>
</tr>
<tr>
<td>imaging</td>
<td>Imaging devices such as scanners.</td>
</tr>
</tbody>
</table>
Table 8-29. USB Device Families (Continued)

<table>
<thead>
<tr>
<th>Device Family Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyboard</td>
<td>Keyboard device.</td>
</tr>
<tr>
<td>mouse</td>
<td>Pointing device such as a mouse.</td>
</tr>
<tr>
<td>other</td>
<td>Family not specified.</td>
</tr>
<tr>
<td>pda</td>
<td>Personal digital assistants.</td>
</tr>
<tr>
<td>physical</td>
<td>Force feedback devices such as force feedback joysticks.</td>
</tr>
<tr>
<td>printer</td>
<td>Printing devices.</td>
</tr>
<tr>
<td>security</td>
<td>Security devices such as fingerprint readers.</td>
</tr>
<tr>
<td>smart-card</td>
<td>Smart-card devices.</td>
</tr>
<tr>
<td>storage</td>
<td>Mass storage devices such as flash drives and external hard disk drives.</td>
</tr>
<tr>
<td>unknown</td>
<td>Family not known.</td>
</tr>
<tr>
<td>vendor</td>
<td>Devices with vendor-specific functions.</td>
</tr>
<tr>
<td>video</td>
<td>Video-input devices.</td>
</tr>
<tr>
<td>wireless</td>
<td>Wireless networking adapters.</td>
</tr>
<tr>
<td>wusb</td>
<td>Wireless USB devices.</td>
</tr>
</tbody>
</table>

**Note**: In releases before View 5.1, View Client for Windows read the device family from the device driver that you installed on the client computer. In View 5.1, you do not need to install the device driver on a Windows client computer. View Client reads the device family from the device itself, and not from the device driver. The firmware on a USB device usually defines the family of the device that describes its intended functionality, although not all devices specify the correct value for the family.

Linux-based thin clients have always read the device family from the device itself.

**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 8-30 describes each policy setting in the View Server Configuration ADM template file. The template contains only Computer Configuration settings.

Table 8-30. View Server Configuration Template Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recursive Enumeration of Trusted Domains</td>
<td>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.</td>
</tr>
</tbody>
</table>
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 8-31 describes the log configuration policy setting in the View Common Configuration ADM template file.

**Table 8-31. View Common Configuration Template: Log Configuration Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of days to keep production logs</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum number of debug logs</td>
<td>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.</td>
</tr>
<tr>
<td>Maximum debug log size in Megabytes</td>
<td>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.</td>
</tr>
<tr>
<td>Log Directory</td>
<td>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.</td>
</tr>
</tbody>
</table>

Performance Alarm Settings

Table 8-32 describe the performance alarm settings in the View Common Configuration ADM template file.

**Table 8-32. View Common Configuration Template: Performance Alarm Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU and Memory Sampling Interval in Seconds</td>
<td>Specifies the CPU and memory polling interval CPU. A low sampling interval can result in an high level of output to the log.</td>
</tr>
<tr>
<td>Overall CPU usage percentage to issue log info</td>
<td>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.</td>
</tr>
<tr>
<td>Overall memory usage percentage to issue log info</td>
<td>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.</td>
</tr>
<tr>
<td>Process CPU usage percentage to issue log info</td>
<td>Specifies the threshold at which the CPU usage of any individual process is logged.</td>
</tr>
</tbody>
</table>
Table 8-32. View Common Configuration Template: Performance Alarm Settings (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process memory usage percentage to issue log info</td>
<td>Specifies the threshold at which the memory usage of any individual process is logged.</td>
</tr>
</tbody>
</table>
| 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 8-33 describes the general settings in the View Common Configuration ADM template file.

Table 8-33. View Common Configuration Template: General Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk threshold for log and events in Megabytes</td>
<td>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.</td>
</tr>
<tr>
<td>Enable extended logging</td>
<td>Determines whether trace and debug events are included in the log files.</td>
</tr>
</tbody>
</table>

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-overrideable 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 208
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 214
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 216
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 217
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.

Table 8-34. View PCoIP General Session Variables

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure clipboard redirection</td>
<td>Determines the direction in which clipboard redirection is allowed. You can select one of these values:</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled client to server only</strong> (That is, allow copy and paste only from the client system to the View desktop.)</td>
</tr>
<tr>
<td></td>
<td><strong>Disabled in both directions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Enabled in both directions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Enabled server to client only</strong> (That is, allow copy and paste only from the View desktop to the client system.)</td>
</tr>
<tr>
<td>Controls clipboard redirection.</td>
<td>Clipboard redirection is implemented as a virtual channel. If virtual channels are disabled, clipboard redirection does not function.</td>
</tr>
<tr>
<td>This setting applies to View Agent only.</td>
<td>When this setting is disabled or not configured, the default value is <strong>Enabled client to server only</strong>.</td>
</tr>
<tr>
<td>Configure PCoIP client image cache</td>
<td>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.</td>
</tr>
<tr>
<td>size policy</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When this setting is not configured or disabled, PCoIP uses a default client image cache size of 250MB.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Configure PCoIP event log verbosity</td>
<td>Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose).</td>
</tr>
<tr>
<td></td>
<td>When this setting is enabled, you can set the verbosity level from 0 to 3. When the setting is not configured or disabled, the default event log verbosity level is 2.</td>
</tr>
<tr>
<td></td>
<td>When this setting is modified during an active PCoIP session, the new setting takes effect immediately.</td>
</tr>
</tbody>
</table>
### Table 8-34. View PCoIP General Session Variables (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure PCoIP image quality levels</td>
<td>Controls how PCoIP renders images during periods of network congestion. The <strong>Minimum Image Quality</strong>, <strong>Maximum Initial Image Quality</strong>, and <strong>Maximum Frame Rate</strong> values interoperate to provide fine control in network-bandwidth constrained environments. Use the <strong>Minimum Image Quality</strong> 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 <strong>Minimum Image Quality</strong> 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 <strong>Minimum Image Quality</strong> value cannot exceed the <strong>Maximum Initial Image Quality</strong> value. Use the <strong>Maximum Frame Rate</strong> 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.</td>
</tr>
<tr>
<td>Configure PCoIP session encryption algorithms</td>
<td>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 <strong>Disable AES-128-GCM encryption</strong> 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.</td>
</tr>
</tbody>
</table>
Table 8-34. View PCoIP General Session Variables (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure PCoIP USB allowed and unallowed device rules</td>
<td>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 (</td>
</tr>
<tr>
<td></td>
<td>For class rules, use one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>Allow all USB devices Format: 23XXXXXX Example: 23XXXXXX</td>
</tr>
<tr>
<td></td>
<td>Allow USB devices with a specific class ID Format: 22classXXXX Example: 22aaXXXX</td>
</tr>
<tr>
<td></td>
<td>Allow a specific subclass Format: 21class-subclassXX Example: 21aabbXX</td>
</tr>
<tr>
<td></td>
<td>Allow a specific protocol Format: 20class-subclass-protocol Example: 20aabbcc</td>
</tr>
<tr>
<td></td>
<td>For example, the USB authorization string to allow USB HID (mouse and keyboard) devices (class ID 0x03) and webcams (class ID 0xe) is 2203XXXX</td>
</tr>
<tr>
<td></td>
<td>Mass Storage devices (class ID 0x08) is 2288XXXX. 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 View Agent only and only when the View Agent desktop 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.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure PCoIP virtual channels</td>
<td>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 (</td>
</tr>
<tr>
<td>Configure the Client PCoIP UDP port</td>
<td>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.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Configure the PCoIP transport header | Configures the PCoIP transport header and sets the transport session priority. The PCoIP transport header is a 32-bit header that is added to all PCoIP UDP packets (only if the transport header is enabled and supported by both sides). The PCoIP transport header allows network devices to make better prioritization/QoS decisions when dealing with network congestion. The transport header is enabled by default. The transport session priority determines the PCoIP session priority reported in the PCoIP transport header. Network devices make better prioritization/QoS decisions based on the specified transport session priority. When the **Configure the PCoIP transport header** setting is enabled, the following transport session priorities are available:  
  - High  
  - Medium (default value)  
  - Low  
  - Undefined  
  The transport session priority value is negotiated by the PCoIP agent and client. If the PCoIP agent specifies a transport session priority value, the session uses the agent-specified session priority. If only the client has specified a transport session priority, the session uses the client-specified session priority. If neither agent nor client has specified a transport session priority, or **Undefined Priority** is specified, the session uses the default value, **Medium** priority. |
<p>| 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 View Agent 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 View Agent 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. |</p>
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable access to a PCoIP session from a vSphere console</td>
<td>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 View Agent 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.</td>
</tr>
<tr>
<td>Enable the FIPS 140-2 approved mode of operation</td>
<td>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.</td>
</tr>
<tr>
<td>Enable/disable audio in the PCoIP session</td>
<td>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.</td>
</tr>
<tr>
<td>Enable/disable microphone noise and DC offset filter in PCoIP session</td>
<td>Determines whether to enable the microphone noise and DC offset filter for microphone input during PCoIP sessions. This setting applies to View Agent 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.</td>
</tr>
<tr>
<td>Turn on PCoIP user default input language synchronization</td>
<td>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 View Agent only.</td>
</tr>
</tbody>
</table>
### View PCoIP Session Bandwidth Variables

The View PCoIP Session Variables ADM template file contains group policy settings that configure PCoIP session bandwidth characteristics.

#### Table 8-35. View PCoIP Session Bandwidth Variables

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the maximum PCoIP session bandwidth</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to View Agent and the client. If the two endpoints have different settings, the lower value is used.</td>
</tr>
<tr>
<td>Configure the PCoIP session bandwidth floor</td>
<td>Specifies a lower limit, in kilobits per second, for the bandwidth that is reserved by the PCoIP session.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to View Agent and the client. If the two endpoints have different settings, the setting only affects the endpoint on which it is configured.</td>
</tr>
<tr>
<td>Configure the PCoIP session MTU</td>
<td>Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>This setting applies to View Agent and the 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 View Agent.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure the PCoIP session audio bandwidth limit</td>
<td>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 View Agent 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.</td>
</tr>
<tr>
<td>Turn off Build-to-Lossless feature</td>
<td>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 217.</td>
</tr>
</tbody>
</table>
### 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 8-36. View PCoIP Session Variables for the Keyboard**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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 View Agent 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 View Agent 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 8-36. View PCoIP Session Variables for the Keyboard (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use alternate key for sending Secure Attention Sequence</td>
<td>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 View Agent only and has no effect on a client.</td>
</tr>
<tr>
<td>Use enhanced keyboard on Windows client if available</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 214.

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 218

   Before you can configure the group policy setting for location-based printing, you must register the DLL file TPVMGpocmap.dll.

2. **Configure the Location-Based Printing Group Policy** on page 219

   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 TPVMGpocmap.dll.

View provides 32-bit and 64-bit versions of TPVMGpocmap.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 218.
- 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 220.
- 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 223 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 the Active Directory server, edit the GPO.

   **AD Version Navigation Path**

   **Windows 2003**
   
   a. Select Start > All Programs > Administrative Tools > Active Directory Users and Computers.
   b. Right-click the OU that contains your View desktops and select Properties.
   c. On the Group Policy tab, click Open to open the Group Policy Management plug-in.
   d. In the right pane, right-click the GPO that you created for the location-based printing group policy setting and select Edit.

   **Windows 2008**
   
   b. Expand your domain, 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.

2. Expand Computer Configuration, open the Software Settings folder, and select AutoConnect Map Additional Printers for VMware View.

3. In the Policy pane, double-click Configure AutoConnect Map Additional Printers.

   The AutoConnect Map Additional Printers for VMware View window appears.
4 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.

5 Add the printers that you want to map to View desktops and define their associated translation rules.

6 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 8-37 describes the syntax of the translation table.

**Table 8-37. Translation Table Columns and Values**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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. |
Table 8-37. Translation Table Columns and Values (Continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Port/ThinPrint Port</td>
<td>For network printers, the IP address of the printer prepended with IP_.</td>
</tr>
<tr>
<td></td>
<td>For example: IP_10.114.24.1</td>
</tr>
<tr>
<td>Default</td>
<td>Indicates whether the printer is the default printer.</td>
</tr>
</tbody>
</table>

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 8-38 shows an example of two translation table rows.

Table 8-38. Location-Based Printing Group Policy Setting Example

<table>
<thead>
<tr>
<th>IP Range</th>
<th>Client Name</th>
<th>Mac Address</th>
<th>User/ Group</th>
<th>Printer Name</th>
<th>Printer Driver</th>
<th>IP Port/ThinPrint Port</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>* * * *</td>
<td>* * *</td>
<td>*</td>
<td>*</td>
<td>PRINTER-1-CLR</td>
<td>HP Color LaserJet 4700 PS</td>
<td>IP_10.114.24.1</td>
<td></td>
</tr>
<tr>
<td>10.112.116.140-10.12.116.145</td>
<td>* * *</td>
<td>*</td>
<td>*</td>
<td>PRINTER-2-CLR</td>
<td>HP Color LaserJet 4700 PS</td>
<td>IP_10.114.24.2</td>
<td>X</td>
</tr>
</tbody>
</table>

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 8-39** describes the Computer Configuration Terminal Services group policy settings that you can use to manage View desktops.
### Table 8-39. General Terminal Services Policy Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enforce Removal of Remote Desktop Wallpaper</td>
<td>Enabling this setting enforces the removal of wallpaper during a remote session, enhancing the user experience over low-bandwidth connections.</td>
</tr>
<tr>
<td>Limit maximum color depth</td>
<td>Enabling this setting lets you specify the color depth of View desktop sessions.</td>
</tr>
<tr>
<td>Allow users to connect remotely using Terminal Services</td>
<td>Enabling this setting allows users to connect remotely to the target computer.</td>
</tr>
<tr>
<td>Remove Windows Security item from Start Menu</td>
<td>Disabling this setting makes the Windows Security item appear in the Settings menu, ensuring that users have a logoff mechanism.</td>
</tr>
<tr>
<td>Remove Disconnect option from Shut Down dialog</td>
<td>Enabling this setting removes the Disconnect option from the Shut Down Windows dialog box, reducing the possibility of users disconnecting instead of logging off.</td>
</tr>
</tbody>
</table>

### Terminal Services Group Policy Settings for Sessions

Terminal Services group policy settings for sessions include settings that control disconnected and idle client sessions.

**Table 8-40** 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>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set time limit for disconnected sessions</td>
<td>Enabling this setting lets you set a time limit for disconnected sessions. Disconnected sessions are logged off after the specified time limit.</td>
</tr>
<tr>
<td>Sets a time limit for active but idle Terminal Services sessions</td>
<td>Enabling this setting lets you set a time limit for idle sessions. Idle sessions are logged off after the specified time limit.</td>
</tr>
</tbody>
</table>

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 223

   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.
Create GPOs for View Group Policies on page 223
Create GPOs to contain group policies for View components and location-based printing and link them to the OU for your View desktops.

Add View ADM Templates to a GPO on page 224
To apply View component group policy settings to your View desktops, add their ADM template files to GPOs.

Enable Loopback Processing for View Desktops on page 225
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
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 the Active Directory server, navigate to the OU and open the GPO editor.

<table>
<thead>
<tr>
<th>AD Version</th>
<th>Navigation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows 2003</strong></td>
<td>a) Select Start &gt; All Programs &gt; Administrative Tools &gt; Active Directory Users and Computers.&lt;br&gt;b) Right-click the OU that contains your View desktops and select Properties.&lt;br&gt;c) On the Group Policy tab, click Open to open the Group Policy Management plug-in.&lt;br&gt;d) Right-click the OU and select Create and Link a GPO Here.</td>
</tr>
<tr>
<td><strong>Windows 2008</strong></td>
<td>a) Select Start &gt; Administrative Tools &gt; Group Policy Management.&lt;br&gt;b) Expand your domain, right-click the OU that contains your View desktops and select Create and Link a GPO Here.</td>
</tr>
</tbody>
</table>

2. Type a name for the GPO and click OK.

   The new GPO appears under the OU in the left pane.

3. (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 the Active Directory server, edit the GPO.

<table>
<thead>
<tr>
<th>AD Version</th>
<th>Navigation Path</th>
</tr>
</thead>
</table>
| Windows 2003 | a Select Start > All Programs > Administrative Tools > Active Directory Users and Computers.  
|             | b Right-click the OU that contains your View desktops and select Properties.  
|             | c On the Group Policy tab, click Open to open the Group Policy Management plug-in.  
|             | d In the right pane, right-click the GPO that you created for the group policy settings and select Edit.  
| Windows 2008 | a Select Start > Administrative Tools > Group Policy Management.  
|             | b Expand your domain, right-click the GPO that you created for the group policy settings and select Edit.  

The Group Policy Object Editor window appears.

3 In the Group Policy Object Editor, right-click Administrative Templates under Computer Configuration and then select Add/Remove Templates.

4 Click Add, browse to the ADM Template file, and click Open.

5 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.

6 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 the Active Directory server, edit the GPO.

<table>
<thead>
<tr>
<th>AD Version</th>
<th>Navigation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b. Right-click the OU that contains your View desktops and select Properties.</td>
</tr>
<tr>
<td></td>
<td>c. On the Group Policy tab, click Open to open the Group Policy Management plug-in.</td>
</tr>
<tr>
<td></td>
<td>d. In the right pane, right-pane, right-click the GPO that you created for the group policy settings and select Edit.</td>
</tr>
</tbody>
</table>

Windows 2008

<table>
<thead>
<tr>
<th>AD Version</th>
<th>Navigation Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>b. Expand your domain, right pane, right-click the GPO that you created for the group policy settings and select Edit.</td>
</tr>
</tbody>
</table>

The Group Policy Object Editor window appears.

2. Expand the Computer Configuration folder and then expand the Administrative Templates, System, and Group Policy folders.

3. In the right pane, right-click User Group Policy loopback processing mode and select Properties.

4. On the Setting tab, select Enabled and then select a loopback processing mode from the Mode drop-down menu.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merge</td>
<td>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.</td>
</tr>
<tr>
<td>Replace</td>
<td>The user policy is defined entirely from the GPOs associated with the computer. Any GPOs associated with the user are ignored.</td>
</tr>
</tbody>
</table>

5. Click OK to save your changes.
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, but does not require Windows roaming profiles to operate.

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,” on page 227
- “Using View Persona Management with Standalone Systems,” on page 228
- “Migrating User Profiles with View Persona Management,” on page 229
- “Persona Management and Windows Roaming Profiles,” on page 231
- “Configuring a View Persona Management Deployment,” on page 232
- “Best Practices for Configuring a View Persona Management Deployment,” on page 240
- “View Persona Management Group Policy Settings,” on page 243

**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.

**Using View Persona Management with Standalone Systems**

You can install a standalone version of View Persona Management on physical computers and virtual machines that are not managed by View. With this software, you can manage user profiles across View desktops and standalone systems.

The standalone View Persona Management software operates on Windows XP SP3, Windows Vista, Windows 7, and Windows 8 operating systems.

You can use the standalone View Persona Management software to accomplish these goals:

- Share user profiles across standalone systems and View desktops.
  
  Your users can continue to use standalone systems as well as View desktops with View Persona Management. If you use the same View Persona Management group policy settings to control View desktops and physical systems, users can receive their up-to-date profiles each time they log in, whether they use their legacy computers or View desktops.

  **Note** View Persona Management does not support concurrent active sessions. A user must log out of one session before logging in to another.

- Migrate user profiles from physical systems to View desktops
  
  If you intend to re-purpose legacy physical computers for use in a View deployment, you can install standalone View Persona Management on the legacy systems before you roll out View desktops to your users. When users log in to their legacy systems, their profiles are stored on the View remote profile repository. When users log in to their View desktops for the first time, their existing profiles are downloaded to their View desktops.

- Perform a staged migration from physical systems to View desktops
  
  If you migrate your deployment in stages, users who do not yet have access to View desktops can use standalone View Persona Management. As each set of View desktops is deployed, users can access their profiles on their View desktops, and the legacy systems can be phased out. This scenario is a hybrid of the previous scenarios.

- Support up-to-date profiles when users go offline.
  
  Users of standalone laptops can disconnect from the network. When a user reconnects, View Persona Management uploads the latest changes in the user's local profile to the remote profile repository.

  **Note** Before a user can go offline, the user profile must be completely downloaded to the local system.
Migrating User Profiles with View Persona Management

With View Persona Management, you can migrate existing user profiles in a variety of settings to View desktops. When users log in to their View desktops after a profile migration is complete, they are presented with the personal settings and data that they used on their legacy systems.

By migrating user profiles, you can accomplish the following desktop migration goals:

- You can upgrade your users' systems from Windows XP to Windows 7 or Windows 8 and migrate your users from physical computers to View for the first time.
- In an existing View deployment, you can upgrade from Windows XP View desktops to Windows 7 or Windows 8 View desktops.
- You can migrate from physical computers to View desktops without upgrading the operating systems.

To support these scenarios, View Persona Management provides a profile migration utility and a standalone View Persona Management installer for physical or virtual machines that do not have View Agent 5.x installed. Table 9-1 shows various migration scenarios and outlines the tasks you should perform in each scenario.
<table>
<thead>
<tr>
<th>If This Is Your Original Deployment...</th>
<th>And This Is Your Destination Deployment...</th>
<th>Perform These Tasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP physical computers</td>
<td>Windows 7 View desktops or</td>
<td>1 Configure Windows 7 or Windows 8 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 232. <strong>Note</strong>: Do not roll out the Windows 7 or Windows 8 View desktops to your users until you complete step 2.</td>
</tr>
</tbody>
</table>
|                                      | Windows 8 View desktops                  | 2 Run the View V1 to V2 profile migration utility.  
|                                       |                                          |   - For the source profiles, specify the local profiles on the Windows XP physical computers.  
|                                       |                                          |   - For the destination profiles, specify the remote profile repository that you configured for the View deployment.  
|                                       |                                          | For details, see the VMware Horizon View User Profile Migration document.  
|                                       |                                          | 3 Allow your users to log in to their Windows 7 or Windows 8 View desktops.  |

Windows XP physical computers or virtual machines that use a roaming user profile solution. For example, your deployment might use one of these solutions:  
- View Persona Management  
- RTO Virtual Profiles  
- Windows roaming profiles  
In this scenario, the original user profiles must be maintained in a remote profile repository.  

| Windows XP physical computers         | Windows 7 View desktops or               | 1 Configure Windows 7 or Windows 8 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 232. **Note**: Do not roll out the Windows 7 or Windows 8 View desktops to your users until you complete step 2. |
|                                      | Windows 8 View desktops                  | 2 Run the View V1 to V2 profile migration utility.  
|                                       |                                          |   - For the source profiles, specify the remote profile repository for the Windows XP systems.  
|                                       |                                          |   - For the destination profiles, specify the remote profile repository that you configured for the View deployment.  
|                                       |                                          | For details, see the VMware Horizon View User Profile Migration document.  
|                                       |                                          | 3 Allow your users to log in to their Windows 7 View desktops.  |
Table 9-1. User Profile Migration Scenarios (Continued)

<table>
<thead>
<tr>
<th>If This Is Your Original Deployment...</th>
<th>And This Is Your Destination Deployment...</th>
<th>Perform These Tasks:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP physical computers or virtual machines. The legacy systems cannot have View Agent 5.x installed.</td>
<td>Windows XP View desktops</td>
<td>1 Configure Windows XP View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 232.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Install the standalone View Persona Management software on the Windows XP systems. See “Install Standalone View Persona Management,” on page 235.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Configure the legacy Windows XP systems to use the same remote profile repository as the View desktops. See “Configure a User Profile Repository,” on page 232.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The easiest approach is to use the same View Persona Management group policy settings in Active Directory to control both the legacy systems and the View desktops. See “Add the View Persona Management ADM Template File,” on page 236.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Roll out your Windows XP View desktops to your users.</td>
</tr>
<tr>
<td>Windows 7 or Windows 8 physical computers or virtual machines. The legacy systems cannot have View Agent 5.x installed.</td>
<td>Windows 7 View desktops or Windows 8 View desktops</td>
<td>1 Configure Windows 7 or Windows 8 View desktops with View Persona Management for your users. See “Configuring a View Persona Management Deployment,” on page 232.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Install the standalone View Persona Management software on the Windows 7 or Windows 8 systems. See “Install Standalone View Persona Management,” on page 235.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Configure the legacy Windows 7 or Windows 8 systems to use the same remote profile repository as the View desktops. See “Configure a User Profile Repository,” on page 232.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The easiest approach is to use the same View Persona Management group policy settings in Active Directory to control both the legacy systems and the View desktops. See “Add the View Persona Management ADM Template File,” on page 236.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Roll out your Windows 7 or Windows 8 View desktops to your users.</td>
</tr>
</tbody>
</table>

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, and configure View Persona Management group policy settings, and deploy desktop pools.

You can also configure View Persona Management for a non-View deployment. You install the standalone version of View Persona Management on your users' non-View laptops, desktops, or virtual machines. You must also set up a remote repository and configure View Persona Management group policy settings.

Overview of Setting Up a View Persona Management Deployment

To set up a View desktop deployment or standalone computers 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.

   To configure View Persona Management for non-View laptops, desktops, or virtual machines, install the standalone View Persona Management software on each computer in your targeted deployment.

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 or non-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 233.

Procedure

1. Determine whether to use an existing Active Directory user profile path or configure a user profile repository on a network share.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use an existing Active Directory user profile path</td>
<td>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.</td>
</tr>
<tr>
<td>Configure a network share to store the user profile repository</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.


   The Security Recommendations for Roaming User Profiles Shared Folders topic lists the following minimum permissions for the security group of users needing to put data on the share: List Folder/Read Data and Create Folders/Append Data - This Folder Only.

   To successfully add the %username%.%userdomain% folder to the network share, you also must configure the Read Attributes permission.

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.

- If you use Windows 8 desktops and your network share uses a OneFS file system on an EMC Isilon NAS device, the OneFS file system must be version 6.5.5.11 or later.
- 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 8 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.

You can use the View profile migration command-line utility to migrate Windows XP profiles to Windows 7 or Windows 8 profiles. See the VMware Horizon View User Profile Migration document.

### Prerequisites

- Verify that you are performing the installation on a Windows 8, Windows 7, Windows Vista, or Windows XP virtual machine. View Persona Management does not operate on Microsoft Terminal Servers.

  Installing View Agent with the View Persona Management setup option does not work on physical computers. You can install the standalone View Persona Management software on physical computers. See “Install Standalone View Persona Management,” on page 235.

- 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 235.

- Familiarize yourself with installing View Agent. See “Install View Agent on a Virtual Machine,” on page 64 or “Install View Agent on an Unmanaged Desktop Source,” on page 55.

### 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 236.

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.


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.

Install Standalone View Persona Management

To use View Persona Management with non-View physical computers or virtual machines, install the standalone version of View Persona Management.

Install the standalone View Persona Management software on each individual computer or virtual machine in your targeted deployment.

Prerequisites

- Verify that you are performing the installation on a Windows 8, Windows 7, Windows Vista, or Windows XP SP3 physical computer or virtual machine. View Persona Management does not operate on Windows Servers or Microsoft Terminal Servers. Verify that the system satisfies the requirements described in XX.
- Verify that you can log in as an administrator on the system.
- Verify that View Agent 5.x or later is not installed on the computer.
- Verify that a native RTO Virtual Profiles 2.0 is not installed on the virtual machine.

Procedure

   The installer filename is VMware-personamanagement-y.y.y-xxxxxx.exe or VMware-viewagent-x86_64-y.y.y-xxxxxx.exe, where y.y.y is the version number and xxxxx is the build number.
2. To start the installation program, double-click the installer file.
3. Accept the VMware license terms.
4. Click Install.
   By default, View Persona Management is installed in the C:\Program Files\VMware\VMware View Persona Management directory.
5. Click Finish.
6. Restart your system to allow the installation changes to take effect.
What to do next

Add the View Persona Management ADM Template file to your Active Directory or local group policy configuration.

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 systems or Active Directory server.

To configure View Persona Management on a single system, 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 example, you might create one OU for View desktops with View Persona Management and another OU for physical computers on which the standalone View Persona Management software is installed.

For an example of implementing Active Directory group policies in View, see “Active Directory Group Policy Example,” on page 222.

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 234.
- 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.
Browse to the directory that contains the ADM Template file, ViewPM.adm.

<table>
<thead>
<tr>
<th>Installation Type</th>
<th>Directory</th>
</tr>
</thead>
</table>
| View Agent with the View Persona Management setup option | install_directory\VMware\VMware View\Agent\bin
The ViewPM.adm file is also installed with the other View ADM Template files in the install_directory\VMware View\Server\extras\GroupPolicyFiles directory on the View Connection Server host. |
| Standalone View Persona Management                     | install_directory\VMware\VMware View Persona Management                                      |

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 gedit.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 238.

**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 222.
- 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 234.

**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.
   
   If standalone View Persona Management is installed on a non-View system, the ViewPM.adm file is located in the install_directory\VMware\VMware View Persona Management directory.

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 244.
- 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 236.
- 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 237.

Procedure

1 Open the Group Policy window.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local system</td>
<td>Open the Local Computer Policy window.</td>
</tr>
<tr>
<td>Active Directory server</td>
<td>Open the Group Policy Object Editor window.</td>
</tr>
</tbody>
</table>

2 Expand the Computer Configuration folder and navigate to the Persona Management folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP or Windows Server 2003</td>
<td>Expand the following folders: Administrative Templates, VMware View Agent Configuration, Persona Management</td>
</tr>
<tr>
<td>Windows Vista and later or Windows Server 2008 and later</td>
<td>Expand the following folders: Administrative Templates, Classic Administrative Templates (ADM), VMware View Agent Configuration, Persona Management</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the network share.</td>
<td>Check the Override Active Directory user profile path if it is configured check box.</td>
</tr>
<tr>
<td>Use an Active Directory user profile path, if one exists.</td>
<td>Do not check the Override Active Directory user profile path if it is configured check box.</td>
</tr>
</tbody>
</table>

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 cannot use View Persona Management on 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 234.

- 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 236 and “Configure View Persona Management Policies,” on page 238.

**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.
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 J Doe sees a folder named J Doe 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 241.

- 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 242.

- If you configure View Persona Management for standalone laptops, make sure that the profiles are kept synchronized when users go offline. See “Manage User Profiles on Standalone Laptops,” on page 242.

**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 244.

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.

Manage User Profiles on Standalone Laptops

If you install View Persona Management on standalone (non-View) laptops, make sure that the user profiles are kept synchronized when users take their standalone laptops offline.

To ensure that a standalone laptop user has an up-to-date local profile, you can configure the View Persona Management group policy setting, Enable background download for laptops. This setting downloads the entire user profile to the standalone laptop in the background.

As a best practice, notify your users to make sure that their user profiles are completely downloaded before they disconnect from the network. Tell users to wait for the Background download complete notice to appear on their laptop screens before they disconnect.

To allow the Background download complete notice to be displayed on user laptops, configure the View Persona Management group policy setting, Show critical errors to users via tray icon alerts.

If a user disconnects from the network before the profile download is complete, the local profile and remote profile might become unsynchronized. While the user is offline, the user might update a local file that was not fully downloaded. When the user reconnects to the network, the local profile is uploaded, overwriting the remote profile. Data that was in the original remote profile might be lost.

The following steps provide an example you might follow.

Prerequisites

Verify that View Persona Management is configured for your users’ standalone laptops. See “Configuring a View Persona Management Deployment,” on page 232.

Procedure

1. In the Active Directory OU that controls your standalone laptops, enable the Enable background download for laptops setting.

   In the Group Policy Object Editor, expand the following folders: Computer Configuration, Administrative Templates, Classic Administrative Templates (ADM), VMware View Agent Configuration, Persona Management, Roaming & Synchronization.

   The Classic Administrative Templates (ADM) folder appears only in Windows Vista or later and Windows Server 2008 or later releases.
For standalone laptops, you must use a non-View method to notify users when they log in.

For example, you might distribute this message:

Your personal data is dynamically downloaded to your laptop after you log in. Make sure your personal data has finished downloading before you disconnect your laptop from the network. A "Background download complete" notice pops up when your personal data finishes downloading.

**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.

When you install standalone View Persona Management on a non-View system, the ViewPM.adm file is installed on the system in the install_directory\VMware\VMware View Persona Management 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 9-2. Location of View Persona Management Settings in the Group Policy Window**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Vista and later or Windows Server 2008 and later</td>
<td>Computer Configuration &gt; Administrative Templates &gt; Classic Administrative Templates (ADM) &gt; VMware View Agent Configuration &gt; Persona Management</td>
</tr>
<tr>
<td>Windows XP or Windows Server 2003</td>
<td>Computer Configuration &gt; Administrative Templates &gt; VMware View Agent Configuration &gt; Persona Management</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Group Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage user persona</td>
<td>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.</td>
</tr>
<tr>
<td>Persona repository location</td>
<td>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 232. 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.</td>
</tr>
<tr>
<td>Remove local persona at log off</td>
<td>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. When using Windows 8, Windows 7, or 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 240. When this setting is disabled or not configured, the locally stored user profiles, including local settings folders, are not deleted when users log off.</td>
</tr>
<tr>
<td>Roam local settings folders</td>
<td>Roams the local settings folders with the rest of each user profile. For Windows 8, 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.</td>
</tr>
<tr>
<td>Group Policy Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Files and folders to preload</td>
<td>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.</td>
</tr>
<tr>
<td>Files and folders to preload (exceptions)</td>
<td>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.</td>
</tr>
<tr>
<td>Windows roaming profiles synchronization</td>
<td>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.</td>
</tr>
<tr>
<td>Windows roaming profiles synchronization (exceptions)</td>
<td>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.</td>
</tr>
<tr>
<td>Files and folders excluded from roaming</td>
<td>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.</td>
</tr>
<tr>
<td>Files and folders excluded from roaming (exceptions)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable background download for laptops</td>
<td>Downloads all files in the user profile when a user logs in to a laptop on which the View Persona Management software is installed. Files are downloaded in the background. When the operation is complete, a pop-up notification appears on the user's screen: Background download complete. To allow this notification to appear on the user's laptop, you must enable the Show critical errors to users via tray icon alerts setting. Note: If you enable this setting, as a best practice, notify your users to make sure that the profile is completely downloaded before the users disconnect from the network. If a user takes a standalone laptop offline before the profile download is complete, the user might not have access to local profile files. While the user is offline, the user will be unable to open a local file that was not fully downloaded. See “Manage User Profiles on Standalone Laptops,” on page 242.</td>
</tr>
</tbody>
</table>
**Group Policy Setting** | **Description**
--- | ---
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.

Excluded processes | The I/O of the specified processes are ignored by View Persona Management. You might have to add certain anti-virus applications to the Excluded processes list to prevent performance problems. If an anti-virus application does not have a feature to disable offline file retrieval during its on-demand scans, the Excluded processes setting prevents the application from retrieving files unnecessarily. However, View Persona Management does replicate changes to files and settings in the users’ profiles that are made by excluded processes.

To add processes to the Excluded processes list, enable this setting, click Show, type the process name, and click OK. For example: process.exe.

### 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 240.
- 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 specify folder paths that are excluded from folder redirection. See Table 9-3.

CAUTION View does not support enabling folder redirection to a folder that is already in a profile managed by View Persona Management. This configuration can cause failures in View Persona Management and loss of user data.

For example, if the root folder in the remote profile repository is \Server\%username\, and you redirect folders to \Server\%username%\Desktop, these settings would cause a failure of folder redirection in View Persona Management and the loss of any contents that were previously in the \Server\%username%\Desktop folder.

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.
### Table 9-3. Folders Excluded from Folder Redirection

<table>
<thead>
<tr>
<th>Group Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files and Folders excluded from Folder Redirection</td>
<td>The selected file and folder paths are not redirected to a network share. In some scenarios, specific files and folders must remain in the local user profile. To add a folder path to the Files and Folders excluded from Folder Redirection list, enable this setting, click Show, type the path name, and click OK. Specify folder paths that are relative to the root of the user’s local profile. For example: Desktop\New Folder.</td>
</tr>
<tr>
<td>Files and folders excluded from Folder Redirection (exceptions)</td>
<td>The selected file and folder paths are exceptions to the paths that are specified in the Files and Folders excluded from Folder Redirection setting. To add a folder path to the Files and folders excluded from Folder Redirection (exceptions) list, enable this setting, click Show, type the path name, and click OK. Specify folder paths that reside within a folder that is specified in the Folders excluded from Folder Redirection setting and are relative to the root of the user’s local profile. For example: Desktop\New Folder\Unique Folder.</td>
</tr>
</tbody>
</table>

### Desktop UI Group Policy Settings

The desktop UI group policy settings control View Persona Management settings that users see on their desktops.

<table>
<thead>
<tr>
<th>Group Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide local offline file icon</td>
<td>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.</td>
</tr>
<tr>
<td>Show progress when downloading large files</td>
<td>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.</td>
</tr>
<tr>
<td>Show critical errors to users via tray icon alerts</td>
<td>Displays critical error icon alerts in the desktop tray when replication or network connectivity failures occur. By default, these icon alerts are hidden.</td>
</tr>
</tbody>
</table>
## Logging Group Policy Settings

The logging group policy settings determine the name, location, and behavior of the View Persona Management log files.

<table>
<thead>
<tr>
<th>Group Policy Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging filename</td>
<td>Specifies the full pathname of the local View Persona Management log file. On Windows 8 and 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.</td>
</tr>
<tr>
<td>Logging destination</td>
<td>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.</td>
</tr>
<tr>
<td>Logging flags</td>
<td>Determines the types of messages to log. When this setting is configured, you can select any or all log message types to generate:</td>
</tr>
<tr>
<td></td>
<td>- Log error messages.</td>
</tr>
<tr>
<td></td>
<td>- Log information messages.</td>
</tr>
<tr>
<td></td>
<td>- Log debug messages.</td>
</tr>
<tr>
<td></td>
<td>By default, error and information log message types are generated.</td>
</tr>
<tr>
<td>Debug flags</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- Debug error messages</td>
</tr>
<tr>
<td></td>
<td>- Debug information messages</td>
</tr>
<tr>
<td></td>
<td>- Debug port messages</td>
</tr>
<tr>
<td></td>
<td>By default, no debug messages are generated.</td>
</tr>
</tbody>
</table>
Managing Linked-Clone Desktops

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 251**
  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 253**
  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 257**
  A desktop rebalance operation evenly redistributes linked-clone desktops among available datastores.

- **Manage View Composer Persistent Disks on page 260**
  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 252.

**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 you force users to log off, the maximum number of concurrent refresh operations on desktops that require logoffs is half the value of the Max concurrent View Composer maintenance operations setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent refresh operations on desktops that require logoffs is 12.

- 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.
   
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To refresh all desktops in the pool</td>
<td>On the selected pool’s page, click the Settings tab.</td>
</tr>
<tr>
<td>To refresh selected desktops</td>
<td>a On the selected pool’s page, click the Inventory tab.</td>
</tr>
<tr>
<td></td>
<td>b Select the desktops to refresh.</td>
</tr>
</tbody>
</table>

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.

If you use native NFS snapshot (VAAI) technology to generate linked clones, certain vendors’ NAS devices take snapshots of the replica disk when they refresh the linked clones’ OS disks. These NAS devices do not support taking direct snapshots of each clone’s OS disk.

You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the refresh operation. See “Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations,” on page 117.

**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 253
  
  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 254
  
  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 255
  
  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 256
  
  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 257
  
  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 8, 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 253.
- Familiarize yourself with the recomposition guidelines. See “Updating Linked Clones with Desktop Recomposition,” on page 256.
- 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.
  If you force users to log off, the maximum number of concurrent recompose operations on desktops that require logoffs is half the value of the Max concurrent View Composer maintenance operations setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent recompose operations on desktops that require logoffs is 12.
- 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To recompose all desktops in the pool</td>
<td>On the selected pool’s page, click the Settings tab.</td>
</tr>
</tbody>
</table>
| 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 106.

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 256.
- 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 253 and “Recompose Linked-Clone Desktops,” on page 254.
- 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 316.

**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 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.
You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the recompose operation. See “Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations,” on page 117.

**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 106.

### 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 or later 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. You can also use the rebalance operation to migrate linked-clone desktops to another datastore. Do not use vSphere Client or vCenter Server to migrate or manage linked-clone virtual machines. See “Migrate Linked-Clone Desktops to Another Datastore,” on page 259.

If possible, schedule rebalance operations during off-peak hours.

For guidelines, see “Rebalancing Linked Clones Among Logical Drives,” on page 258.

**Prerequisites**

- Familiarize yourself with the rebalance operation. See “Rebalancing Linked Clones Among Logical Drives,” on page 258.
- 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.

  If you force users to log off, the maximum number of concurrent rebalance operations on desktops that require logoffs is half the value of the Max concurrent View Composer maintenance operations setting. For example, if this setting is configured as 24 and you force users to log off, the maximum number of concurrent rebalance operations on desktops that require logoffs is 12.

- 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To rebalance all desktops in the pool</td>
<td>On the selected pool’s page, click the <strong>Settings</strong> tab.</td>
</tr>
</tbody>
</table>
| 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.

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.

You can set a minimum number of ready, provisioned desktops that remain available for users to connect to during the rebalance operation. See “Keeping Linked-Clone Desktops Provisioned and Ready During View Composer Operations,” on page 117.

Migrate Linked-Clone Desktops to Another Datastore

To migrate linked-clone virtual machines from one set of datastores to another, use the rebalance operation.

When you use rebalance, View Composer manages the movement of the linked clones between datastores. View Composer ensures that the linked clones' access to the replica is maintained during and after the rebalance operation. If necessary, View Composer creates an instance of the replica on the destination datastore.

**Note** Do not use vSphere Client or vCenter Server to migrate or manage linked clone virtual machines. Do not use Storage vMotion to migrate linked-clone virtual machines to other datastores.

**Prerequisites**

Familiarize yourself with the rebalance operation. See “Rebalance Linked-Clone Desktops,” on page 257 and “Rebalancing Linked Clones Among Logical Drives,” on page 258.

**Procedure**

1. In View Administrator, select the linked-clone pool you want to migrate and click **Edit**.
2. In the vCenter Settings tab, scroll down to **Datastores** and click **Browse**.
3. On the Select Linked Clone Datastores page, deselect the datastores that currently store the linked clones, select the destination datastores, and click **OK**.
4. In the Edit **pool name** window, click **OK**.
5. On the **pool name** page, click **View Composer > Rebalance**.
6. Follow the wizard instructions to rebalance the linked-clone desktops.

The linked-clone desktops are refreshed and migrated to the destination datastores.
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 92.

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 8, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use current datastore</td>
<td>Store the persistent disk on the datastore where it is currently located.</td>
</tr>
<tr>
<td>Use the following datastore</td>
<td>Select a new datastore on which to store the persistent disk. Click <strong>Browse</strong>, click the down arrow, and select a new datastore from the <strong>Choose a Datastore</strong> menu. You cannot select a local datastore to store a detached persistent disk. You must use a shared datastore.</td>
</tr>
</tbody>
</table>

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 262.

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.
   
   You cannot import a persistent disk from a local datastore. Only shared datastores are available.
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 262 and “Attach a View Composer Persistent Disk to Another Linked-Clone Desktop,” on page 261.

---

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Delete from disk</strong></td>
<td>After the deletion, the persistent disk no longer exists.</td>
</tr>
<tr>
<td><strong>Delete from View Manager only</strong></td>
<td>After the deletion, the persistent disk is no longer accessible in View Manager but remains on the datastore.</td>
</tr>
</tbody>
</table>

6 Click **OK**.
In View Administrator, you can manage desktop pools, virtual-machine desktops, and desktop sessions.

This chapter includes the following topics:

- “Managing Desktop Pools,” on page 265
- “Reducing Adobe Flash Bandwidth,” on page 271
- “Managing Virtual-Machine Desktops,” on page 272
- “Export View Information to External Files,” on page 278

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 266 and “Fixed Settings in an Existing Desktop Pool,” on page 266.

**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

<table>
<thead>
<tr>
<th>Configuration Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Edit pool-naming options.</td>
</tr>
<tr>
<td>Pool Settings</td>
<td>Edit desktop settings such as the remote desktop power policy, display protocol, and Adobe Flash settings.</td>
</tr>
<tr>
<td>Provisioning Settings</td>
<td>Edit pool-provisioning options and add desktops to the pool. This tab is available for automated pools only.</td>
</tr>
<tr>
<td>vCenter Settings</td>
<td>Edit the virtual machine template or default base image. Add or change the vCenter Server instance, ESXi host or cluster, datastores, and other vCenter features. The new values only affect 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.</td>
</tr>
<tr>
<td>Guest Customization</td>
<td>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.</td>
</tr>
<tr>
<td>Advanced Storage</td>
<td>Choose whether to use native NFS snapshots (VAAI) and host caching. If you select or deselect Use native NFS snapshots (VAAI), the new setting only affects virtual machines that are created after the settings are changed. You can change existing virtual machines to become native NFS snapshot clones by recomposing and, if needed, rebalancing the desktop pool. See “Using View Composer Array Integration with Native NFS Snapshot Technology (VAAI),” on page 114. If you select or deselect Use View Storage Accelerator, or reschedule when the View Storage Accelerator digest files are regenerated, the new settings do affect existing virtual machines. See “Configure View Storage Accelerator for Desktop Pools,” on page 145. Note: If you select Use View Storage Accelerator on an existing linked-clone pool, and the replica was not previously enabled for View Storage Accelerator, this feature might not take effect right away. View Storage Accelerator cannot be enabled while the replica is in use. You can force View Storage Accelerator to be enabled by recomposing the pool to a new parent virtual machine.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool type</td>
<td>After you create an automated, manual, or Terminal Services pool, you cannot change the pool type.</td>
</tr>
<tr>
<td>User assignment</td>
<td>You cannot switch between dedicated assignments and floating assignments.</td>
</tr>
</tbody>
</table>
Table 11-2. Fixed Settings in an Existing Desktop Pool (Continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of virtual machine</td>
<td>You cannot switch between full desktops and linked-clone desktops.</td>
</tr>
<tr>
<td>Pool ID</td>
<td>You cannot change the pool ID.</td>
</tr>
<tr>
<td>Desktop-naming and provisioning method</td>
<td>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.</td>
</tr>
<tr>
<td>vCenter settings</td>
<td>You cannot change vCenter settings for existing virtual machines. You can change vCenter settings in the <code>Editpool_name</code> dialog, but the values only affect new virtual machines that are created after the settings are changed.</td>
</tr>
<tr>
<td>View Composer persistent disks</td>
<td>You cannot configure persistent disks after a linked-clone pool is created without persistent disks.</td>
</tr>
<tr>
<td>View Composer customization method</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 268.
- 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 value that is specified in **Max number of desktops**.
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 !.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the pool</td>
<td>Click Status &gt; Disable Pool.</td>
</tr>
<tr>
<td>Enable the pool</td>
<td>Click Status &gt; Enable Pool.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable provisioning</td>
<td>Click Status &gt; Disable Provisioning.</td>
</tr>
<tr>
<td>Enable provisioning</td>
<td>Click Status &gt; Enable Provisioning.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pool that contains full virtual-machine desktops</td>
<td>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.</td>
</tr>
<tr>
<td>Linked-clone pool with View Composer persistent disks</td>
<td>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, the linked-clone desktop that contained the persistent disk can be recreated, or the persistent disk can be attached to another desktop. You can store detached persistent disks in the same datastore or a different one. If you select a different datastore, you cannot store detached persistent disks on a local datastore. You must use a shared datastore. You can only detach persistent disks that were created in View 4.5 or later releases.</td>
</tr>
<tr>
<td>Linked-clone pool without View Composer persistent disks</td>
<td>vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops.</td>
</tr>
</tbody>
</table>

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 271.

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

<table>
<thead>
<tr>
<th>Quality Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do not control</td>
<td>Quality is determined by Web page settings.</td>
</tr>
<tr>
<td>Low</td>
<td>This setting results in the most bandwidth savings.</td>
</tr>
<tr>
<td>Medium</td>
<td>This setting results in moderate bandwidth savings.</td>
</tr>
<tr>
<td>High</td>
<td>This setting results in the least bandwidth savings.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Throttling Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>No throttling is performed. The timer interval is not modified.</td>
</tr>
<tr>
<td>Conservative</td>
<td>Timer interval is 100 milliseconds. This setting results in the lowest number of dropped frames.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Timer interval is 500 milliseconds.</td>
</tr>
<tr>
<td>Aggressive</td>
<td>Timer interval is 2500 milliseconds. This setting results in the highest number of dropped frames.</td>
</tr>
</tbody>
</table>

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, Restart, or Send Messages to 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, restart active sessions, or send messages to users’ desktops.

**Procedure**

1. In View Administrator, click **Inventory > Pool**.
2. Double-click a pool and click the **Sessions** tab.
3 Select a desktop.

If you intend to send a message to users, you can select multiple desktops. You can perform the other operations on only one desktop at a time.

4 Choose whether to disconnect, log off, restart the session, or send a message.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect Session</td>
<td>Disconnects the user from the desktop. The session remains active. The user can log back in to the session if <strong>Automatically logoff after disconnect</strong> is set to <strong>Never</strong>, or the specified length of time after the disconnect occurs is not exceeded. You can configure the <strong>Automatically logoff after disconnect</strong> setting when the pool is created or edit the setting after the pool is created.</td>
</tr>
<tr>
<td>Logoff Session</td>
<td>Disconnects the user from the desktop. The user is logged off.</td>
</tr>
<tr>
<td>Reset</td>
<td>Shuts down the desktop and restarts the session without a graceful logoff and disconnection.</td>
</tr>
<tr>
<td>Send Message</td>
<td>Lets you type a message that is displayed on users’ desktops. You can select multiple desktops to receive the message. You can label the message as <strong>Info</strong>, <strong>Warning</strong>, or <strong>Error</strong>. The message is sent to all selected desktops in active sessions.</td>
</tr>
</tbody>
</table>

**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 `vdmadm` command to assign desktops to users. See “Assigning Dedicated Desktops Using the -L Option,” on page 418.

**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 418.

**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 131.

**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 275.
Procedure

1. In View Administrator, click Dashboard.

2. In the Desktop Status pane, expand a status folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing</td>
<td>Lists the desktop states while the virtual machine is being provisioned,</td>
</tr>
<tr>
<td></td>
<td>deleted, or in maintenance mode.</td>
</tr>
<tr>
<td>Problem Desktops</td>
<td>Lists the desktop error states.</td>
</tr>
<tr>
<td>Prepared for use</td>
<td>Lists the desktop states when the desktop is ready for use.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Status</th>
<th>Type of State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning</td>
<td>Provisioning</td>
<td>The virtual machine is being provisioned.</td>
</tr>
<tr>
<td>Provisioning error</td>
<td>Provisioning</td>
<td>An error occurred during provisioning.</td>
</tr>
<tr>
<td>Customizing</td>
<td>Provisioning</td>
<td>The virtual machine in an automated pool is being customized.</td>
</tr>
<tr>
<td>Deleting</td>
<td>Provisioning</td>
<td>The virtual machine is marked for deletion. View Manager will delete the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>virtual machine soon.</td>
</tr>
<tr>
<td>Maintenance mode</td>
<td>Provisioning</td>
<td>The virtual machine is in maintenance mode. Users cannot log in or use the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>virtual machine.</td>
</tr>
<tr>
<td>Waiting for Agent</td>
<td>Agent state</td>
<td>View Connection Server is waiting to establish communication with View</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Agent on a virtual machine in a manual pool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> This state is the same as the Customizing state for a virtual</td>
</tr>
<tr>
<td></td>
<td></td>
<td>machine in an automated pool.</td>
</tr>
<tr>
<td>Startup</td>
<td>Agent state</td>
<td>View Agent has started on the virtual machine, but other required services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>such as the display protocol are still starting. For example, View Agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cannot establish an RDP connection with client computers until RDP has</td>
</tr>
<tr>
<td></td>
<td></td>
<td>finished starting. View Agent startup period allows other processes such as</td>
</tr>
<tr>
<td></td>
<td></td>
<td>protocol services to start up as well.</td>
</tr>
<tr>
<td>Agent unreachable</td>
<td>Agent state</td>
<td>View Connection Server cannot establish communication with View Agent on a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>virtual machine.</td>
</tr>
<tr>
<td>Configuration error</td>
<td>Agent state</td>
<td>The display protocol such as RDP or PCoIP is not enabled.</td>
</tr>
</tbody>
</table>
## Table 11-5. Status of Virtual-Machine Desktops That Are Managed by vCenter Server (Continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Type of State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent disabled</td>
<td>Agent state</td>
<td>This state can occur in two cases. First, in a desktop pool with the <strong>Delete or refresh desktop on logoff</strong> or <strong>Delete desktop after logoff</strong> setting enabled, a desktop session is logged out, but the virtual machine is not yet refreshed or deleted. Second, View Connection Server disables View Agent just before sending a request to power off the virtual machine. This state ensures that a new desktop session cannot be started on the virtual machine.</td>
</tr>
<tr>
<td>Invalid IP</td>
<td>Agent state</td>
<td>The subnet mask registry setting is configured on the virtual machine, and no active network adapters have an IP address within the configured range.</td>
</tr>
<tr>
<td>Agent needs reboot</td>
<td>Agent state</td>
<td>A View component was upgraded, and the virtual machine must be restarted to allow View Agent to operate with the upgraded component.</td>
</tr>
<tr>
<td>Protocol failure</td>
<td>Agent state</td>
<td>A display protocol did not start before the View Agent startup period expired.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> View Administrator can display desktops in a <strong>Protocol failure</strong> state when one protocol failed but other protocols started successfully. For example, the <strong>Protocol failure</strong> state might be displayed when HTML Access failed but PCoIP and RDP are working. In this case, the desktops are available and View Client devices can access them through PCoIP or RDP.</td>
</tr>
<tr>
<td>Domain failure</td>
<td>Agent state</td>
<td>The virtual machine encountered a problem reaching the domain. The domain server was not accessible, or the domain authentication failed.</td>
</tr>
<tr>
<td>Provisioned</td>
<td>Availability</td>
<td>The virtual machine is powered off or suspended.</td>
</tr>
<tr>
<td>Available</td>
<td>Availability</td>
<td>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.</td>
</tr>
<tr>
<td>Checked out</td>
<td>Session state</td>
<td>The virtual machine for a local desktop is checked out.</td>
</tr>
<tr>
<td>Connected</td>
<td>Session state</td>
<td>The virtual machine is in an active session and has an active remote connection to a View client.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>Session state</td>
<td>The virtual machine is in an active session, but it is disconnected from the View client.</td>
</tr>
<tr>
<td>Unassigned user connected</td>
<td>Session state</td>
<td>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.</td>
</tr>
<tr>
<td>Unassigned user disconnected</td>
<td>Session state</td>
<td>A user other than the assigned user is logged in and disconnected from a virtual machine in a dedicated pool.</td>
</tr>
<tr>
<td>Already used</td>
<td>Session state</td>
<td>In a desktop pool with the <strong>Delete or refresh desktop on logoff</strong> or <strong>Delete desktop after logoff</strong> setting enabled, there is no active session on the virtual machine, but the session was not logged off. This condition might occur if a virtual machine shuts down unexpectedly or the user resets the desktop during an active session. By default, when a virtual machine is in this state, View prevents any other View Client devices from accessing the desktop.</td>
</tr>
<tr>
<td>Checked out</td>
<td>Local mode</td>
<td>The virtual machine is checked out for use in local mode.</td>
</tr>
<tr>
<td>Checking out</td>
<td>Local mode</td>
<td>The virtual machine is being checked out for use in local mode.</td>
</tr>
<tr>
<td>Checked in</td>
<td>Local mode</td>
<td>A virtual machine that was checked out for use in local mode is now checked in again.</td>
</tr>
</tbody>
</table>
Table 11-5. Status of Virtual-Machine Desktops That Are Managed by vCenter Server (Continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>Type of State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking in</td>
<td>Local mode</td>
<td>A virtual machine that is checked out for use in local mode is being checked in to the vCenter Server virtual machine in the datacenter.</td>
</tr>
<tr>
<td>Replicating</td>
<td>Local mode</td>
<td>The virtual machine is checked out for use in local mode and is replicating data to the vCenter Server virtual machine in the datacenter.</td>
</tr>
<tr>
<td>Rolling back</td>
<td>Local mode</td>
<td>A virtual machine that is checked out for use in local mode is rolling back. The local desktop virtual machine is being discarded and the lock is being released on the vCenter Server version of the virtual machine.</td>
</tr>
<tr>
<td>In progress</td>
<td>Miscellaneous</td>
<td>The virtual machine is in a transitional state during a maintenance operation.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Miscellaneous</td>
<td>The virtual machine is in an unknown state.</td>
</tr>
<tr>
<td>Error</td>
<td>Miscellaneous</td>
<td>An unknown error occurred in the virtual machine.</td>
</tr>
<tr>
<td>–</td>
<td>Miscellaneous</td>
<td>A failure occurred when the virtual machine was in any of the preceding states.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>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.</td>
</tr>
<tr>
<td>Task halted</td>
<td>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 257. For details about View Composer error states, see “View Composer Provisioning Errors,” on page 400. 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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pool that contains full virtual-machine desktops</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Linked-clone pool with View Composer persistent disks</strong></td>
<td>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, the linked-clone desktop that contained the persistent disk can be recreated, or the persistent disk can be attached to another desktop. You can store detached persistent disks in the same datastore or a different one. If you select a different datastore, you cannot store detached persistent disks on a local datastore. You must use a shared datastore. You can only detach persistent disks that were created in View 4.5 or later releases.</td>
</tr>
<tr>
<td><strong>Linked-clone pool without View Composer persistent disks</strong></td>
<td>vCenter Server deletes the linked-clone virtual machines from disk. Users in currently active sessions are disconnected from their linked-clone desktops.</td>
</tr>
</tbody>
</table>

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

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,” on page 281
- “Remove an Unmanaged Desktop Source from a Pool,” on page 282
- “Delete a Pool That Contains Unmanaged Desktops,” on page 282
- “Unregister an Unmanaged Desktop Source,” on page 283
- “Desktop Status of Physical Computers and Terminal Servers,” on page 283

### 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 55.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave active</td>
<td>Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions.</td>
</tr>
<tr>
<td>Terminate</td>
<td>Active sessions end immediately.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leave active</td>
<td>Active sessions remain until the user logs off. View Connection Server does not keep track of these sessions.</td>
</tr>
<tr>
<td>Terminate</td>
<td>Active sessions end immediately.</td>
</tr>
</tbody>
</table>
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 283.
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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Type of State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waiting for Agent</td>
<td>Agent state</td>
<td>View Connection Server is waiting to receive the first request from View Agent on a physical-computer or terminal-server desktop.</td>
</tr>
<tr>
<td>Agent not reachable</td>
<td>Agent state</td>
<td>View Connection Server cannot establish communication with View Agent on the desktop. The desktop-source computer might be powered off.</td>
</tr>
<tr>
<td>Configuration error</td>
<td>Agent state</td>
<td>The display protocol such as RDP is not enabled, a terminal server is not enabled, or another protocol is not enabled.</td>
</tr>
<tr>
<td>Available</td>
<td>Availability</td>
<td>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.</td>
</tr>
<tr>
<td>Connected</td>
<td>Session state</td>
<td>The desktop is in an active session and has an active remote connection to a View client.</td>
</tr>
<tr>
<td>Disconnected</td>
<td>Session state</td>
<td>The desktop is in an active session, but it is disconnected from the View client.</td>
</tr>
<tr>
<td>-</td>
<td>Miscellaneous</td>
<td>A failure occurred when the desktop was in any of the preceding states.</td>
</tr>
</tbody>
</table>
Managing ThinApp Applications in View Administrator

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.

**IMPORTANT** If, instead of distributing ThinApps by assigning them to desktops and pools, you would rather assign ThinApps to Active Directory users and groups, you can use VMware Horizon Workspace.

This chapter includes the following topics:

- “View Requirements for ThinApp Applications,” on page 285
- “Capturing and Storing Application Packages,” on page 286
- “Assigning ThinApp Applications to Desktops and Pools,” on page 289
- “Maintaining ThinApp Applications in View Administrator,” on page 296
- “Monitoring and Troubleshooting ThinApp Applications in View Administrator,” on page 299
- “ThinApp Configuration Example,” on page 302

**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 repackgage the MSI packages.
- You must store the MSI packages on a Windows network share that resides in an Active Directory domain that is 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 Controllers. 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 286
   You use the ThinApp Setup Capture wizard to capture and package your applications.

2. **Create a Windows Network Share** on page 287
   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 287
   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 288
   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 288
   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**


- 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 MSISmoothing property to 1 in the `package.ini` file.

```
MSISmoothing=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 285 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 290  
  Follow best practices when you assign ThinApp applications to desktops and pools.

- **Assign a ThinApp Application to Multiple Desktops** on page 290  
  You can assign a particular ThinApp to one or more desktops.

- **Assign Multiple ThinApp Applications to a Desktop** on page 291  
  You can assign one or more ThinApp applications to a particular desktop.

- **Assign a ThinApp Application to Multiple Pools** on page 292  
  You can assign a particular ThinApp application to one or more pools.
Assign Multiple ThinApp Applications to a Pool on page 293
You can assign one more ThinApp applications to a particular pool.

Assign a ThinApp Template to a Desktop or Pool on page 293
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 294
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 295
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 288.

---

VMware Horizon View Administration
**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Find a specific desktop</strong></td>
<td>Type the name of the desktop in the Find text box and click Find.</td>
</tr>
<tr>
<td><strong>Find all of the desktops that follow</strong></td>
<td>Type a partial desktop name in the Find text box and click Find.</td>
</tr>
<tr>
<td><strong>the same naming convention</strong></td>
<td></td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Streaming</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Full</strong></td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

   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 288.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming</td>
<td>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.</td>
</tr>
<tr>
<td>Full</td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

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 288.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find a specific pool</td>
<td>Type the name of the pool in the Find text box and click Find.</td>
</tr>
<tr>
<td>Find all of the pools that follow the same naming convention</td>
<td>Type a partial pool name in the Find text box and click Find.</td>
</tr>
</tbody>
</table>

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**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming</td>
<td>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.</td>
</tr>
<tr>
<td>Full</td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

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 reinstall 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 288.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming</td>
<td>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.</td>
</tr>
<tr>
<td>Full</td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

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 288.

Procedure

1. In View Administrator, select Inventory > ThinApps.
2. Select the ThinApp template.
From the Add Assignment drop-down menu, select Desktops or Pools. All desktops or pools appear in the table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find a specific desktop or pool</td>
<td>Type the name of the desktop or pool in the Find text box and click Find.</td>
</tr>
<tr>
<td>Find all of the desktops or pools that follow the same naming convention</td>
<td>Type a partial desktop or pool name in the Find text box and click Find.</td>
</tr>
</tbody>
</table>

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.

Select an installation type and click OK.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming</td>
<td>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.</td>
</tr>
<tr>
<td>Full</td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

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 295.
Procedure

- Select the ThinApp application assignments that you want to review.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review all of the desktops and pools that a particular ThinApp application is assigned to</td>
<td>Select Inventory &gt; 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. <strong>Note</strong> When you assign a ThinApp application to a pool, desktops in the pool appear on the Desktops tab only after the application is installed.</td>
</tr>
<tr>
<td>Review all of the ThinApp applications that are assigned to a particular desktop</td>
<td>Select Inventory &gt; Desktops and double-click the name of the desktop in the Desktop column. The ThinApps pane on Summary tab shows each application that is currently assigned to the desktop, including the installation status.</td>
</tr>
<tr>
<td>Review all of the ThinApp applications that are assigned to a particular pool</td>
<td>Select Inventory &gt; 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.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned</td>
<td>The ThinApp application is assigned to the desktop.</td>
</tr>
<tr>
<td>Install Error</td>
<td>An error occurred when View Administrator attempted to install the ThinApp application.</td>
</tr>
<tr>
<td>Uninstall Error</td>
<td>An error occurred when View Administrator attempted to uninstall the ThinApp application.</td>
</tr>
<tr>
<td>Installed</td>
<td>The ThinApp application is installed.</td>
</tr>
<tr>
<td>Pending Install</td>
<td>View Administrator is attempting to install the ThinApp application.</td>
</tr>
<tr>
<td></td>
<td>You cannot unassign an application that has this status.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This value does not appear for desktops in pools.</td>
</tr>
<tr>
<td>Pending Uninstall</td>
<td>View Administrator is attempting to uninstall the ThinApp application.</td>
</tr>
</tbody>
</table>

**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 296
  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 297
  You can remove assignments to one or more ThinApp applications from a particular desktop.

- **Remove a ThinApp Application Assignment from Multiple Pools** on page 297
  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 297
  You can remove one or more ThinApp application assignments from a particular pool.

- **Remove a ThinApp Application from View Administrator** on page 298
  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 298
  You can add and remove applications from a ThinApp template. You can also delete a ThinApp template.

- **Remove an Application Repository** on page 298
  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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add or remove ThinApp...</td>
<td>Click Edit Template.</td>
</tr>
<tr>
<td>from the template</td>
<td></td>
</tr>
<tr>
<td>Delete the template</td>
<td>Click Delete Template.</td>
</tr>
</tbody>
</table>

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 285 for more information.
- Verify that the directories in the network share have the proper permissions. See “Cannot Register an Application Repository,” on page 299 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.

**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 286
- “Assigning ThinApp Applications to Desktops and Pools,” on page 289

**Procedure**

   
   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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Streaming</td>
<td>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.</td>
</tr>
<tr>
<td>Full</td>
<td>Installs the full application on the local file system.</td>
</tr>
</tbody>
</table>

9. In View Administrator, check the installation status of the ThinApp applications.
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,” on page 303
- “Managing View Transfer Server,” on page 309
- “Managing the Transfer Server Repository,” on page 313
- “Managing Data Transfers,” on page 319
- “Configure Security and Optimization for Local Desktop Operations,” on page 323
- “Configuring Endpoint Resource Usage,” on page 328
- “Configuring an HTTP Cache to Provision Local Desktops Over a WAN,” on page 332
- “Configuring the Heartbeat Interval for Local Desktop Client Computers,” on page 336
- “Manually Downloading a Local Desktop to a Location with Poor Network Connections,” on page 337
- “Troubleshooting View Transfer Server and Local Desktop Operations,” on page 340

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 6 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 8, 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 8, 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 Server, 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 Server is replicated to vCenter Server 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 Server is replicated to vCenter Server 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 Horizon 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.
- 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 Horizon 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 > Servers > Transfer Servers > 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 desktop cannot be checked out, and an error message will appear.
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.

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.

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.

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 305.

- Familiarize yourself with the policies and settings specific to local mode.
  
  See “Managing Data Transfers,” on page 319.

**Procedure**

1. In View Administrator, view the policy for the appropriate level.
Set the **Remote Mode** View policy to **Deny**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All desktops and pools or a single pool</td>
<td>In the Edit View Policies dialog box, set <strong>Remote Mode</strong> to <strong>Deny</strong> and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Single user</td>
<td>Complete the Add User wizard to specify the user and set <strong>Remote Mode</strong> to <strong>Deny</strong>.</td>
</tr>
</tbody>
</table>

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 328.
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

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual machine configuration</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>View Transfer Server</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Transfer Server Repository</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Pool settings</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Data replication</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Small Deployment with Minimal Capital Expenditure

You can reduce the number of ESX/ESXi servers required for your deployment if you increase the number of virtual machines on each server.

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

- Set a View policy so that end users must use their View desktops in local mode only. With this setting, the virtual machines in the datacenter remain locked and powered off.
- Set local mode policies so that end users cannot initiate desktop 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 six 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.
- If View Transfer Server is version 5.1 or later, and you plan to use linked-clone desktops in local mode, verify that all replicated View Connection Server instances in the View configuration are version 5.1 or later. If an earlier version of View Connection Server sends a request to publish a base image to the Transfer Server repository, View Transfer Server cannot perform the publish operation.

**Procedure**

1. In View Administrator, click View Configuration > Servers.
2. Click the Transfer Servers tab and click Add.
3. In the Add Transfer Server wizard, select the vCenter Server instance that manages the View Transfer Server virtual machine and click Next.
4. Select the virtual machine where View Transfer Server is installed and click Finish.

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

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

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

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

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

   When multiple SCSI controllers are added to the View Transfer Server virtual machine, Windows removes the static IP address and reconfigures the virtual machine to use DHCP. After the virtual machine restarts, you must re-enter the static IP address in the virtual machine.
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. Click the Transfer Servers panel and 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 317.

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.

**NOTE** As a best practice, before you update or migrate virtual machines that can be used in local mode, place View Transfer Server in maintenance mode and make sure that all data transfers are complete or stopped. For example, place View Transfer Server in maintenance mode before you use Storage vMotion to migrate full virtual machines or the View Composer rebalance operation to migrate linked clones to other datastores. This practice prevents local mode data transfers from taking place while maintenance operations are performed on the virtual machines.

**Procedure**

1. In View Administrator, click **View Configuration > Servers**.
2. Click the Transfer Servers tab and 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 **Maintenance Mode 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.

### 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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>View Transfer Server and the Transfer Server repository are configured and operating properly.</td>
</tr>
<tr>
<td>Pending</td>
<td>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.</td>
</tr>
<tr>
<td>Maintenance mode pending</td>
<td>View Transfer Server is entering Maintenance mode while waiting for active transfers and package publish operations to be completed.</td>
</tr>
<tr>
<td>Maintenance mode</td>
<td>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.</td>
</tr>
<tr>
<td>Initializing Transfer Server repository</td>
<td>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.</td>
</tr>
<tr>
<td>No Transfer Server repository configured</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 340.
Table 14-2. View Transfer Server Error States

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Transfer Server repository</td>
<td>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.</td>
</tr>
<tr>
<td>Repository connection error</td>
<td>View Transfer Server cannot connect to the configured Transfer Server repository.</td>
</tr>
<tr>
<td>Bad health check</td>
<td>View Transfer Server failed the View Manager health check. View Transfer Server is unavailable or not operating properly.</td>
</tr>
<tr>
<td>Transfer Server repository conflict</td>
<td>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.</td>
</tr>
<tr>
<td>Web Server down</td>
<td>The Apache2.2 service that supports the Transfer Server repository is not running.</td>
</tr>
</tbody>
</table>

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 255.

**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 310.

**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 314.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Transfer Server repository</td>
<td>On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: C:\TransferRepository\</td>
</tr>
<tr>
<td>Remote Transfer Server repository</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

3. Put all View Transfer Server instances into maintenance mode.
   a. Click the Transfer Servers tab and 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 Server Repository panel, click the General tab and click Edit.

5. Type the Transfer Server repository location and other information.

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

6. Click OK.

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

7. In the Transfer Servers panel, 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 310.
- If View Transfer Server is version 5.1 or later, verify that all replicated View Connection Server instances in the View configuration are version 5.1 or later. If an earlier version of View Connection Server sends a publish request, View Transfer Server cannot perform the publish operation.
- Verify that the Transfer Server repository is configured in View Manager. See “Configure the Transfer Server Repository,” on page 314.
- 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 314.
- Verify that a linked-clone desktop pool that will be used in local mode is created.

Procedure

1. In View Administrator, click View Configuration > Servers.
2. Click the Transfer Servers tab.
3. In the Transfer Server Repository panel, click the Contents tab and click Publish.
4. Select a View Composer base image from the list and click OK.

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 310.
Verify that a Transfer Server repository is configured. See “Configure the Transfer Server Repository,” on page 314.

**Procedure**

1. In View Administrator, click **View Configuration > Servers**.
2. Click the Transfer Server tab.
3. In the Transfer Server Repository panel, click the Contents tab and select a package file.
4. Click **Delete**.

   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.

5. 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 310.
- 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Transfer Server repository</strong></td>
<td>On the virtual machine where View Transfer Server is installed, create a path and folder for the Transfer Server repository. For example: <code>C:\TransferRepository\</code></td>
</tr>
<tr>
<td><strong>Remote Transfer Server repository</strong></td>
<td>Configure a UNC path for the network share. For example: <code>\server.domain.com\TransferRepository\</code> All View Transfer Server instances that you add to this View Manager deployment must have network access to the shared drive.</td>
</tr>
</tbody>
</table>
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 Click the Transfer Servers tab and 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 Server Repository panel, click the General tab and click Edit.
6 Type the destination Transfer Server repository location and other information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network share</td>
<td><img src="#" alt="Path" /> Type the UNC path that you configured.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="User name" /> Type the user ID of an administrator with credentials to access the network share.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Password" /> Type the administrator password.</td>
</tr>
<tr>
<td></td>
<td><img src="#" alt="Domain" /> Type the domain name of the network share in NetBIOS format. Do not use the .com suffix.</td>
</tr>
<tr>
<td>Local filesystem</td>
<td>Type the path that you configured on the local View Transfer Server virtual machine.</td>
</tr>
</tbody>
</table>
7 Click OK.
8 In the Transfer Servers panel, select each View Transfer Server instance, click Exit Maintenance Mode, and click OK.
   The View Transfer Server status changes to Ready.
9 (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 314.
- 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 309.

**Procedure**

1 Remove all instances of View Transfer Server from View Manager.
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 320**
  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 321**
  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 321**
  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 322

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 178.

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 175.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Starts the replication the next time View Client is running and the desktop contacts the datacenter.</td>
</tr>
<tr>
<td>No</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 321.

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 321.

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Administrator user</td>
<td>In View Administrator, select Monitoring &gt; Local Sessions, select the desktop, and click <strong>Rollback.</strong></td>
</tr>
</tbody>
</table>
| 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 322.

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 321.
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.

<table>
<thead>
<tr>
<th>Desktop Operating System</th>
<th>Default Check-Out Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default directory on Windows 8, Windows 7, and Windows Vista</td>
<td>%USERPROFILE%\AppData\Local\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
<tr>
<td>Default directory on Windows XP</td>
<td>%USERPROFILE%\Documents and Settings\Local Settings\Application Data\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
</tbody>
</table>

The AppData directory in Windows 8 and 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 324.
- 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 323.

Procedure

1. In View Administrator, click View Configuration > Servers.
2. Click the View Connection Servers tab, select a View Connection Server instance, and click Edit.
3. In the Edit View Connection Server Settings dialog box, click the Local Mode tab.
4. 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 326.
Table 14-3. Deduplication and Compression Settings for Data Transfers

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use deduplication for Local Mode operations</td>
<td>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.</td>
</tr>
<tr>
<td>Use compression for Local Mode operations</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use secure tunnel connection for Local Mode operations</td>
<td>Determines whether local desktops use tunneled communications. If this setting is enabled, network traffic is routed through View Connection Server or a security server if one is configured. If this setting is disabled, data transfers take place directly between local desktops and View Transfer Server. This setting is disabled by default.</td>
</tr>
<tr>
<td>Use SSL for Local Mode operations</td>
<td>Determines whether 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. These operations involve connections between client computers and View Transfer Server. This setting is enabled by default.</td>
</tr>
<tr>
<td>Use SSL when provisioning desktops in Local Mode</td>
<td>Determines whether 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. This setting is enabled by default.</td>
</tr>
</tbody>
</table>

### 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 326.

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. In the Connection Settings dialog box, select or connect to `DC=vdi, DC=vmware, DC=int`.
3. In the Computer pane, select or type `localhost:389` or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.
   
   For example: `localhost:389` or `mycomputer.mydomain.com:389`  
4. 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 325.
- 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. In the Connection Settings dialog box, select or connect to `DC=vdi, DC=vmware, DC=int`.
4. In the Computer pane, select or type `localhost:389` or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.
   
   For example: `localhost:389` or `mycomputer.mydomain.com:389`
5. In the `pae-VM` record for the local desktop, clear the values for the `pae-mVDIOfflineAuthKey`, `pae-mVDIOfflineDataKey`, and `pae-mVDIOfflineObfuscationKey` attributes.
6. 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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 8, Windows 7 and Windows Vista</td>
<td>C:\Users\user name\AppData\Local\VMware\VDM\Logs\</td>
</tr>
<tr>
<td>Windows XP</td>
<td>C:\Documents and Settings\user name\Local Settings\Application Data\VMware\VDM\Logs\</td>
</tr>
</tbody>
</table>

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 8, 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 323.

**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 8, 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>
<thead>
<tr>
<th>Memory Allocation</th>
<th>Windows XP Guests</th>
<th>Windows 8, Windows 7, and Vista Guests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>512MB</td>
<td>1GB</td>
</tr>
<tr>
<td>Best effort</td>
<td>512MB + (Available/2)</td>
<td>1GB + (Available/2)</td>
</tr>
<tr>
<td>Maximum</td>
<td>2GB</td>
<td>4GB</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Scope</th>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server specific</td>
<td>broker_guid</td>
<td>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 414.</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>remote_user_sid</td>
<td>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.</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>desktop_ID</td>
<td>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.</td>
</tr>
</tbody>
</table>

You can also find the broker GUID in the vdi.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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopMemoryScaleup</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\disableOfflineDesktopMemoryScaleup</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopDefaultMemoryScaleupValue</td>
</tr>
</tbody>
</table>

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\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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopReportedHostMemoryValue</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopReportedHostMemoryValue</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\disableOfflineDesktopCPU Scaleup</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\disableOfflineDesktopCPU Scaleup</td>
</tr>
</tbody>
</table>

The value 1 indicates that disableOfflineDesktopCPU Scaleup 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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopDefaultCPU ScaleupValue</td>
</tr>
<tr>
<td>Server specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\offlineDesktopDefaultCPU ScaleupValue</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopDefaultCPU ScaleupValue</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopDefaultCPU ScaleupValue</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Scope</th>
<th>Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server specific</td>
<td>broker_guid</td>
<td>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 414.</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>remote_user_sid</td>
<td>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.</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>desktop_ID</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Scope of Setting</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-wide</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\offlineDesktopUseBridgedNetworking</td>
</tr>
<tr>
<td>Server and user specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\offlineDesktopUseBridgedNetworking</td>
</tr>
<tr>
<td>Server, user, and desktop specific</td>
<td>HKCU\Software\VMware, Inc.\VMware VDM\Client\broker_guid\remote_user_sid\desktop_ID\offlineDesktopUseBridgedNetworking</td>
</tr>
</tbody>
</table>

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 333
   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 334
   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 334
   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 335
   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. Click the View Connection Servers tab, select a View Connection Server instance, and click **Edit**.

3. Click the Local Mode tab and 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.

5 Click **OK.**

**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 433.

**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
```
2 In the left pane, expand the registry path.

<table>
<thead>
<tr>
<th>Processor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>HKEY_LOCAL_MACHINE, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM</td>
</tr>
<tr>
<td>32-bit</td>
<td>HKEY_LOCAL_MACHINE, SOFTWARE, VMware Inc., VMware VDM</td>
</tr>
</tbody>
</table>

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.

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 334.
- 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 333.

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 336
  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 337
  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. In the Connection Settings dialog box, select or connect to DC=vdi, DC=vmware, DC=int.
3. In the Computer pane, select or type localhost:389 or the fully qualified domain name (FQDN) of the View Connection Server host followed by port 389.
   
   For example: localhost:389 or mycomputer.mydomain.com:389

4. 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>64-bit</td>
<td>Add <code>policyUpdateFrequency</code> to <strong>HKEY_LOCAL_MACHINE</strong>, SOFTWARE, Wow6432Node, VMware Inc., VMware VDM.</td>
</tr>
<tr>
<td>32-bit</td>
<td>Add <code>policyUpdateFrequency</code> to <strong>HKEY_LOCAL_MACHINE</strong>, SOFTWARE, VMware Inc., VMware VDM.</td>
</tr>
</tbody>
</table>

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 8 or 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 338

   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 338
   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 339
   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 339
   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 305.
- 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 316.

Procedure

1 In View Administrator, click View Configuration > Servers.
2 Click the Transfer Servers tab.
3 In the Transfer Server Repository panel, click Contents tab, select the package that is associated with
   desktop pool from which you will check out a desktop, and click Details.
4 Verify that the desktop pool is associated with this package.
5 Locate the Repository path, including the package ID.
   For example: \"mycomputer.com\ImageRepository\Published\f222434a-e52a-4ce3-92d1-c14122fca996
6 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 338.

Procedure

1 Deliver the portable device that contains the desktop pool’s package files to the user.
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.

<table>
<thead>
<tr>
<th>Check-Out Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default directory on Windows 8, Windows 7, and Windows Vista</td>
<td>C:\Users\User Name\AppData\Local\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
<tr>
<td>Default directory on Windows XP</td>
<td>C:\Documents and Settings\User Name\Local Settings\Application Data\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
<tr>
<td>Custom directory</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 8 or 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 338.

Procedure

1. Log in to the Windows 8 or 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 339.

Procedure

1. On the client computer, start 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 341
  When users try to check out desktops, the operations fail and an error message, _No available Transfer Server_, is displayed.

- **Problems with Desktop Check-Outs After Initial Check-Out** on page 342
  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.

- **Login Window Takes a Long Time to Appear** on page 342
  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.

- **View Transfer Server Remains in a Pending State** on page 343
  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.

- **View Transfer Server Fails to Enter Maintenance Mode** on page 343
  When you attempt to place View Transfer Server in maintenance mode, it remains in the Maintenance mode pending state for an excessively long time.

- **The Transfer Server Repository Is Invalid** on page 344
  In View Administrator, View Transfer Server displays a status of Bad Transfer Server repository.

- **View Transfer Server Cannot Connect to the Transfer Server Repository** on page 344
  In View Administrator, View Transfer Server displays a status of Repository Connection Error.
- **View Transfer Server Fails the Health Check** on page 345
  
  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.

- **The Transfer Server Repository Is Not Configured** on page 345
  
  In View Administrator, View Transfer Server displays a status of No Transfer Server Repository Configured.

- **View Transfer Server Instances Have Conflicting Transfer Server Repositories** on page 346
  
  In View Administrator, View Transfer Server instances display a status of Transfer Server Repository Conflict.

- **The View Transfer Server Web Service Is Down** on page 346
  
  In View Administrator, View Transfer Server displays a status of Web Server Down.

- **Local Mode Operation Fails After the Datacenter Desktop Was Modified** on page 346
  
  During a local mode operation such as a check-out or check-in, the operation fails, and the following message is displayed: This desktop has been modified at the datacenter. Please contact your system administrator.

- **Recover Data from a Local Desktop** on page 348
  
  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.

### 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 Horizon 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.

<table>
<thead>
<tr>
<th>Desktop Operating System</th>
<th>Default Check-Out Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default directory on Windows 8, Windows 7, and Windows Vista</td>
<td>C:\Users\User Name\AppData\Local\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
<tr>
<td>Default directory on Windows XP</td>
<td>C:\Documents and Settings\User Name\Local Settings\Application Data\VMware\VDM\Local Desktops\pool_display_name</td>
</tr>
</tbody>
</table>

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.
  - On the View Transfer Server virtual machine, open the Control Panel > Administrative Tools > Services dialog box.
  - 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 Horizon 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 317.

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. Click the Transfer Servers tab and select a View Transfer Server instance.
   c. Click Enter Maintenance Mode.
   d. 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.
   e. Click OK.
   f. Repeat these steps for all View Transfer Server instances.
2. In the Transfer Server Repository panel, click the General tab.
3. Click Edit and configure the Transfer Server repository again.
   View 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 Horizon View Installation Guide*.

The Transfer Server Repository Is Not Configured

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. Click the Transfer Servers tab and select a View Transfer Server instance.
   c. Click Enter Maintenance Mode.
   d. 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.
   e. Click OK.
   f. Repeat these steps for all View Transfer Server instances.
2. In the Transfer Server Repository panel, click the General tab.
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 344.

**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.

**Local Mode Operation Fails After the Datacenter Desktop Was Modified**

During a local mode operation such as a check-out or check-in, the operation fails, and the following message is displayed: This desktop has been modified at the datacenter. Please contact your system administrator.

**Problem**
A local mode operation fails when a user initiates the operation, or when the operation is interrupted or paused and then resumes. This problem can occur with the following local mode operations: check-out, resume check-out, cancel check-out, check-in, resume check-in, cancel check-in, roll back, initiate replication, resume replication.

In addition to the user error message, View events are generated if the View Event database is configured, and messages are generated in the View Connection Server logs.
If this problem occurs during a replication, the status of the operation changes to *Wait to resume backup*. The error message, *This desktop has been modified at the datacenter. Please contact your system administrator.*, is not displayed to the user.

**Cause**

When a View desktop is checked out, a snapshot is taken in vCenter Server 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.

This problem can occur if vSphere allows the datacenter copy of a virtual machine to be unlocked and then, perhaps inadvertently, another process or person powers on the virtual machine. For example, a virtual machine might be unlocked during a vCenter Server upgrade. The virtual machine in the datacenter and the local desktop are no longer synchronized.

When a local mode operation is initiated or resumed, View detects that the virtual machine versions are not synchronized and stops the operation.

**Solution**

You can recover the client version or vCenter Server version of the virtual machine, depending on the local mode operation that was underway.

If a check-in or replication failed, recover the client version. You can use a `vdmadmin -V` command that reverts the vCenter Server virtual machine to the snapshot that was taken during the last synchronization.

1. On the View Connection Server computer, open a command prompt and navigate to the `C:\Program Files\VMware\VMware View\Server\tools\bin` directory.
2. Run the `vdmadmin -V -recoverClientVM` command.
   
   For example: `vdmadmin -V -recoverClientVM -d lmdtpool -m machine1`
3. Instruct the user to start the check-in operation again.

If a check-out failed, recover the vCenter Server version. You can use a `vdmadmin -V` command that takes a new snapshot of the vCenter Server virtual machine, deletes the old snapshot, and rolls back the virtual machine. During a rollback, the local View desktop is discarded.

1. On the View Connection Server computer, open a command prompt and navigate to the `C:\Program Files\VMware\VMware View\Server\tools\bin` directory.
2. Run the `vdmadmin -V -recoverServerVM` command.
   
   For example: `vdmadmin -V -recoverServerVM -d lmdtpool -m machine2`
3. Instruct the user to start the check-out operation again.

In a special situation in which a desktop is fully checked out, and no check-in or replication was underway when the vCenter Server virtual machine was opened, you might want to preserve both the client and vCenter Server virtual machines. Perhaps valid, useful contents were created on both virtual machines. In vCenter Server, you can clone the vCenter Server virtual machine to preserve an identical copy. Next, you can use the `vdmadmin` command with the `-V -recoverClientVM` option to recover the client virtual machine.

For information about using the `vdmadmin` command with the `-V` option, see “Recovering a Local Desktop by Using the -V Option When the Desktop Was Modified in the Datacenter,” on page 435.
Recover Data from a Local Desktop

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
   ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d desktop</code></td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td><code>-infile path_to_VM_file</code></td>
<td>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 <code>-infile</code> 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 <code>-infile</code> option. Do not specify a VMDK file that corresponds to a disk slice.</td>
</tr>
<tr>
<td><code>-u domain\user</code></td>
<td>Specifies the domain and name of the local desktop's end user.</td>
</tr>
</tbody>
</table>

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-caf14c8ddbb14a3d-scsi00.vmdk
5215df4df635a14d-caf14c8ddbb14a3d-scsi00-s001.vmdk
5215df4df635a14d-caf14c8ddbb14a3d-scsi00-s002.vmdk
5215df4df635a14d-caf14c8ddbb14a3d-scsi00-s003.vmdk
5215df4df635a14d-caf14c8ddbb14a3d-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.
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,” on page 351
- “Monitor View Components,” on page 358
- “Monitor Desktop Status,” on page 358
- “Understanding View Manager Services,” on page 359
- “Add Licenses to VMware Horizon View,” on page 361
- “Update General User Information from Active Directory,” on page 361
- “Migrate View Composer to Another Computer,” on page 362
- “Update the Certificates on a View Connection Server Instance, Security Server, or View Composer,” on page 367
- “Information Collected by the Customer Experience Improvement Program,” on page 368

### 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 encrypted LDAP data interchange format (LDIF). For a description of View LDAP, see “View LDAP Directory,” on page 36.

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** utility. This utility is provided with each instance of View Connection Server.

The **vdmexport** utility can export View LDAP data as encrypted LDIF data, plain text, or plain text with passwords and other sensitive data removed.

**NOTE** The **vdmexport** tool backs up the View LDAP data only. This tool does not back up View Composer database information.

The following guidelines apply to backing up View configuration data:

- 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.

### 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 353.

**Procedure**

1. In View Administrator, click **Configuration > Servers**.
2. Select the View Connection Server instance to be backed up and click **Edit**.
3. Click the Backup tab.
4. Specify the View Manager Configuration Backup settings to configure the backup frequency, maximum number of backups, and the folder location of the backup files.
5. (Optional) Change the data recovery password.
   a. Click **Change data recovery password**.
   b. Type and retype the new password.
   c. (Optional) Type a password reminder.
   d. Click **OK**.
6. 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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic backup frequency</td>
<td>Every Hour. Backups take place every hour on the hour.</td>
</tr>
<tr>
<td></td>
<td>Every 6 Hours. Backups take place at midnight, 6 am, noon, and 6 pm.</td>
</tr>
<tr>
<td></td>
<td>Every 12 Hours. Backups take place at midnight and noon.</td>
</tr>
<tr>
<td></td>
<td>Every Day. Backups take place every day at midnight.</td>
</tr>
<tr>
<td></td>
<td>Every 2 Days. Backups occur at midnight on Saturday, Monday, Wednesday, and Friday.</td>
</tr>
<tr>
<td></td>
<td>Every Week. Backups take place weekly at midnight on Saturday.</td>
</tr>
<tr>
<td></td>
<td>Every 2 Weeks. Backups take place every other week at midnight on Saturday.</td>
</tr>
<tr>
<td></td>
<td>Never. Backups do not take place automatically.</td>
</tr>
<tr>
<td>Max number of backups</td>
<td>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.</td>
</tr>
<tr>
<td>Folder location</td>
<td>Default location of the backup files on the computer where View Connection Server is running: C:\Programdata\VMWare\VDM\backups When you use Backup Now, View Manager also stores the backup files in this location.</td>
</tr>
</tbody>
</table>

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 View LDAP configuration data to an encrypted LDIF file. You can also use the vdmexport -v (verbatim) option to export the data to a plain text LDIF file, or the vdmexport -c (cleansed) option to export the data as plain text with passwords and other sensitive data removed.

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
   By default, the exported data is encrypted.
You can specify the output file name as an argument to the \texttt{\-f} option. For example:

\texttt{vdmexport \-f Myexport.LDF}

You can export the data in plain text format (verbatim) by using the \texttt{\-v} option. For example:

\texttt{vdmexport \-f Myexport.LDF \-v}

You can export the data in plain text format with passwords and sensitive data removed (cleansed) by using the \texttt{\-c} option. For example:

\texttt{vdmexport \-f Myexport.LDF \-c}

\textbf{Note} \quad Do not plan on using cleansed backup data to restore a View LDAP configuration. The cleansed configuration data is missing passwords and other critical information.

For more information about the \texttt{vdmexport} command, see the \textit{VMware Horizon View Integration} document.

\section*{What to do next}

You can restore or transfer the configuration information of View Connection Server by using the \texttt{vdmimport} command.

For details about importing the LDIF file, see “Restoring View Connection Server and View Composer Configuration Data,” on page 354.

\section*{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 351.

You use the \texttt{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 \texttt{SviConfig} utility to import the View Composer data from the .svi backup files to the View Composer SQL database.

\textbf{Note} \quad In certain situations, you might have to install the current version of a View Connection Server instance and restore the existing View configuration by importing the View Connection Server LDAP configuration files. You might require this procedure as part of a business continuity and disaster recovery (BC/DR) plan, as a step in setting up a second datacenter with the existing View configuration, or for other reasons. For more information, see “Reinstall View Connection Server with a Backup Configuration” in the \textit{VMware Horizon View Installation} document.

\section*{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 \texttt{vdmimport} command to import the data from the LDIF file to the View LDAP repository in the View Connection Server instance.

If you backed up your View LDAP configuration by using View Administrator or the default \texttt{vdmexport} command, the exported LDIF file is encrypted. You must decrypt the LDIF file before you can import it.
If the exported LDIF file is in plain text format, you do not have to decrypt the file.

**NOTE** Do not import an LDIF file in cleansed format, which is plain text with passwords and other sensitive data removed. If you do, critical configuration information will be missing from the restored View LDAP repository.

For information about backing up the View LDAP repository, see “Back up View Connection Server and View Composer Data,” on page 351.

**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 with the View Administrators role.

- Verify that you know the data recovery password. If a password reminder was configured, you can display the reminder by running the `vdmimport` command without the password option.

**Procedure**

1. Select **Start > Command Prompt**.
2. Decrypt the encrypted LDIF file.
   
   At the command prompt, type the `vdmimport` command. Specify the `-d` option, the `-p` option with the data recovery password, and the `-f` option with an existing encrypted LDIF file followed by a name for the decrypted LDIF file. For example:
   
   ```bash
   vdmimport -d -p mypassword
   -f MyEncryptedexport.LDF > MyDecryptedexport.LDF
   ```

   If you do not remember your data recovery password, type the command without the `-p` option. The utility displays the password reminder and prompts you to enter the password.

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

   Specify the `-f` option with the decrypted LDIF file. For example:
   
   ```bash
   vdmimport -f MyDecryptedexport.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 Horizon 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, at `C:\ProgramData\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

Familiarize yourself with the SviConfig restoredata parameters:

- DsnName - The DSN that is used to connect to the database. The DsnName parameter is mandatory and cannot be an empty string.
- Username - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- Password - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- BackupFilePath - The path to the View Composer backup file.

The DsnName and BackupFilePath parameters are required and cannot be empty strings. The Username and Password parameters are optional.

Procedure

1. Copy the View Composer backup files from the View Connection Server computer to a location that is accessible from the computer where the View Composer service is installed.
2. On the computer where View Composer is installed, stop the VMware View Composer service.
3. 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 356.

Result Codes for Restoring the View Composer Database

When you restore a View Composer database, the SviConfig restoredata command displays a result code.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The operation ended successfully.</td>
</tr>
<tr>
<td>1</td>
<td>The supplied DSN could not be found.</td>
</tr>
</tbody>
</table>
### Table 15-2. Restoredata Result Codes (Continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Invalid database administrator credentials were provided.</td>
</tr>
<tr>
<td>3</td>
<td>The driver for the database is not supported.</td>
</tr>
<tr>
<td>4</td>
<td>An unexpected problem occurred and the command failed to complete.</td>
</tr>
<tr>
<td>14</td>
<td>Another application is using the View Composer service. Shut down the service before executing the command.</td>
</tr>
<tr>
<td>15</td>
<td>A problem occurred during the restore process. Details are provided in the onscreen log output.</td>
</tr>
</tbody>
</table>

### Export Data in View Composer Database

You can export data from your View Composer database to file.

**IMPORTANT** Use the SviConfig utility only if you are an experienced View Composer administrator.

**Prerequisites**

By default, View Manager stores the backup files on the C: drive of the View Connection Server computer, at C:\ProgramData\VMWare\VDM\backups.

Familiarize yourself with the SviConfig exportdata parameters:

- **DsnName** - The DSN that is used to connect to the database. If it is not specified, DSN name, user name and password will be retrieved from server configuration file.
- **Username** - The user name that is used to connect to the database. If this parameter is not specified, Windows authentication is used.
- **Password** - The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- **OutputFilePath** - The path to the output file.

**Procedure**

1. On the computer where View Composer is installed, stop the VMware View Composer service.
2. Open a Windows command prompt and navigate to the SviConfig executable file. The file is located with the View Composer application.

   `<View Composer installation directory>\sviconfig.exe`

3. Run the SviConfig exportdata command.

   ```shell
   sviconfig -operation=exportdata
   -DsnName=target_database_source_name_(DSN)
   -Username=database_administrator_username
   -Password=database_administrator_password
   -OutputFilePath=path_to_View_Composer_output_file
   ```

   For example:

   ```shell
   sviconfig -operation=exportdata -dsnname=LinkedClone
   -username=Admin -password=Pass
   -outputfilepath="C:\Program Files\VMware\VMware View Composer\Export-20090304000010-foobar_test_org.SVI"
   ```
What to do next

For export result codes for the `sviConfig exportdata` command, see “Result Codes for Exporting the View Composer Database,” on page 358.

Result Codes for Exporting the View Composer Database

When you export a View Composer database, the `sviConfig exportdata` command displays an exit code.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Exporting data ended successfully.</td>
</tr>
<tr>
<td>1</td>
<td>The supplied DSN name cannot be found.</td>
</tr>
<tr>
<td>2</td>
<td>The supplied credentials are invalid.</td>
</tr>
<tr>
<td>3</td>
<td>Unsupported driver for the provided database.</td>
</tr>
<tr>
<td>4</td>
<td>An unexpected problem has occurred.</td>
</tr>
<tr>
<td>18</td>
<td>Unable to connect to the database server.</td>
</tr>
<tr>
<td>24</td>
<td>Unable to open the output file.</td>
</tr>
</tbody>
</table>

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 275.
Procedure

1. In View Administrator, click Dashboard.
2. In the Desktop Status pane, expand a status folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparing</td>
<td>Lists the desktop states while the virtual machine is being provisioned,</td>
</tr>
<tr>
<td></td>
<td>deleted, or in maintenance mode.</td>
</tr>
<tr>
<td>Problem Desktops</td>
<td>Lists the desktop error states.</td>
</tr>
<tr>
<td>Prepared for use</td>
<td>Lists the desktop states when the desktop is ready for use.</td>
</tr>
</tbody>
</table>

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 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 360 and “Services on a Security Server,” on page 360.

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 15-4. View Connection Server Host Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Startup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware View Connection Server</td>
<td>Automatic</td>
<td>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.</td>
</tr>
<tr>
<td>VMware View Framework Component</td>
<td>Manual</td>
<td>Provides event logging, security, and COM+ framework services for View Manager. This service must be running for the correct operation of View Manager.</td>
</tr>
<tr>
<td>VMware View Message Bus Component</td>
<td>Manual</td>
<td>Provides messaging services between View Manager components. This service must be running for the correct operation of View Manager.</td>
</tr>
<tr>
<td>VMware View PCoIP Secure Gateway</td>
<td>Manual</td>
<td>Provides PCoIP Secure Gateway services. This service must be running if clients connect to View Connection Server through the PCoIP Secure Gateway.</td>
</tr>
<tr>
<td>VMware View Script Host</td>
<td>Automatic (if enabled)</td>
<td>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.</td>
</tr>
<tr>
<td>VMware View Security Gateway Component</td>
<td>Manual</td>
<td>Provides secure tunnel services for View Manager. This service must be running for the correct operation of View Manager.</td>
</tr>
<tr>
<td>VMware View Web Component</td>
<td>Manual</td>
<td>Provides web services for View Manager. This service must be running for the correct operation of View Manager.</td>
</tr>
<tr>
<td>VMwareVDMDS</td>
<td>Automatic</td>
<td>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 View to ensure that existing data is migrated correctly.</td>
</tr>
</tbody>
</table>

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 15-5. Security Server Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Startup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware View Security Server</td>
<td>Automatic</td>
<td>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.</td>
</tr>
<tr>
<td>VMware View Framework Component</td>
<td>Manual</td>
<td>Provides event logging, security, and COM+ framework services. This service must be running for the correct operation of a security server.</td>
</tr>
<tr>
<td>VMware View PCoIP Secure Gateway</td>
<td>Manual</td>
<td>Provides PCoIP Secure Gateway services. This service must be running if clients connect to a security server through the PCoIP Secure Gateway.</td>
</tr>
<tr>
<td>VMware View Security Gateway Component</td>
<td>Manual</td>
<td>Provides secure tunnel services. This service must be running for the correct operation of a security server.</td>
</tr>
</tbody>
</table>
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 15-6. View Transfer Server Host Services

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Startup Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware View Transfer Server</td>
<td>Automatic</td>
<td>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.</td>
</tr>
<tr>
<td>VMware View Transfer Server Control Service</td>
<td>Manual</td>
<td>Provides management capabilities for View Transfer Server and handles communication with View Connection Server.</td>
</tr>
<tr>
<td>VMware View Framework Component</td>
<td>Manual</td>
<td>Provides event logging, security, and COM+ framework services for View Manager.</td>
</tr>
<tr>
<td>Apache2.2 service</td>
<td>Automatic</td>
<td>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.</td>
</tr>
</tbody>
</table>

Add Licenses to VMware Horizon View

If the current licenses on a system expire, or if you want to access VMware Horizon View features that are currently unlicensed, you can use View Administrator to add licenses.

You can add a license to VMware Horizon 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 414.

### Prerequisites

Verify that you can log in to View Administrator as an administrator with the Manage Global Configuration and Policies privilege.

### Procedure

1. In View Administrator, click Users and Groups.
2. Choose whether to update information for all users or an individual user.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all users</td>
<td>Click Update General User Information. Updating all users and groups can take a long time.</td>
</tr>
<tr>
<td>For an individual user</td>
<td>a Click the user name to update. &lt;br&gt;b Click Update General User Information.</td>
</tr>
</tbody>
</table>

### Migrate View Composer to Another Computer

In some situations, you might need to migrate a View Composer service to a new Windows Server computer. For example, you might migrate View Composer and vCenter Server to a new ESXi host or cluster to expand your View deployment. In addition, View Composer and vCenter Server do not have to be installed on the same Windows Server computer.

You can migrate View Composer from the vCenter Server computer to a standalone computer or from a standalone computer to the vCenter Server computer.

- **Guidelines for Migrating View Composer** on page 363
  - The steps you take to migrate the View Composer service depend on whether you intend to preserve existing linked-clone desktops.

- **Migrate View Composer with an Existing Database** on page 363
  - When you migrate View Composer to another computer, if you intend to preserve your current linked-clone desktops, the new View Composer service must continue to use the existing View Composer database.

- **Migrate View Composer Without Linked-Clone Desktops** on page 365
  - If the current View Composer service does not manage any linked-clone desktops, you can migrate View Composer to a new computer without migrating the RSA keys to the new computer. The migrated View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

- **Prepare a Microsoft .NET Framework for Migrating RSA Keys** on page 366
  - 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.

- **Migrate the RSA Key Container to the New View Composer Service** on page 366
  - 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 computer on which you want to install the new View Composer service.
Guidelines for Migrating View Composer

The steps you take to migrate the View Composer service depend on whether you intend to preserve existing linked-clone desktops.

To preserve the linked-clone desktops in your deployment, the View Composer service that you install on the new computer must continue to use the existing View Composer database. The View Composer database contains data that is required to create, provision, maintain, and delete the linked clones.

When you migrate the View Composer service, you can also migrate the View Composer database to a new computer.

Whether or not you migrate the View Composer database, the database must be configured on an available computer in the same domain as the new computer on which you install the 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.

If the current View Composer service does not manage any linked-clone desktops, you can migrate the service without using the existing View Composer database. You do not have to migrate the RSA keys, whether or not you use the existing database.

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.

Migrate View Composer with an Existing Database

When you migrate View Composer to another computer, if you intend to preserve your current linked-clone desktops, the new View Composer service must continue to use the existing View Composer database.

Follow the steps in this procedure when you migrate View Composer in any of the following directions:

- From a vCenter Server computer to a standalone computer
- From a standalone computer to a vCenter Server computer
- From a standalone computer to another standalone computer
- From a vCenter Server computer to another vCenter Server computer

When you migrate the View Composer service, you can also migrate the View Composer database to a new location. For example, you might need to migrate the View Composer database if the current database is located on a vCenter Server computer that you are migrating as well.

When you install the View Composer service on the new computer, you must configure the service to connect to the View Composer database.

Prerequisites

- Familiarize yourself with the View Composer migration requirements. See “Guidelines for Migrating View Composer,” on page 363.
- Familiarize yourself with the steps for migrating the RSA key container to the new View Composer Service. See “Prepare a Microsoft .NET Framework for Migrating RSA Keys,” on page 366 and “Migrate the RSA Key Container to the New View Composer Service,” on page 366.
- Familiarize yourself with installing the View Composer service. See "Installing View Composer" in the VMware Horizon View Installation document.
Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the *VMware Horizon View Installation* document.


**Procedure**

1. Disable virtual machine provisioning in the vCenter Server instance that is associated with the View Composer service.
   a. In View Administrator, click View Configuration > Servers.
   b. In the vCenter Server tab, select the vCenter Server instance and click Disable provisioning.

2. (Optional) Migrate the View Composer database to a new location.
   If you need to take this step, consult your database administrator for migration instructions.

3. Uninstall the View Composer service from the current computer.

4. (Optional) Migrate the RSA key container to the new computer.

5. Install the View Composer service on the new computer.
   During the installation, specify the DSN of the database that was used by the original View Composer service. Also specify the domain administrator user name and password that were provided for the ODBC data source for that database.
   If you migrated the database, the DSN and data source information must point to the new location of the database. Whether or not you migrated the database, the new View Composer service must have access to the original database information about the linked clones.

6. Configure an SSL server certificate for View Composer on the new computer.
   You can copy the certificate that was installed for View Composer on the original computer or install a new certificate.

7. In View Administrator, configure the new View Composer settings.
   a. In View Administrator, click View Configuration > Servers, select the vCenter Server instance that is associated with this View Composer service, and click Edit.
   b. In the View Composer tab, provide the new View Composer settings.
      If you are installing View Composer with vCenter Server on the new computer, select View Composer co-installed with the vCenter Server.
      If you are installing View Composer on a standalone computer, select Standalone View Composer Server and provide the FQDN of the View Composer computer and the user name and password of the View Composer user.
   c. In the Domains pane, click Verify Server Information and add or edit the View Composer domains as needed.
   d. Click OK.
Migrate View Composer Without Linked-Clone Desktops

If the current View Composer service does not manage any linked-clone desktops, you can migrate View Composer to a new computer without migrating the RSA keys to the new computer. The migrated View Composer service can connect to the original View Composer database, or you can prepare a new database for View Composer.

Prerequisites

- Familiarize yourself with installing the View Composer service. See "Installing View Composer" in the VMware Horizon View Installation document.
- Familiarize yourself with configuring an SSL certificate for View Composer. See "Configuring SSL Certificates for View Servers" in the VMware Horizon View Installation document.
- Familiarize yourself with the steps for removing View Composer from View Manager. See “Remove View Composer from View Manager,” on page 24.
  Before you can remove View Composer, verify that it no longer manages any linked-clone desktops. If any linked clones remain, you must delete them.

Procedure

1. In View Administrator, remove View Composer from View Manager.
   a. In the Edit vCenter Server dialog, make sure that Do not use View Composer is selected.
   b. In the Edit vCenter Server dialog, click OK.

2. Uninstall the View Composer service from the current computer.

3. Install the View Composer service on the new computer.
   During the installation, configure View Composer to connect to the DSN of the original or new View Composer database.

4. Configure an SSL server certificate for View Composer on the new computer.
   You can copy the certificate that was installed for View Composer on the original computer or install a new certificate.

5. In View Administrator, configure the new View Composer settings.
   a. In View Administrator, click View Configuration > Servers, select the vCenter Server instance that is associated with this View Composer service, and click Edit.
   b. In the View Composer Server Settings pane, click Edit.
   c. Provide the new View Composer settings.
      If you are installing View Composer with vCenter Server on the new computer, select View Composer co-installed with the vCenter Server.
      If you are installing View Composer on a standalone computer, select Standalone View Composer Server and provide the FQDN of the View Composer computer and the user name and password of the View Composer user.
   d. In the Domains pane, click Verify Server Information and add or edit the View Composer domains as needed.
   e. Click OK.
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

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 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 366.

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 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 366.

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\v2.0xxxxx directory.
2. Type the aspnet_regiis command to save the RSA key pair in a local file.
   ```bash
   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\v2.0xxxxx directory.
5. Type the aspnet_regiis command to migrate the RSA key pair data.
   ```bash
   aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" --exp
   ```
   where path is the path to the exported file.
The `-exp` option creates an exportable key pair. If a future migration is required, the keys can be exported from this computer and imported to another computer. If you previously migrated the keys to this computer without using the `-exp` option, you can import the keys again using the `-exp` option so that you can export the keys in the future.

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 computer. Provide the DSN and ODBC data source information that allows View Composer to connect to the same database information that was used by the original View Composer service. For installation instructions, see "Installing View Composer" in the *VMware Horizon View Installation* document.

Complete the steps to migrate View Composer to a new computer and use the same database. See “Migrate View Composer with an Existing Database,” on page 363.

**Update the Certificates on a View Connection Server Instance, Security Server, or View Composer**

When you receive updated server SSL certificates or intermediate certificates, you import the certificates into the Windows local computer certificate store on each View Connection Server, security server, or View Composer host.

Typically, server certificates expire after 12 months. Root and intermediate certificates expire after 5 or 10 years.

For detailed information about importing server and intermediate certificates, see “Configure View Connection Server, Security Server, or View Composer to Use a New SSL Certificate” in the *VMware Horizon View Installation* document.

**Prerequisites**

- Obtain updated server and intermediate certificates from the CA before the currently valid certificates expire.
- Verify that the Certificate snap-in was added to MMC on the Windows Server on which the View Connection Server instance, security server, or View Composer service was installed.

**Procedure**

1. Import the signed SSL server certificate into the Windows local computer certificate store on the Windows Server host.
   a. In the Certificate snap-in, import the server certificate into the **Certificates (Local Computer) > Personal > Certificates** folder.
   b. Select **Mark this key as exportable**.
   c. Click **Next** and click **Finish**.

2. For View Connection Server or security server, delete the certificate Friendly name, *vdm*, from the old certificate that was issued to the View server.
   a. Right-click the old certificate and click **Properties**
   b. On the General tab, delete the Friendly name text, *vdm*. 
3 For View Connection Server or security server, add the certificate Friendly name, \texttt{vdm}, to the new certificate that is replacing the previous certificate.
   a Right-click the new certificate and click \texttt{Properties}.
   b On the General tab, in the Friendly name field, type \texttt{vdm}.
   c Click \texttt{Apply} and click \texttt{OK}.

4 For a server certificate that is issued to View Composer, run the \texttt{SviConfig ReplaceCertificate} utility to bind the new certificate to the port used by View Composer.
   This utility replaces the old certificate binding with the new certificate binding.
   a Stop the View Composer service.
   b In a Windows command prompt, type the \texttt{SviConfig ReplaceCertificate} command. For example:
     \begin{verbatim}
     sviconfig -operation=ReplaceCertificate
     -delete=false
     \end{verbatim}
     The utility displays a numbered list of SSL certificates that are available in the Windows local computer certificate store.
   c To select a certificate, type the number of the certificate and press Enter.

5 If intermediate certificates are issued to a View Connection Server, security server, or View Composer host, import the most recent update to the intermediate certificates into the \texttt{Certificates (Local Computer) > Intermediate Certification Authorities > Certificates} folder in the Windows certificate store.

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

\textbf{Information Collected by the Customer Experience Improvement Program}

You can participate in a customer experience improvement program when you install View Connection Server with a new configuration or by using View Administrator after the installation. If you participate in the program, VMware collects anonymous data about your deployment in order to improve VMware's response to customer requirements. No data that identifies your organization is collected.

Before collecting the data, VMware makes anonymous all fields that contain information that is specific to your organization. The sanitized fields identify computers, data storage, networking features, applications, and users. For example, IP addresses and desktop customization specifications are made anonymous.

VMware sanitizes a field by generating a hash of the actual value. When a hash value is collected, VMware cannot identify the actual value but can detect changes in the value when you change your environment.

To help you determine whether to join the program, you can review the fields from which VMware gathers data. You can also examine all the sanitized fields. The fields are organized by View component.

\textbf{Global View Data Collected by VMware}

If you join the customer experience improvement program, VMware collects global data about the View environment. Fields containing sensitive information are made anonymous.

\textbf{Table 15-7. Global Data Collected for the Customer Experience Improvement Program}

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>View servers can contact the domain controller.</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The DNS of the Active Directory domain</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 15-7. Global Data Collected for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The domain is an NT4-style domain.</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The name of the domain</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The status of the domain</td>
<td>No</td>
<td>OK</td>
</tr>
<tr>
<td>The type of trust relationship with the domain</td>
<td>No</td>
<td>Primary domain, Two way, Two way forest, and so on.</td>
</tr>
</tbody>
</table>

View Connection Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain View Connection Server fields. Fields containing sensitive information are made anonymous.

Table 15-8. Data Collected from View Connection Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The common name (CN) for the View Connection Server entry in View LDAP</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>View Connection Server is disabled</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>SecureID authentication is configured and active</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Type of View Connection Server installation</td>
<td>No</td>
<td>0 = View Connection Server 1 = security server</td>
</tr>
<tr>
<td>Must the SecureID authentication name match the Active Directory name?</td>
<td>No</td>
<td>True = SecureID authentication name is mapped False = SecureID authentication name is not mapped</td>
</tr>
<tr>
<td>Are clients allowed to bypass the secure tunnel?</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Are clients allowed to bypass the PCoIP Secure Gateway?</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Configuration of smart card authentication</td>
<td>No</td>
<td>Off, Optional, or Required</td>
</tr>
<tr>
<td>Should users be automatically logged off when their smart card is removed?</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Folder in which View LDAP backups are stored</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Units of time for setting the View LDAP backup frequency</td>
<td>No</td>
<td>Hour, Day, or Week</td>
</tr>
<tr>
<td>Frequency of View LDAP backups</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Time of View LDAP backup</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Maximum number of View LDAP backups to store</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Time of last View LDAP backup</td>
<td>No</td>
<td>Feb 21, 2012 12:00:10 AM</td>
</tr>
<tr>
<td>Status of the last View LDAP backup</td>
<td>No</td>
<td>OK</td>
</tr>
<tr>
<td>Pending immediate View LDAP backup</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Description</td>
<td>Is This Field Made Anonymous?</td>
<td>Example Value</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Local Mode configuration settings</td>
<td>No</td>
<td>Use secure tunnel connection for Local Mode operations = True or false Use an editable secure tunnel connection for Local Mode operations = True or false Use SSL for Local Mode operations = True or false Use SSL when provisioning base-image packages for desktops in Local Mode = True or false Use compression for Local Mode operations = True or false Use deduplication for Local Mode operations = True or false</td>
</tr>
<tr>
<td>Tags associated with the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Whether the View Connection Server instance is paired with a security server</td>
<td>No</td>
<td>0 = Not paired 1 = Paired</td>
</tr>
<tr>
<td>The distinguished name (DN) of the View Connection Server instance in LDAP</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Length of time the security server pairing password is valid</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>The host/node name of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The version number only of the View Connection Server instance</td>
<td>No</td>
<td>5.1.0</td>
</tr>
<tr>
<td>The full build and version of the View Connection Server instance</td>
<td>No</td>
<td>5.1.0-123455</td>
</tr>
<tr>
<td>Auto-reconnect to the secure gateway</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Tunnel client protocol</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Protocol the View Connection Server instance or security server listens on</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>The View Connection Server instance's build number</td>
<td>No</td>
<td>123456</td>
</tr>
<tr>
<td>Name of the View Connection Server replicated group, typically the first View Connection Server instance's node name</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>DNS name of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>IP address of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>NetBIOS host name of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The current number of desktops that have been checked out</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The maximum number of desktops that have been checked out</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The current number of sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The maximum number of sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The current number of View Composer sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
</tbody>
</table>
Table 15-8. Data Collected from View Connection Server for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The maximum number of View Composer sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The version of the View Connection Server instance</td>
<td>No</td>
<td>5.1.0</td>
</tr>
<tr>
<td>Number of times individual PowerShell cmdlets have been invoked</td>
<td>No</td>
<td>List of integers</td>
</tr>
<tr>
<td>Login rate, using passwords, over time</td>
<td>No</td>
<td>Float</td>
</tr>
<tr>
<td>Login rate, using the SSL server certificate, over time</td>
<td>No</td>
<td>Float</td>
</tr>
<tr>
<td>Average percent CPU utilization</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Average percent memory utilization</td>
<td>No</td>
<td>Integer</td>
</tr>
</tbody>
</table>

Table 15-9. Status Information Collected from View Connection Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The View Connection Server instance's build number</td>
<td>No</td>
<td>123456</td>
</tr>
<tr>
<td>Name of the View Connection Server replicated group, typically the first View Connection Server instance's node name</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>DNS name of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>IP address of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>NetBIOS host name of the View Connection Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The current number of desktops that have been checked out</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The maximum number of desktops that have been checked out</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The current number of sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The maximum number of sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The current number of View Composer sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The maximum number of View Composer sessions on this View Connection Server instance</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The version of the View Connection Server instance</td>
<td>No</td>
<td>5.1.0</td>
</tr>
</tbody>
</table>

Table 15-10. Dynamic Usage Data Collected from View Connection Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of times individual PowerShell cmdlets have been invoked</td>
<td>No</td>
<td>List of integers</td>
</tr>
<tr>
<td>Login rate, using passwords, over time</td>
<td>No</td>
<td>Float</td>
</tr>
</tbody>
</table>
Table 15-10. Dynamic Usage Data Collected from View Connection Server for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login rate, using the SSL server certificate, over time</td>
<td>No</td>
<td>Float</td>
</tr>
<tr>
<td>Average percent CPU utilization</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Average percent memory utilization</td>
<td>No</td>
<td>Integer</td>
</tr>
</tbody>
</table>

Security Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from security server fields. Fields containing sensitive information are made anonymous.

Table 15-11. Security Server Data Collected for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of PCoIP sessions that are running on the security server secure gateway</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The number of sessions of any type that are running on the security server secure gateway</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The security server build number</td>
<td>No</td>
<td>123456</td>
</tr>
<tr>
<td>The host name of the security server</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>IPsec is active.</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The secure gateway is down.</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The current number of sessions</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The URL of the secure gateway</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The security server version number</td>
<td>No</td>
<td>5.1.0</td>
</tr>
</tbody>
</table>

Desktop Pool Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain View desktop pool fields. Fields containing sensitive information are made anonymous.

Table 15-12. Data Collected from View Desktop Pools for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The common name (CN) for the View desktop pool entry in View LDAP</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The descriptive, display name of the desktop pool</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The desktop pool is disabled</td>
<td>No</td>
<td>True or false</td>
</tr>
</tbody>
</table>
**Table 15-12.** Data Collected from View Desktop Pools for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The View Administrator folder under which this desktop pool is grouped</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
| The list of virtual machine Distinguished Names (DNs) that belong to the desktop pool | No                           | An example list item: \
|                                                                             |                              | ["CN=8f11d7cf-b0ef-43ad-92ce-691aa929d3c4,OU=Servers,DC=vdi,DC=vmware,DC=int"] |
| Are multiple sessions allowed in the desktop pool?                          | No                           | True or false                                                                 |
| Are users of this desktop pool allowed to reset their desktops?             | No                           | Off, Optional, or Required                                                   |
| Time after which a forced logoff message is displayed                       | No                           | True or false                                                                 |
| The Distinguished Name (DN) of the vCenter Server instance that manages the desktops in the pool | No                           | "CN=e7a718de-d0f7-444a-9452-156dce289828,OU=VirtualCenter,OU=Properties,DC=vdi,DC=vmware,DC=int" |
| Minimum number of desktops in the pool                                       | No                           | Integer                                                                      |
| Maximum number of desktops in the pool                                       | No                           | Integer                                                                      |
| Number of spare, provisioned desktops in the pool                           | No                           | Integer                                                                      |
| Deletion policy for the desktop pool                                        | No                           | Default, DeleteOnUse, or RefreshOnUse                                       |
| DNS suffix used in provisioning                                             | Yes                          | None                                                                          |
| The naming pattern (prefix) to use for auto-deployed virtual machine names  | Yes                          | None                                                                          |
| The template from which to clone virtual machines                           | Yes                          | None                                                                          |
| The folder in vCenter Server in which deployed virtual machines are stored   | Yes                          | None                                                                          |
| The resource pool used for the virtual machines                              | Yes                          | None                                                                          |
| A list of datastores                                                        | Yes                          | None                                                                          |
| The customization specification used to deploy virtual machines             | Yes                          | None                                                                          |
| Enable auto-provisioning for the desktop pool                                | No                           | True or false                                                                 |
| Errors encountered while provisioning                                       | No                           | True or false                                                                 |
| Stop provisioning when an error is encountered                               | No                           | True or false                                                                 |
Table 15-12. Data Collected from View Desktop Pools for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start provisioning</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Pool values have been calculated</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The parent virtual machine used to provision linked clones</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The snapshot name used for linked-clone provisioning</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The snapshot ID used for linked-clone provisioning</td>
<td>No</td>
<td>&quot;snapshot-38685&quot;</td>
</tr>
<tr>
<td>Deployment group ID used by the View Composer service</td>
<td>No</td>
<td>&quot;7119316F-00A8-463D-BBBA-c3000F105AEB&quot;</td>
</tr>
<tr>
<td>View Composer persistent disk datastore path</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Type of View Composer disk</td>
<td>No</td>
<td>&quot;SystemDisposable&quot;, UserProfile, and so on</td>
</tr>
<tr>
<td>Create the persistent disk as a sparse disk</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The drive mount letter for the persistent disk or disposable data disk</td>
<td>No</td>
<td>&quot;A&quot;, &quot;C&quot;, and so on</td>
</tr>
<tr>
<td>Target size of the persistent disk</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Type of refresh policy</td>
<td>No</td>
<td>Always, Never, or Conditional</td>
</tr>
<tr>
<td>Usage threshold for refresh operations</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Time threshold for refresh operations</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Level of overcommit for a datastore that stores linked clones</td>
<td>No</td>
<td>None, Conservative, Moderate, Aggressive</td>
</tr>
<tr>
<td>Datastore path for a datastore that stores linked clones</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>List of IDs this datastore is used for</td>
<td>No</td>
<td>List of GUIDs, such as the following: [&quot;7119316F-00A8-463D-BBBA-c3000F105AEB&quot;]</td>
</tr>
<tr>
<td>Offline published View Transfer Server package chain</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Desktop state</td>
<td>No</td>
<td>Ready, Pre-provisioned, Cloning, Cloning Error, Customizing, Deleting, Maintenance, Error, or Logout</td>
</tr>
<tr>
<td>Assign a desktop to a user when the user first logs in</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Flags for the pool</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Multimonitor configuration settings</td>
<td>No</td>
<td>svga.maxWidth:int, svga.vramSize:int, svga.maxHeight:int, svga.enable3d:bool, svga.numDisplays:int</td>
</tr>
<tr>
<td>An individual desktop was converted to a manual pool</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The linked-clone pool uses native snapshot cloning with VAAI</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>CBRC is enabled</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Frequency that the CBRC cache is refreshed</td>
<td>No</td>
<td>Integer</td>
</tr>
</tbody>
</table>
Table 15-12. Data Collected from View Desktop Pools for the Customer Experience Improvement Program (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBRC cache refresh blackout periods</td>
<td>No</td>
<td>List</td>
</tr>
<tr>
<td>The disk types that are cached for CBRC (OS disks, persistent disks)</td>
<td>No</td>
<td>List</td>
</tr>
</tbody>
</table>

Desktop Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from View desktop fields and from vCenter Server fields that describe desktop virtual machines. Fields containing sensitive information are made anonymous.

Table 15-13. Data Collected from View Desktops for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The desktop was marked as dirty. The desktop was used when useonce=true, and therefore should not accept new sessions</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The desktop was checked out for use in local mode</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The GUID that identifies the offline session</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The user who checked out the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>State of a desktop that is used in local mode</td>
<td>No</td>
<td>Checked in, Checked out</td>
</tr>
<tr>
<td>The type of data transfer from a client to the datacenter</td>
<td>No</td>
<td>Full check-in, Replicate and stay offline</td>
</tr>
<tr>
<td>Determines if a replication was requested from View Administrator</td>
<td>No</td>
<td>Set or Unset</td>
</tr>
<tr>
<td>The time when the explicit replication was requested</td>
<td>No</td>
<td>Time</td>
</tr>
<tr>
<td>The time when the desktop’s current offline session started</td>
<td>No</td>
<td>Time</td>
</tr>
<tr>
<td>The host name of the client computer that checked out the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The IP address of the client computer that checked out the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The time when the offline desktop last received a policy update</td>
<td>No</td>
<td>Time</td>
</tr>
<tr>
<td>A snapshot ID used for local mode</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>A list of snapshot IDs used for local mode</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Mapping of devices to change IDs</td>
<td>No</td>
<td>A set of IDs such as the following: 2000=01874583;01874583&amp;2016=3910f513;3910f513</td>
</tr>
<tr>
<td>The offline desktop is pending a roll back</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The time that the desktop has been offline (not updated by replications)</td>
<td>No</td>
<td>Date</td>
</tr>
<tr>
<td>An identifier for the virtual machine that is used to correlate data</td>
<td>No</td>
<td>vm-10</td>
</tr>
<tr>
<td>Sysprep customization is used for the desktop</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Description</td>
<td>Is This Field Made Anonymous?</td>
<td>Example Value</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Timeout value. The period of time before the desktop is disconnected.</td>
<td>No</td>
<td>Time</td>
</tr>
<tr>
<td>A random ID for the View Agent for this desktop</td>
<td>No</td>
<td>GUID</td>
</tr>
<tr>
<td>Miscellaneous configuration values</td>
<td>No</td>
<td>Integers and booleans (true or false)</td>
</tr>
<tr>
<td>The GUID of the base-image package that is used for the offline desktop</td>
<td>No</td>
<td>GUID</td>
</tr>
<tr>
<td>The ID of the endpoint that checked out the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>View LDAP identifier for the previously View Composer persistent disk</td>
<td>No</td>
<td>LDAP entry</td>
</tr>
<tr>
<td>Thinapps that are entitled to the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Thinapps that are pending an uninstallation</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Thinapps that are installed in the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The state of the desktop</td>
<td>No</td>
<td>Undefined, Pre-provisioned, Cloning, Cloning error, Customizing, Ready, Deleting, Maintenance, Error, or Logout</td>
</tr>
<tr>
<td>Timestamp of when customization started</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The virtual machine is powered on for customization</td>
<td>No</td>
<td>Integer. The values are 0 or 1.</td>
</tr>
<tr>
<td>The virtual machine is powered on</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The virtual machine is suspended</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The virtual machine state is in transition</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The virtual machine is configured</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The path to the virtual machine in vCenter Server</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Customization template used to customize the desktop</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>View Composer linked clone ID for the desktop</td>
<td>No</td>
<td>GUID of the linked clone</td>
</tr>
<tr>
<td>The virtual machine missing in vCenter Server</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>Number of times View tried to power off the virtual machine</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Status of CBRC</td>
<td>No</td>
<td>Off, Current, Out of date, or Error</td>
</tr>
<tr>
<td>Time of the latest CBRC refresh</td>
<td>No</td>
<td>Date</td>
</tr>
<tr>
<td>Time of the latest CBRC error</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Time of the latest incomplete attempt to configure CBRC</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The version of View Agent on the desktop</td>
<td>No</td>
<td>5.1.0-551711</td>
</tr>
<tr>
<td>View Persona Management is enabled on the desktop</td>
<td>No</td>
<td>True or false</td>
</tr>
</tbody>
</table>
Table 15-14. Desktop Virtual Machine Data Collected from vCenter Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The virtual machine hardware version</td>
<td>No</td>
<td>v8</td>
</tr>
<tr>
<td>The amount of RAM that is allocated to the virtual machine</td>
<td>No</td>
<td>1024</td>
</tr>
<tr>
<td>The number of virtual CPUs that are configured in the virtual machine</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The operating system installed in the virtual machine</td>
<td>No</td>
<td>Microsoft Windows 7 (32-bit), Microsoft Windows 8 (32-bit), Microsoft Windows Server 2008 R2 (64-bit), and so on</td>
</tr>
</tbody>
</table>

vCenter Server Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from certain vCenter Server fields. Fields containing sensitive information are made anonymous.

Table 15-15. Host System and Status Data Collected from vCenter Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>The time that View last communicated with this vCenter Server host</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The URL of the vCenter Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The API version of the vCenter Server instance</td>
<td>No</td>
<td>5.0</td>
</tr>
<tr>
<td>The build number of the vCenter Server instance</td>
<td>No</td>
<td>456789</td>
</tr>
<tr>
<td>The version number of the vCenter Server instance</td>
<td>No</td>
<td>5.0.0</td>
</tr>
<tr>
<td>The internal status code of the connection status between vCenter Server and View Connection Server</td>
<td>No</td>
<td>Status_Up</td>
</tr>
<tr>
<td>Description of the connection status code</td>
<td>No</td>
<td>Connected</td>
</tr>
<tr>
<td>The vCenter Server SSL certificate is valid.</td>
<td>No</td>
<td>True or false</td>
</tr>
<tr>
<td>The reason that the SSL certificate is not valid</td>
<td>No</td>
<td>Name mismatch, not trusted, cannot check revocation, and so on.</td>
</tr>
</tbody>
</table>

Table 15-16. Datastore Data Collected from vCenter Server for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk capacity of this datastore</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Free disk space on this datastore</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The type of storage</td>
<td>No</td>
<td>NFS, VMFS</td>
</tr>
<tr>
<td>Multiple hosts can access this datastore concurrently.</td>
<td>No</td>
<td>True or false</td>
</tr>
</tbody>
</table>
View Transfer Server and Transfer Server Repository Data Collected by VMware

If you join the customer experience improvement program, VMware collects data from View Transfer Server fields and fields that describe the Transfer Server repository. Fields containing sensitive information are made anonymous.

Table 15-17. View Transfer Server and Transfer Server Repository Data Collected for the Customer Experience Improvement Program

<table>
<thead>
<tr>
<th>Description</th>
<th>Is This Field Made Anonymous?</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name of the View Transfer Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Number of active transfers</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Path of the Transfer Server repository. This is a View Transfer Server field.</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>The status of View Transfer Server instance</td>
<td>No</td>
<td>Ready, Maintenance, or Error</td>
</tr>
<tr>
<td>Total amount of disk space on the View Transfer Server virtual computer</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Amount of used disk space on the View Transfer Server virtual computer</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>The version and build number of the View Transfer Server instance</td>
<td>No</td>
<td>5.0.0.123456</td>
</tr>
<tr>
<td>Path to the Transfer Server repository. This is a global View LDAP field.</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Amount of used disk space in the Transfer Server repository</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Amount of free disk space in the Transfer Server repository</td>
<td>No</td>
<td>Integer</td>
</tr>
<tr>
<td>Mount point on the View Transfer Server instance</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>
Troubleshooting View Components

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,” on page 380
- “Monitor Events in View Manager,” on page 380
- “Send Messages to Desktop Users,” on page 381
- “Display Desktops with Suspected Problems,” on page 381
- “Troubleshoot a Problem Desktop Virtual Machine Using the vSphere Web Client,” on page 382
- “Manage Desktops and Policies for Unentitled Users,” on page 383
- “Collecting Diagnostic Information for VMware Horizon View,” on page 383
- “Update Support Requests,” on page 387
- “Troubleshooting Network Connection Problems,” on page 388
- “Troubleshooting Desktop Pool Creation Problems,” on page 391
- “Troubleshooting an Unsuccessful Security Server Pairing with View Connection Server,” on page 395
- “Troubleshooting View Server Certificate Revocation Checking,” on page 395
- “Troubleshooting Smart Card Certificate Revocation Checking,” on page 396
- “Troubleshooting USB Redirection Problems,” on page 397
- “Troubleshooting Desktops That Are Repeatedly Deleted and Recreated,” on page 398
- “Troubleshooting QuickPrep Customization Problems,” on page 399
- “View Composer Provisioning Errors,” on page 400
- “Removing Orphaned or Deleted Linked Clones,” on page 401
- “Finding and Unprotecting Unused View Composer Replicas,” on page 402
- “Windows XP Linked Clones Fail to Join the Domain,” on page 404
- “Troubleshooting GINA Problems on Windows XP Desktops,” on page 404
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.

- **ProblemDesktops**
  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 Horizon View Integration* document.

In addition to monitoring events in View Administrator, you can generate View events in Syslog format so that the event data can be accessible to analytics software. See “Generating View Event Log Messages in Syslog Format Using the -I Option,” on page 417 and "Configure Event Logging for Syslog Servers" in the *VMware Horizon View Installation* document.

Prerequisites

Create and configure the event database as described in the *VMware Horizon 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

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Failure or Audit Success</td>
<td>Reports the failure or success of a change that an administrator or user makes to the operation or configuration of View.</td>
</tr>
<tr>
<td>Error</td>
<td>Reports a failed operation by View Manager.</td>
</tr>
<tr>
<td>Information</td>
<td>Reports normal operations within View.</td>
</tr>
<tr>
<td>Warning</td>
<td>Reports minor problems with operations or configuration settings that might lead to more serious problems over time.</td>
</tr>
</tbody>
</table>

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 desktops, you can ask the users to log out temporarily, or warn them of a future interruption of service. You can send a message to multiple users.

Procedure

1. In View Administrator, click Inventory > Pools.
2. Double-click a pool and click the Sessions tab.
3. Select one or more desktops and click Send Message.
4. Type the message, select the message type, and click OK.

A message type can be Info, Warning, or Error.

The message is sent to all selected desktops in active sessions.

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 the View Desktops plug-in was added to the vSphere Web Client, you can use the vSphere Web Client to search for a View user, display the desktops that are associated with that user, and troubleshoot the underlying virtual machines in vCenter Server. See “Troubleshoot a Problem Desktop Virtual Machine Using the vSphere Web Client,” on page 382.
- If a linked-clone desktop is in an error state, the View Manager automatic recovery mechanism attempts to power on, or shut down and restart, the linked clone. If repeated recovery attempts fail, the linked clone is deleted. In certain situations, a linked clone might be repeatedly deleted and recreated. See “Troubleshooting Desktops That Are Repeatedly Deleted and Recreated,” on page 398.
- 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 411.
- 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 394.
- 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 390.
- 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.

Troubleshoot a Problem Desktop Virtual Machine Using the vSphere Web Client

If a View desktop has a problem, you can use the View Desktops feature in the vSphere Web Client to search for a View user, display the user’s desktop, and troubleshoot problems with the underlying virtual machine in vCenter Server.

For example, if a user calls in with a problem such as a desktop that is performing slowly, you can immediately jump to the user’s virtual machine on the Virtual Machines page in the vSphere Web Client and troubleshoot the issue.

Prerequisites

- Verify that the View Desktops plug-in was added to the vSphere Web Client. See "Adding the View Desktops Plug-in to the vSphere Web Client" in the VMware Horizon View Installation document.
- Verify that you can log in to the vSphere Web Client as a user with the View Administrators role or View Administrators (Read only) role and with the vSphere Administrator privilege for the View desktop virtual machines and vCenter Server folders that store the virtual machines.
  
  If you search for desktops without having the vSphere Administrator privilege, the virtual machine names are displayed as disabled links and you cannot access the virtual machine information.

Procedure

1. Log in to the vSphere Web Client as a user with the View Administrators role or View Administrators (Read only) role and the appropriate vSphere Administrator privileges.

   For example: https://vSphere_Web_Client_IP_address_or_FQDN:9443/vsphere-client/

2. In the Search box, type the username of a View user.
3 Select the username from the search results.

4 Select a desktop from the list of desktops that is associated with the user.

5 Navigate to the Virtual Machines page to see details about the underlying desktop virtual machine.

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 427.

Procedure

1 In View Administrator, select Desktops.

2 Select More Commands > View Unentitled Desktops.

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 Desktops 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 Horizon View

You can collect diagnostic information to help VMware Technical Support diagnose and resolve issues with VMware Horizon View.

You can collect diagnostic information for various components of View. How you collect this information varies depending on the View component.

- **Create a Data Collection Tool Bundle for View Agent** on page 384
  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 can also obtain the DCT bundle manually, without using `vdmadmin`.

- **Save Diagnostic Information for View Client** on page 385
  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 385
  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 386
  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 386

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 can also obtain the DCT bundle manually, without using vdmadmin.

For your convenience, you can use the vdmadmin command on a View Connection Server instance to request a DCT bundle from a View desktop. The bundle is returned to View Connection Server.

You can alternatively log in to a specific View desktop and run a support command that creates the DCT bundle on that desktop. If the operating system of the View desktop is Windows 8 or Windows 7 and User Account Control (UAC) is turned on, you must obtain the DCT bundle in this fashion.

Procedure

1. Log in as a user with the required privileges.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On View Connection Server, using vdmadmin</td>
<td>Log in to a standard or replica instance View Connection Server as a user with the Administrators role.</td>
</tr>
<tr>
<td>On the View desktop</td>
<td>Log in to the View desktop as a user with administrative privileges.</td>
</tr>
</tbody>
</table>

2. Open a command prompt and run the command to generate the DCT bundle.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>On View Connection Server, using vdmadmin</td>
<td>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</td>
</tr>
<tr>
<td>On the View desktop</td>
<td>Change directories to c:\Program Files\VMware\VMware View\Agent\DCT and run the following command: support</td>
</tr>
</tbody>
</table>

The command writes the bundle to the specified output file.

Example: Example of Using vdmadmin to Create 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 388.

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 View processes.

   The information is written to a zip file in a folder on the client machine’s desktop.


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 computer 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 386.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Resets the logging level to the default value.</td>
</tr>
<tr>
<td>1</td>
<td>Selects a normal level of logging (default).</td>
</tr>
<tr>
<td>2</td>
<td>Selects a debug level of logging.</td>
</tr>
<tr>
<td>3</td>
<td>Selects full logging.</td>
</tr>
</tbody>
</table>

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 View component that you want to collect diagnostic information for.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Agent</td>
<td>Change to the C:\Program Files\VMware View\Agent\DCT directory.</td>
</tr>
<tr>
<td>View Client</td>
<td>Change to the C:\Program Files\VMware View\Client\DCT directory.</td>
</tr>
<tr>
<td>View Connection Server</td>
<td>Change to the C:\Program Files\VMware View\Server\DCT directory.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Resets the logging level to the default value.</td>
</tr>
<tr>
<td>1</td>
<td>Selects a normal level of logging (default).</td>
</tr>
<tr>
<td>2</td>
<td>Selects a debug level of logging.</td>
</tr>
<tr>
<td>3</td>
<td>Selects full logging.</td>
</tr>
<tr>
<td>4</td>
<td>Selects informational logging for PCoIP (View Agent and View Client only).</td>
</tr>
<tr>
<td>5</td>
<td>Selects debug logging for PCoIP (View Agent and View Client only).</td>
</tr>
<tr>
<td>6</td>
<td>Selects informational logging for virtual channels (View Agent and View Client only).</td>
</tr>
<tr>
<td>7</td>
<td>Selects debug logging for virtual channels (View Agent and View Client only).</td>
</tr>
<tr>
<td>8</td>
<td>Selects trace logging for virtual channels (View Agent and View Client only).</td>
</tr>
</tbody>
</table>

   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.

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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 4172</td>
<td>From View Client to the security server or View Connection Server host.</td>
</tr>
<tr>
<td>UDP 4172</td>
<td>Between View client and the security server or View Connection Server host, in both directions.</td>
</tr>
<tr>
<td>TCP 4172</td>
<td>From the security server or View Connection Server host to the View desktop.</td>
</tr>
<tr>
<td>UDP 4172</td>
<td>Between the security server or View Connection Server host and the View desktop, in both directions.</td>
</tr>
</tbody>
</table>

- 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: **10.20.30.40:4172**

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 Server Being Overloaded

If vCenter Server 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 Server.
- Configure additional vCenter Server instances.
  
  For more information about configuring vCenter, see the *VMware Horizon 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 an Unsuccessful Security Server Pairing with View Connection Server

A security server might not be working if it failed to pair successfully with a View Connection Server instance.

**Problem**

The following security server issues might occur if a security server failed to pair with View Connection Server:

- When you try to install the security server a second time, the security server cannot connect to View Connection Server.
- View Clients cannot connect to View. The following error message appears: The View Connection Server authentication failed. No gateway is available to provide a secure connection to a desktop. Contact your network administrator.
- The security server is displayed in the View Administrator dashboard as Down.

**Cause**

This problem can occur if you started to install a security server and the attempt was cancelled or otherwise aborted after you entered a security server pairing password.

**Solution**

If you intend to keep the security server in your View environment, take these steps:

1. In View Administrator, click **View Configuration > Servers**.
2. In the Security Servers tab, select a security server and click **More Commands > Prepare for Upgrade or Reinstallation** and click OK.
3. Select the Connection Servers tab, select the View Connection Server instance that you want to pair with the security server, click **More Commands > Specify a Security Server Pairing Password**, enter a password, and click OK.
4. Install the security server again.

If you intend to remove the security server entry from your View environment, run the `vdmadmin -S` command.

For example: `vdmadmin -S -r -s security_server_name`

Troubleshooting View Server Certificate Revocation Checking

A security server or a View Connection Server instance that is used for secure View Client connections might show as red in View Administrator if certificate revocation checking cannot be performed on the server's SSL certificate.

**Problem**

A security server or View Connection Server icon is red on the View Administrator dashboard. The View server's status shows the following message: Server's certificate cannot be checked.

**Cause**

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a View Connection Server instance cannot reach the servers that provide revocation checking because of firewalls or other controls.
A View Connection Server instance performs certificate revocation checking on its own certificate and on those of the security servers paired to it. By default, the VMware View Connection Server Service is started with the LocalSystem account. When it runs under LocalSystem, a View Connection Server instance cannot use the proxy settings configured in Internet Explorer to access the CRL DP URL or OCSP responder to determine the revocation status of the certificate.

You can use Microsoft Netshell commands to import the proxy settings to the View Connection Server instance so that the server can access the certificate revocation checking sites on the Internet.

### Solution

1. On the View Connection Server computer, open a command-line window with the **Run as administrator** setting.
   
   For example, click **Start**, type **cmd**, right-click the **cmd.exe** icon, and select **Run as administrator**.

2. Type **netsh** and press Enter.

3. Type **winhttp** and press Enter.

4. Type **show proxy** and press Enter.

   Netshell shows that the proxy was set to DIRECT connection. With this setting, the View Connection Server computer cannot connect to the Internet if a proxy is in use in your organization.

5. Configure the proxy settings.

   For example, at the **netsh winhttp>** prompt, type **import proxy source=ie**.

   The proxy settings are imported to the View Connection Server computer.

6. Verify the proxy settings by typing **show proxy**.

7. Restart the VMware View Connection Server Service.

8. On the View Administrator dashboard, verify that the security server or View Connection Server icon is green.

### Troubleshooting Smart Card Certificate Revocation Checking

The View Connection Server instance or security server that has the smart card connected cannot perform certificate revocation checking on the server’s SSL certificate unless you have configured smart card certificate revocation checking.

**Problem**

Certificate revocation checking might fail if your organization uses a proxy server for Internet access, or if a View Connection Server instance or security server cannot reach the servers that provide revocation checking because of firewalls or other controls.

---

**IMPORTANT** Make sure the CRL file is up to date.

**Cause**

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 (Certificate Authority) that issued the certificates. OCSP is a certificate validation protocol that is used to get the revocation status of an X.509 certificate. The CA must be accessible from the View Connection Server or security server host. This issue can only occur if you configured revocation checking of smart card certificates. See “Using Smart Card Certificate Revocation Checking,” on page 165.
Solution

1. Create your own (manual) procedure for downloading an up-to-date CRL from the CA website you use to a path on your View server.

2. 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`

3. Add the `enableRevocationChecking` and `crlLocation` properties in the `locked.properties` file to the local path to where the CRL is stored.

4. Restart the View Connection Server service or security server service to make your changes take effect.

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](http://kb.vmware.com/kb/1021409).

- By default, View Client for Windows does not allow you to select keyboard, mouse, smart card and audio-out devices for redirection. See [http://kb.vmware.com/kb/1011600](http://kb.vmware.com/kb/1011600).

- RDP does not support the redirection of USB HID devices for the console session, or of smart card readers. See [http://kb.vmware.com/kb/1011600](http://kb.vmware.com/kb/1011600).

- Windows Mobile Device Center can prevent the redirection of USB devices for RDP sessions. See [http://kb.vmware.com/kb/1019205](http://kb.vmware.com/kb/1019205).

- For some USB HID devices, you must configure the virtual machine to update the position of the mouse pointer. See [http://kb.vmware.com/kb/1022076](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](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](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.

For View Client from View 5.0.x or earlier, missing or disabled drivers for the device that is being redirected on the client. View Client from View 5.0.x or earlier requires that you install the USB driver for a redirected device on the client. View Client from View 5.1 and later does not have this requirement.”

**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 ws_vhub, and the log on the client for entries of class vmware-view-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 Host Controller and VMware View Virtual USB Hub drivers if these drivers are missing or re-enable them if they are disabled.

**Troubleshooting Desktops That Are Repeatedly Deleted and Recreated**

View Manager can repeatedly delete and recreate linked-clone and full-clone desktops that are in an Error state.

**Problem**

A linked-clone or full-clone desktop is created in an Error state, deleted, and recreated in an Error state. This cycle keeps repeating.

**Cause**

When a large desktop pool is provisioned, one or more virtual machines might end up in an Error state. The View Manager automatic recovery mechanism attempts to power on the failed virtual machine. If the virtual machine does not power on after a certain number of attempts, View Manager deletes the virtual machine. Following the pool size requirements, View Manager creates a new virtual machine, often with the same desktop name as the original desktop. If the new virtual machine is provisioned with the same error, that virtual machine is deleted, and the cycle repeats.

Automatic recovery is performed on linked-clone and full-clone desktops.

If automatic recovery attempts fail for a virtual machine, View Manager deletes the virtual machine only if it is a floating desktop or a dedicated desktop that is not assigned to a user. Also, View Manager does not delete virtual machines when pool provisioning is disabled.

**Solution**

Examine the parent virtual machine or template that was used to create the desktop pool. Check for errors in the virtual machine or guest operating system that might cause the error in the virtual machine.
For linked clones, resolve errors in the parent virtual machine and take a new snapshot.

- If many desktops are in an Error state, use the new snapshot or template to recreate the pool.
- If most desktops are healthy, select the desktop pool in View Administrator, click Edit, select the vCenter Settings tab, select the new snapshot as a default base image, and save your edits.

    New linked-clone desktops are created using the new snapshot.

For full clones, resolve errors in the virtual machine, generate a new template, and recreate the pool.

**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:\tmp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\tmp\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\myvbs.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\myvbs.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

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The policy was applied successfully. <strong>Note</strong>: 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.</td>
</tr>
<tr>
<td>1</td>
<td>Failed to set the computer name.</td>
</tr>
<tr>
<td>2</td>
<td>Failed to redirect the user profiles to the View Composer persistent disk.</td>
</tr>
<tr>
<td>3</td>
<td>Failed to set the computer's domain account password.</td>
</tr>
<tr>
<td>4</td>
<td>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 see the old profile data.</td>
</tr>
<tr>
<td>5</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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. |
### Table 16-2. View Composer Provisioning Errors (Continued)

<table>
<thead>
<tr>
<th>Error</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>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.</td>
</tr>
<tr>
<td>16</td>
<td>The View Composer agent did not start because the volume license for the guest OS was not activated.</td>
</tr>
<tr>
<td>17</td>
<td>The View Composer agent did not start. The agent timed out while waiting for Sysprep to start.</td>
</tr>
<tr>
<td>18</td>
<td>The View Composer agent failed to join the linked-clone virtual machine to a domain during customization.</td>
</tr>
<tr>
<td>19</td>
<td>The View Composer agent failed to execute a post-synchronization script.</td>
</tr>
<tr>
<td>20</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Removing Orphaned or Deleted Linked Clones

Under certain conditions, linked-clone data in View, View Composer, and vCenter Server might get out of synchronization, and you might be unable to provision or delete linked-clone desktops.

**Problem**

- You cannot provision a linked-clone desktop pool.
- Provisioning linked-clone desktops fails, and the following error occurs: Virtual machine with Input Specification already exists
- In View Administrator, linked-clone desktops are stuck in a Deleting state. You cannot restart the Delete command in View Administrator because the desktops are already in the Deleting state.

**Cause**

This issue occurs if the View Composer database contains information about linked clones that is inconsistent with the information in View LDAP, Active Directory, or vCenter Server. Several situations can cause this inconsistency:

- The linked-clone virtual machine name is changed manually in vCenter Server after the pool was created, causing View Composer and vCenter Server refer to the same virtual machine with different names.
- A storage failure or manual operation causes the virtual machine to be deleted from vCenter Server. The linked-clone desktop data still exists in the View Composer database, View LDAP, and Active Directory.
- While a pool is being deleted from View Administrator, a networking or other failure leaves the virtual machine in vCenter Server.

**Solution**

If the virtual machine name was renamed in vSphere Client after the desktop pool was provisioned, try renaming the virtual machine to the name that was used when it was deployed in View.

If other database information is inconsistent, use the `SviConfig RemoveSviClone` command to remove these items:

- The linked clone database entries from the View Composer database
- The linked clone machine account from Active Directory
- The linked clone virtual machine from vCenter Server
The sviConfig utility is located on the computer on which View Composer is installed in the following location:

- 32-bit computers: Install_drive\Program Files\VMware\VMware View Composer
- 64-bit computers: Install_drive\Program Files (x86)\VMware\VMware View Composer

**IMPORTANT** Only experienced View Composer administrators should use the sviConfig utility. This utility is intended to resolve issues relating to the View Composer service.

Take these steps:

1. Verify that the View Composer service is running.
2. From a Windows command prompt on the View Composer computer, run the sviConfig RemoveSviClone command in the following form:

   ```
   sviConfig -operation=removesviclone
   -VmName=virtual machine name
   [-AdminUser=local administrator username]
   -AdminPassword=local administrator password
   [-ServerUrl=View Composer server URL]
   ```

   For example:

   ```
   sviConfig -operation=removesviclone -vmname=MyLinkedClone
   -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
   ```

   The VmName and AdminPassword parameters are required. The default value of the AdminUser parameter is Administrator. The default value of the ServerURL parameter is https://localhost:18443/SviService/v2_0

   For more information about removing virtual machine information from View LDAP, see VMware Knowledge Base article 2015112: Manually deleting linked clones or stale virtual desktop entries from VMware View Manager 4.5 and later.

**Finding and Unprotecting Unused View Composer Replicas**

Under certain conditions, View Composer replicas might remain in vCenter Server when they no longer have any linked clones associated with them.

**Problem**

An unused replica remains in a vCenter Server folder. You are unable to remove the replica by using vSphere Client.

**Cause**

Network outages during View Composer operations, or removing the associated linked clones directly from vSphere without using the proper View commands, might leave an unused replica in vCenter Server.

Replicas are protected entities in vCenter Server. They cannot be removed by ordinary vCenter Server or vSphere Client management commands.

**Solution**

Use the sviConfig FindUnusedReplica command to find the replica in a specified folder. You can use the -Move parameter to move the replica to another folder. The -Move parameter unprotects an unused replica before moving it.

**IMPORTANT** Only experienced View Composer administrators should use the sviConfig utility. This utility is intended to resolve issues relating to the View Composer service.
The SvConfig utility is located in the following location on the computer on which View Composer is installed:

- 32-bit computers: \Install_drive\Program Files\VMware\VMware View Composer
- 64-bit computers: \Install_drive\Program Files (x86)\VMware\VMware View Composer

Before you begin, verify that no linked clones are associated with the replica.

Familiarize yourself with the SvConfig FindUnusedReplica parameters:

- **DsnName**. The DSN that must be used to connect to the database.
- **UserName**. The user name used to connect to the database. If this parameter is not specified, Windows authentication is used.
- **Password**. The password for the user that connects to the database. If this parameter is not specified and Windows authentication is not used, you are prompted to enter the password later.
- **ReplicaFolder**. The name of the replica folder. Use an empty string for the root folder. The default value is VMwareViewComposerReplicaFolder.
- **UnusedReplicaFolder**. The name of the folder to contain all unused replicas. The default value is UnusedViewComposerReplicaFolder. Use this parameter to specify the destination folder when you use the Move parameter.
- **OutputDir**. The name of the output directory in which the list of unused replicas, stored in the unused-replica-*.txt file, is generated. The default value is the current working directory.
- **Move**. Determines whether to unprotect unused replica virtual machines and move them to a specified folder. The UnusedReplicaFolder parameter specifies the destination folder. The default value of the Move parameter is false.

The DsnName, UserName, and Password parameters are required. The DsnName cannot be an empty string.

Take these steps:

1. Stop the View Composer service.
2. From a Windows command prompt on the View Composer computer, run the SvConfig FindUnusedReplica command in the following form:

   ```bash
   sviconfig -operation=findunusedreplica
   -DsnName=DSN name
   -Username=Database administrator username
   -Password=Database administrator password
   [-ReplicaFolder=Replica folder name]
   [-UnusedReplicaFolder=Unused replica folder name.]
   [-OutputDir=Output file directory]
   [-Move=true or false]
   ```

   For example:

   ```bash
   sviconfig -operation=FindUnusedReplica -DsnName=SVI
   -Username=SVIUser -Password=1234 -Move=True
   ```

3. Restart the View Composer service.
4. (Optional) After the replica is moved to the new folder, remove the replica virtual machine from vCenter Server.
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:

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 vdmGinaChain.dll 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.

**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
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 Horizon View Integration document.

- **vdmadmin Command Usage** on page 409
  The syntax of the `vdmadmin` command controls its operation.

- **Configuring Logging in View Agent Using the `-A` Option** on page 411
  You can use the `vdmadmin` command with the `-A` option to configure logging by View Agent.

- **Overriding IP Addresses Using the `-A` Option** on page 413
  You can use the `vdmadmin` command with the `-A` option to override the IP address reported by a View Agent.

- **Setting the Name of a View Connection Server Group Using the `-C` Option** on page 414
  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.

- **Updating Foreign Security Principals Using the `-F` Option** on page 414
  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.

- **Listing and Displaying Health Monitors Using the `-H` Option** on page 415
  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.

- **Listing and Displaying Reports of View Manager Operation Using the `-I` Option** on page 416
  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.

- **Generating View Event Log Messages in Syslog Format Using the `-I` Option** on page 417
  You can use the `vdmadmin` command with the `-I` option to record View event messages in Syslog format in event log files. Many third-party analytics products require flat-file Syslog data as input for their analytics operations.

- **Assigning Dedicated Desktops Using the `-L` Option** on page 418
  You can use the `vdmadmin` command with the `-L` option to assign desktops from a dedicated pool to users.
Displaying Information About Machines Using the -M Option on page 419
You can use the `vdmadmin` command with the `-M` option to display information about the configuration of virtual machines or physical computers.

Reclaiming Disk Space on Virtual Machines Using the -M Option on page 420
You can use the `vdmadmin` command with the `-M` option to mark a linked-clone virtual machine for disk space reclamation. View directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in View Administrator.

Configuring Domain Filters Using the -N Option on page 421
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 423
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 427
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 428
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 432
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 or Security Server Using the -S Option on page 432
You can use the `vdmadmin` command with the `-S` option to remove the entry for a View Connection Server instance or security server from the View Manager configuration.

Setting the Split Limit for Publishing View Transfer Server Packages Using the -T Option on page 433
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 434
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 434
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.
Recovering a Local Desktop by Using the -V Option When the Desktop Was Modified in the Datacenter on page 435

When a local mode operation such as a check-out, check-in, or replication is performed, View validates that the View desktop’s virtual machine in vCenter Server was not modified since the last synchronization with the local View desktop. If a virtual machine disk in vCenter Server was modified, and the disk is not the same as the local desktop version, you can use the vdmadmin command with the -V option to preserve data on the local desktop and vCenter Server virtual machine and ensure that both versions are synchronized.

Unlocking or Locking Virtual Machines Using the -V Option on page 437

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 438

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 409

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 410

Some vdmadmin command options allow you to specify the format of the output information.

vdmadmin Command Options on page 410

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 39.
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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–csv</td>
<td>Formats the output as comma-separated values.</td>
</tr>
<tr>
<td>–n</td>
<td>Display the output using ASCII (UTF-8) characters. This is the default character set for comma-separated values and plain text output.</td>
</tr>
<tr>
<td>–w</td>
<td>Display the output using Unicode (UTF-16) characters. This is the default character set for XML output.</td>
</tr>
<tr>
<td>–xml</td>
<td>Formats the output as XML.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–A</td>
<td>Administers the information that a View Agent records in its log files. See “Configuring Logging in View Agent Using the -A Option,” on page 411. Overrides the IP address reported by a View Agent. See “Overriding IP Addresses Using the -A Option,” on page 413.</td>
</tr>
<tr>
<td>–C</td>
<td>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 414.</td>
</tr>
<tr>
<td>–F</td>
<td>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 414.</td>
</tr>
<tr>
<td>–H</td>
<td>Displays health information about View Manager services. See “Listing and Displaying Health Monitors Using the -H Option,” on page 415.</td>
</tr>
<tr>
<td>–I</td>
<td>Generates reports about View Manager operation. See “Listing and Displaying Reports of View Manager Operation Using the -I Option,” on page 416.</td>
</tr>
<tr>
<td>–L</td>
<td>Assigns a dedicated desktop to a user or removes an assignment. See “Assigning Dedicated Desktops Using the -L Option,” on page 418.</td>
</tr>
<tr>
<td>–M</td>
<td>Displays information about a virtual machine or physical computer. See “Displaying Information About Machines Using the -M Option,” on page 419.</td>
</tr>
</tbody>
</table>
### Table 17-2. Vdmadmin Command Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-N</td>
<td>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 421.</td>
</tr>
<tr>
<td>-O</td>
<td>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 427.</td>
</tr>
<tr>
<td>-P</td>
<td>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 427.</td>
</tr>
<tr>
<td>-Q</td>
<td>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 428.</td>
</tr>
<tr>
<td>-R</td>
<td>Reports the first user who accessed a desktop. See “Displaying the First User of a Desktop Using the -R Option,” on page 432.</td>
</tr>
<tr>
<td>-S</td>
<td>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 or Security Server Using the -S Option,” on page 432.</td>
</tr>
<tr>
<td>-T</td>
<td>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 433.</td>
</tr>
<tr>
<td>-U</td>
<td>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 434.</td>
</tr>
<tr>
<td>-V</td>
<td>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 434. 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 437.</td>
</tr>
<tr>
<td>-X</td>
<td>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 438.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the desktop pool.</td>
</tr>
<tr>
<td>-getDCT</td>
<td>Creates a Data Collection Tool (DCT) bundle and saves it to a local file.</td>
</tr>
<tr>
<td>-getlogfile logfile</td>
<td>Specifies the name of the log file to save a copy of.</td>
</tr>
<tr>
<td>-getloglevel</td>
<td>Displays the current logging level of View Agent.</td>
</tr>
<tr>
<td>-getstatus</td>
<td>Displays the status of View Agent.</td>
</tr>
<tr>
<td>-getversion</td>
<td>Displays the version of View Agent.</td>
</tr>
<tr>
<td>-list</td>
<td>List the log files for View Agent.</td>
</tr>
<tr>
<td>-m machine</td>
<td>Specifies the machine within a desktop pool.</td>
</tr>
<tr>
<td>-outfile local_file</td>
<td>Specifies the name of the local file in which to save a DCT bundle or a copy of a log file.</td>
</tr>
<tr>
<td>-setloglevel level</td>
<td>Sets the logging level of View Agent.</td>
</tr>
<tr>
<td></td>
<td>debug Logs error, warning, and debugging events.</td>
</tr>
<tr>
<td></td>
<td>normal Logs error and warning events.</td>
</tr>
<tr>
<td></td>
<td>trace Logs error, warning, informational, and debugging events.</td>
</tr>
</tbody>
</table>

### 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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the desktop pool.</td>
</tr>
<tr>
<td>-i ip_or_dns</td>
<td>Specifies the IP address or resolvable domain name in DNS.</td>
</tr>
<tr>
<td>-m machine</td>
<td>Specifies the name of the machine in a desktop pool.</td>
</tr>
<tr>
<td>-override</td>
<td>Specifies an operation for overriding IP addresses.</td>
</tr>
<tr>
<td>-r</td>
<td>Removes an overridden IP address.</td>
</tr>
</tbody>
</table>

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 View, see the VMware Horizon 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>
<thead>
<tr>
<th>Monitor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBMonitor</td>
<td>Monitors the health of View Connection Server instances.</td>
</tr>
<tr>
<td>DBMonitor</td>
<td>Monitors the health of the events database.</td>
</tr>
<tr>
<td>DomainMonitor</td>
<td>Monitors the health of the View Connection Server host's local domain and all trusted domains.</td>
</tr>
<tr>
<td>SGMonitor</td>
<td>Monitors the health of security gateway services and security servers.</td>
</tr>
<tr>
<td>TSMonitor</td>
<td>Monitors the health of transfer servers.</td>
</tr>
<tr>
<td>VCMonitor</td>
<td>Monitors the health of vCenter servers.</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-instanceid instance_id</td>
<td>Specifies a health monitor instance</td>
</tr>
<tr>
<td>-list</td>
<td>Displays the existing health monitors if a health monitor ID is not specified.</td>
</tr>
<tr>
<td>-list -monitorid monitor_id</td>
<td>Displays the monitor instances for the specified health monitor ID.</td>
</tr>
<tr>
<td>-monitorid monitor_id</td>
<td>Specifies a health monitor ID.</td>
</tr>
</tbody>
</table>
**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]
```

```
```

**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.

You can also use the `vdmadmin` command with the `-I` option to generate View log messages in syslog format. See “Generating View Event Log Messages in Syslog Format Using the -I Option,” on page 417.

**Options**

**Table 17-7** shows the options that you can specify to list and display reports and views.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-enddate yyyy-MM-dd-HH:mm:ss</code></td>
<td>Specifies a upper limit for the date of information to be displayed.</td>
</tr>
<tr>
<td><code>-list</code></td>
<td>Lists the available reports and views.</td>
</tr>
<tr>
<td><code>-report report</code></td>
<td>Specifies a report.</td>
</tr>
<tr>
<td><code>-startdate yyyy-MM-dd-HH:mm:ss</code></td>
<td>Specifies a lower limit for the date of information to be displayed.</td>
</tr>
<tr>
<td><code>-view view</code></td>
<td>Specifies a view.</td>
</tr>
</tbody>
</table>

**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
```

**Generating View Event Log Messages in Syslog Format Using the -I Option**

You can use the `vdmadmin` command with the `-I` option to record View event messages in Syslog format in event log files. Many third-party analytics products require flat-file Syslog data as input for their analytics operations.

**Syntax**

```
vdmadmin -I -eventSyslog -disable
vdmadmin -I -eventSyslog -enable -localOnly
vdmadmin -I -eventSyslog -enable -path path
vdmadmin -I -eventSyslog -enable -path path
   -user DomainName\username -password password
```

**Usage Notes**

You can use the command to generate View event log messages in Syslog format. In a Syslog file, View event log messages are formatted in key-value pairs, which makes the logging data accessible to analytics software.

You can also use the `vdmadmin` command with the `-I` option to list the available reports and views and to display the contents of a specified report. See “Listing and Displaying Reports of View Manager Operation Using the -I Option,” on page 416.

**Options**

You can disable or enable the `eventSyslog` option. You can direct the Syslog output to the local system only or to another location. Direct UDP connection to a Syslog server is supported with View 5.2 or later. See “Configure Event Logging for Syslog Servers” in the *VMware Horizon View Installation* document.

**Table 17-8. Options for Generating View Event Log Messages in Syslog Format**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-disable</td>
<td>Disables Syslog logging.</td>
</tr>
<tr>
<td>-e</td>
<td>—enable</td>
</tr>
<tr>
<td>-eventSyslog</td>
<td>Specifies that View events are generated in Syslog format.</td>
</tr>
<tr>
<td>-localOnly</td>
<td>Stores the Syslog output on the local system only. When you use the -localOnly option, the default destination of the Syslog output is %PROGRAMDATA%\VMware\VDM\events.</td>
</tr>
<tr>
<td>-password password</td>
<td>Specifies the password for the user that authorizes access to the specified destination path for the Syslog output.</td>
</tr>
<tr>
<td>-path</td>
<td>Determines the destination UNC path for the Syslog output.</td>
</tr>
<tr>
<td>-u</td>
<td>-user DomainName\username</td>
</tr>
</tbody>
</table>
Examples

Disable generating View events in Syslog format.
`vdmadmin -I -eventSyslog -disable`

Direct Syslog output of View events to the local system only.
`vdmadmin -I -eventSyslog -enable -localOnly`

Direct Syslog output of View events to a specified path.
`vdmadmin -I -eventSyslog -enable -path path`

Direct Syslog output of View events to a specified path that requires access by an authorized domain user.
`vdmadmin -I -eventSyslog -enable -path \logserver\share\ViewEvents -user mydomain\myuser -password mypassword`

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.

**Note** The `vdmadmin -L` command does not assign ownership to View Composer persistent disks. To assign linked-clone desktops with persistent disks to users, use the Assign User menu option in View Administrator or the View PowerCLI `Update-UserOwnership` cmdlet.

If you do use `vdmadmin -L` to assign a linked-clone desktop with a persistent disk to a user, unexpected results can occur in certain situations. For example, if you detach a persistent disk and use it to recreate a desktop, the recreated desktop is not assigned to the owner of the original desktop.

Options

Table 17-9 shows the options that you can specify to assign a desktop to a user or to remove an assignment.
Table 17-9. Options for Assigning Dedicated Desktops

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td>-m machine</td>
<td>Specifies the name of the virtual machine.</td>
</tr>
<tr>
<td>-r</td>
<td>Removes an assignment to a specified user, or all assignments to a specified machine.</td>
</tr>
<tr>
<td>-u domain\user</td>
<td>Specifies the login name and domain of the user.</td>
</tr>
</tbody>
</table>

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.
  
  The machine state can be one of the following values: UNDEFINED, PRE_PROVISIONED, CLONING, CLONINGERROR, CUSTOMIZING, READY, DELETING, MAINTENANCE, ERROR, LOGOUT.

  The command does not display all dynamic machine states, such as Connected or Disconnected, that are displayed in View Administrator.
- 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).
Options

Table 17-10 shows the options that you can use to specify the machine whose details you want to display.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td>-m machine</td>
<td>Specifies the name of the virtual machine.</td>
</tr>
<tr>
<td>-u domain\user</td>
<td>Specifies the login name and domain of the user.</td>
</tr>
</tbody>
</table>

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

Reclaiming Disk Space on Virtual Machines Using the -M Option

You can use the vdmadmin command with the -M option to mark a linked-clone virtual machine for disk space reclamation. View directs the ESXi host to reclaim disk space on the linked-clone OS disk without waiting for the unused space on the OS disk to reach the minimum threshold that is specified in View Administrator.

Syntax

vdmadmin -M [-b authentication_arguments] -d desktop -m machine -markForSpaceReclamation

Usage Notes

With this option, you can initiate disk space reclamation on a particular virtual machine for demonstration or troubleshooting purposes.

Space reclamation does not take place if you run this command when a blackout period is in effect.

The following prerequisites must be met before you can reclaim disk space by using the vdmadmin command with the -M option:

- Verify that View is using vCenter Server and ESXi version 5.1 or later.
- Verify that VMware Tools that are provided with vSphere version 5.1 or later are installed on the virtual machine.
- Verify that the virtual machine is virtual hardware version 9 or later.
- In View Administrator, verify that the Enable space reclamation option is selected for vCenter Server. See “Allow vSphere to Reclaim Disk Space in Linked-Clone Virtual Machines,” on page 19.
- In View Administrator, verify that the Reclaim VM disk space option was selected for the desktop pool. See “Reclaim Disk Space on Linked-Clone Desktops,” on page 115.
- Verify that the virtual machine is powered on before you initiate the space reclamation operation.
- Verify that a blackout period is not in effect. See “Set Blackout Times for ESXi Operations on View Desktops,” on page 116.
Options

Table 17-11. Options for Reclaiming Disk Space on Virtual Machines

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td>-m machine</td>
<td>Specifies the name of the virtual machine.</td>
</tr>
<tr>
<td>-MarkForSpaceReclamation</td>
<td>Marks the virtual machine for disk space reclamation.</td>
</tr>
</tbody>
</table>

Example

Marks the virtual machine machine3 in the desktop pool pool1 for disk space reclamation.

vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation

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 17-12 shows the options that you can specify to configure domain filters.

Table 17-12. Options for Configuring Domain Filters

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--domain domain</td>
<td>Specifies the domain to be filtered. You must specify domains by their NetBIOS names and not by their DNS names.</td>
</tr>
<tr>
<td>--add</td>
<td>Adds a domain to a list.</td>
</tr>
</tbody>
</table>
Table 17-12. Options for Configuring Domain Filters (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-domains</td>
<td>Specifies a domain filter operation.</td>
</tr>
<tr>
<td>-exclude</td>
<td>Specifies an operation on an exclusion list.</td>
</tr>
<tr>
<td>-include</td>
<td>Specifies an operation on an inclusion list.</td>
</tr>
<tr>
<td>-list</td>
<td>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.</td>
</tr>
<tr>
<td>-list-active</td>
<td>Displays the available domains for the View Connection Server instance on which you run the command.</td>
</tr>
<tr>
<td>-remove</td>
<td>Removes a domain from a list.</td>
</tr>
<tr>
<td>-removeall</td>
<td>Removes all domains from a list.</td>
</tr>
<tr>
<td>-s connsvr</td>
<td>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.</td>
</tr>
<tr>
<td>-search</td>
<td>Specifies an operation on a search exclusion list.</td>
</tr>
</tbody>
</table>

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)**

```
Domain: 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 17-13 shows the types of domain lists that you can specify to configure domain filtering.
Table 17-13. Types of Domain List

<table>
<thead>
<tr>
<th>Domain List Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search exclusion list</td>
<td>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.</td>
</tr>
<tr>
<td>Exclusion list</td>
<td>Specifies the domains that View Manager excludes from the results of a domain search. You cannot exclude the primary domain.</td>
</tr>
<tr>
<td>Inclusion list</td>
<td>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.</td>
</tr>
</tbody>
</table>

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
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.

```bash
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

Display the new domain search configuration.

```bash
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.

```bash
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.

```bash
C:\ vdmadmin -N -domains -list -active
```

Domain Information (CONSVR-2)
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 17-14 shows the options that you can specify to display the desktops and policies of unentitled users.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-ld</td>
<td>Orders output entries by desktop.</td>
</tr>
<tr>
<td>-lu</td>
<td>Orders output entries by user.</td>
</tr>
<tr>
<td>-noxslt</td>
<td>Specifies that the default stylesheet should not be applied to the XML output.</td>
</tr>
<tr>
<td>-xsltpath path</td>
<td>Specifies the path to the stylesheet that is used to transform XML output.</td>
</tr>
</tbody>
</table>

Table 17-15 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>
<thead>
<tr>
<th>Stylesheet File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-checkedout-unentitled.xsl</td>
<td>Transforms reports containing a list of desktops that are checked out by unentitled users.</td>
</tr>
<tr>
<td>unentitled-machines.xsl</td>
<td>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.</td>
</tr>
<tr>
<td>unentitled-policies.xsl</td>
<td>Transforms reports containing a list of desktops with user-level policies that are applied to unentitled users.</td>
</tr>
</tbody>
</table>
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 -xs1tpath "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 -xs1tpath "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 -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 17-16 shows the options that you can specify to configure clients in kiosk mode.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-add</td>
<td>Adds an account for a client in kiosk mode.</td>
</tr>
<tr>
<td>-clientauth</td>
<td>Specifies an operation that configures authentication for a client in kiosk mode.</td>
</tr>
<tr>
<td>-clientid client_id</td>
<td>Specifies the name or the MAC address of the client.</td>
</tr>
<tr>
<td>-description &quot;description_text&quot;</td>
<td>Creates a description of the account for the client device in Active Directory.</td>
</tr>
<tr>
<td>-disable</td>
<td>Disables authentication of clients in kiosk mode on a specified View Connection Server instance.</td>
</tr>
<tr>
<td>-domain domain_name</td>
<td>Specifies the domain for the account for the client device.</td>
</tr>
<tr>
<td>-enable</td>
<td>Enables authentication of clients in kiosk mode on a specified View Connection Server instance.</td>
</tr>
</tbody>
</table>
### Table 17-16. Options for Configuring Clients in Kiosk Mode (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-expirepassword</td>
<td>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.</td>
</tr>
<tr>
<td>-force</td>
<td>Disables the confirmation prompt when removing the account for a client in kiosk mode.</td>
</tr>
<tr>
<td>-genpassword</td>
<td>Generates a password for the client's account. This is the default behavior if you do not specify either -password or -genpassword.</td>
</tr>
<tr>
<td>-getdefaults</td>
<td>Gets the default values that are used for adding client accounts.</td>
</tr>
<tr>
<td>-group group_name</td>
<td>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.</td>
</tr>
<tr>
<td>-list</td>
<td>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.</td>
</tr>
<tr>
<td>-noexpirepassword</td>
<td>Specifies that the password on an account does not expire.</td>
</tr>
<tr>
<td>-nogroup</td>
<td>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.</td>
</tr>
<tr>
<td>-ou DN</td>
<td>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.</td>
</tr>
<tr>
<td>-password 'password'</td>
<td>Specifies an explicit password for the client's account.</td>
</tr>
<tr>
<td>-remove</td>
<td>Removes the account for a client in kiosk mode.</td>
</tr>
<tr>
<td>-removeall</td>
<td>Removes the accounts of all clients in kiosk mode.</td>
</tr>
<tr>
<td>-requirepassword</td>
<td>Specifies that clients in kiosk mode must provide passwords. View Manager will not accept generated passwords for new connections.</td>
</tr>
<tr>
<td>-s connection_server</td>
<td>Specifies the NetBIOS name of the View Connection Server instance on which to enable or disable the authentication of clients in kiosk mode.</td>
</tr>
<tr>
<td>-setdefaults</td>
<td>Sets the default values that are used for adding client accounts.</td>
</tr>
<tr>
<td>-update</td>
<td>Updates an account for a client in kiosk mode.</td>
</tr>
</tbody>
</table>

### 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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```bash
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.

```bash
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

Disable authentication of clients for the View Connection Server instance csvr-1.

```bash
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.

```bash
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.

**NOTE** The `vdmadmin` command with the `-R` option works only on desktops that are earlier than View Agent 5.1. On desktops that run View Agent 5.1 and later versions, this option does not work. To locate the first user of a desktop, use the Events database to determine which users logged into the desktop.

**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 or Security Server Using the -S Option

You can use the `vdmadmin` command with the `-S` option to remove the entry for a View Connection Server instance or security server 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.
You can also use the `vdmadmin` command with the `-S` option to remove a security server from your View environment. You do not have to use this option if you intend to upgrade or reinstall a security server without removing it permanently.

To make the removal permanent, perform these tasks:

1. Uninstall the View Connection Server instance or security server 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 or security server from the configuration.

If you want to reinstall 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 or security server 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

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 17-17 shows the options that you must specify to decrypt a full virtual machine or one of its disks.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d desktop</td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td>-infile path_to_VM_file</td>
<td>Specifies the path to the VMX or VMDK file for the local desktop's virtual machine.</td>
</tr>
<tr>
<td>-u domain\user</td>
<td>Specifies the domain and name of the local desktop's end user.</td>
</tr>
</tbody>
</table>

### Examples

Decrypt a full virtual machine by specifying its VMX file.

```bash
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.

```bash
vdmadmin -V -rescue -d lmdtpool -u MYCORP\jo -infile "J:\Temp\LMDT_Recovery\52e52b7c26a2f683-42b945f934e0fbb2-scsi00-000001.vmdk"
```

### Recovering a Local Desktop by Using the -V Option When the Desktop Was Modified in the Datacenter

When a local mode operation such as a check-out, check-in, or replication is performed, View validates that the View desktop's virtual machine in vCenter Server was not modified since the last synchronization with the local View desktop. If a virtual machine disk in vCenter Server was modified, and the disk is not the same as the local desktop version, you can use the vdmadmin command with the -V option to preserve data on the local desktop and vCenter Server virtual machine and ensure that both versions are synchronized.

#### Syntax

```bash
vdmadmin -V -recoverClientVM -d desktop_pool -m virtual_machine
```

```bash
vdmadmin -V -recoverServerVM -d desktop_pool -m virtual_machine
```

#### Usage Notes

When a View desktop is checked out, a snapshot is taken in vCenter Server 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.

If vSphere allows a virtual machine to be unlocked and the virtual machine is inadvertently powered on, the vCenter Server virtual machine in the datacenter and the local desktop are no longer synchronized. For example, a virtual machine might be unlocked during a vCenter Server upgrade.
When a local mode operation is initiated or resumed, View uses the virtual machine disk’s content ID (CID) to track whether a vCenter Server disk was modified since the last synchronization between a vCenter Server disk and the corresponding local desktop disk. If the vCenter Server virtual machine in the datacenter and the local desktop are not the same, the local mode operation is stopped, and the user sees the following message:

This desktop has been modified at the datacenter. Please contact your system administrator.

You can recover the local desktop virtual machine, vCenter Server virtual machine, or both versions, depending on the local mode operation that was underway.

**Recovering the Local Desktop Version of the Virtual Machine**

If a desktop is fully checked out or a user is checking in or replicating a desktop, and the vCenter Server virtual machine is modified, the user might have valuable data on the local desktop.

You can recover the local desktop version by using the `vdmadmin` command with the `-V -recoverClientVM` option. This option reverts the vCenter Server virtual machine to the snapshot that was taken during the last synchronization. You can then instruct the user to start the check-in operation again.

**Recovering the vCenter Server Version of the Virtual Machine**

If a desktop is fully checked out or a user is checking out a desktop, and the vCenter Server virtual machine in the datacenter was modified, you might have installed applications or performed valuable updates on the vCenter Server virtual machine.

You can recover the vCenter Server version by using the `vdmadmin` command with the `-V -recoverServerVM` option. This option takes a new snapshot of the vCenter Server virtual machine, deletes the old snapshot, and rolls back the virtual machine. During a rollback, the local View desktop is discarded. You can then instruct the user to start the check-out operation again.

**Recovering Both Versions of the Virtual Machine**

In a special situation in which a desktop is fully checked out, and no check-in or replication was underway when the vCenter Server virtual machine was opened, you might want to preserve both the client and vCenter Server virtual machines. Perhaps valid, useful contents were created on both virtual machines. In vCenter Server, you can clone the vCenter Server virtual machine to preserve an identical copy. Next, you can use the `vdmadmin` command with the `-V -recoverClientVM` option to recover the client virtual machine.

**Options**

Table 17-18. Options for Recovering the Client or vCenter Server Versions of a Local Desktop

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-recoverClientVM</code></td>
<td>Recovers a local desktop virtual machine that resides on a client system. The vCenter Server virtual machine is reverted to the snapshot that was taken during the last synchronization.</td>
</tr>
<tr>
<td><code>-recoverServerVM</code></td>
<td>Recovers a vCenter Server virtual machine by taking a new snapshot of the virtual machine. The old snapshot is deleted. The virtual machine is rolled back, which discards the local desktop virtual machine.</td>
</tr>
<tr>
<td><code>-d desktop_pool</code></td>
<td>Specifies the name of the desktop pool.</td>
</tr>
<tr>
<td><code>-m virtual_machine</code></td>
<td>Specifies the name of the local desktop's virtual machine.</td>
</tr>
</tbody>
</table>
Examples

Recover a local desktop virtual machine that resides on a client system.

```
vdmadmin -V -recoverClientVM -d lmdtpool -m machine1
```

Recover a vCenter Server virtual machine and roll back the virtual machine.

```
vdmadmin -V -recoverServerVM -d lmdtpool -m machine2
```

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 17-19 shows the options that you can specify to unlock or lock virtual machines.

**Table 17-19. Options for Unlocking or Locking Virtual Machines**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-d desktop</code></td>
<td>Specifies the desktop pool.</td>
</tr>
<tr>
<td><code>-e</code></td>
<td>Unlocks a virtual machine.</td>
</tr>
<tr>
<td><code>-m machine</code></td>
<td>Specifies the name of the virtual machine.</td>
</tr>
<tr>
<td><code>-p</code></td>
<td>Locks a virtual machine.</td>
</tr>
<tr>
<td><code>-vcdn vCenter_dn</code></td>
<td>Specifies the distinguished name of the vCenter Server.</td>
</tr>
<tr>
<td><code>-vmpath inventory_path</code></td>
<td>Specifies the inventory path of the virtual machine.</td>
</tr>
</tbody>
</table>
Examples

Unlock the virtual machines machine1 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 17-20 shows the options that you can specify to detect and resolve colliding LDAP entries.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-collisions</td>
<td>Specifies an operation for detecting LDAP collisions in a View Connection Server group.</td>
</tr>
<tr>
<td>-resolve</td>
<td>Resolves all detected LDAP collisions.</td>
</tr>
</tbody>
</table>

Examples

Detect LDAP entry collisions in a View Connection Server group.

```
vdmadmin -X -collisions
```

Detect and resolve LDAP entry collisions.

```
vdmadmin -X -collisions -resolve
```
Setting Up Clients in Kiosk Mode

You can set up unattended clients that can obtain access to their desktops from VMware Horizon 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 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 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 440
   
   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 441
   
   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 442
   
   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 443
   
   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 444
   
   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 445
   
   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 446
   
   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]
  ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-expirepassword</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-group group_name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-noexpirepassword</code></td>
<td>Specifies that passwords on client accounts do not expire.</td>
</tr>
</tbody>
</table>
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 Clients 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Enter <code>C:\Program Files\VMware\VMware View\Client\bin\wswc -printEnvironmentInfo</code> 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.</td>
</tr>
<tr>
<td>Linux</td>
<td>Enter <code>vmware-view --printEnvironmentInfo -s connection_server</code> 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.</td>
</tr>
</tbody>
</table>

**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.

```bash
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-clientid</code> <code>client_id</code></td>
<td>Specifies the name or the MAC address of the client.</td>
</tr>
<tr>
<td><code>-description&quot;description_text&quot;</code></td>
<td>Creates a description of the account for the client device in Active Directory.</td>
</tr>
<tr>
<td><code>-domain</code> <code>domain_name</code></td>
<td>Specifies the domain for the client.</td>
</tr>
<tr>
<td><code>-expirepassword</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-genpassword</code></td>
<td>Generates a password for the client's account. This is the default behavior if you do not specify either <code>-password</code> or <code>-genpassword</code>. 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 <code>-password</code> option to specify the password.</td>
</tr>
<tr>
<td><code>-group</code> <code>group_name</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-noexpirepassword</code></td>
<td>Specifies that the password on the client's account does not expire.</td>
</tr>
<tr>
<td><code>-nogroup</code></td>
<td>Specifies that the client's account is not added to the default group.</td>
</tr>
<tr>
<td><code>-ou</code> <code>DN</code></td>
<td>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</td>
</tr>
<tr>
<td><code>-password&quot;password&quot;</code></td>
<td>Specifies an explicit password for the client's account.</td>
</tr>
</tbody>
</table>

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 -genpassword
```

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 -genpassword -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]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-requirepassword</td>
<td>Specifies that you require clients to provide passwords.</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT</strong> 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.</td>
</tr>
<tr>
<td>-s connection_server</td>
<td>Specifies the NetBIOS name of the View Connection Server instance on which to enable authentication of clients.</td>
</tr>
</tbody>
</table>

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. For View Client from View 4.6.x and earlier, 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Enter <code>C:\Program Files\VMware\VMware View\Client\bin\wswc -unattended [-serverURL connection_server] [-userName user_name] [-password password]</code></td>
</tr>
<tr>
<td><code>-password</code></td>
<td>Specifies the password for the client's account. If you defined a password for the account, you must specify this password.</td>
</tr>
<tr>
<td><code>-serverURL</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>-userName</code></td>
<td>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 &quot;custom-&quot;, rather than using its MAC address, you must specify this name.</td>
</tr>
<tr>
<td>Linux</td>
<td>Enter <code>vmware-view --unattended -s connection_server [--once] [-p password]</code></td>
</tr>
<tr>
<td><code>--once</code></td>
<td>Specifies that you do not want View Client to retry connecting in the case of an error occurring. <strong>IMPORTANT</strong> You should usually specify this option, and use the exit code to handle the error. Otherwise, you might find it difficult to kill the <code>vmware-view</code> process remotely.</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>Specifies the password for the client's account. If you defined a password for the account, you must specify this password.</td>
</tr>
<tr>
<td><code>-s</code></td>
<td>Specifies the IP address or FQDN of the View Connection Server instance that View Client will use to connect to its desktop.</td>
</tr>
<tr>
<td><code>-u</code></td>
<td>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 &quot;custom-&quot;, rather than using its MAC address, you must specify this name.</td>
</tr>
</tbody>
</table>

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!"
```
## Index

### Numerics

<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3D renderer</td>
<td>138</td>
</tr>
<tr>
<td>best practices</td>
<td>138</td>
</tr>
<tr>
<td>configuring</td>
<td>136</td>
</tr>
<tr>
<td>options</td>
<td>137</td>
</tr>
</tbody>
</table>

### A

#### Active Directory

- preparing for clients in kiosk mode 440
- preparing for smart card authentication 162
- troubleshooting linked clones failing to join the domain 404
- updating Foreign Security Principals of users 414
- updating general user information 361
- using existing computer accounts for linked clones 117

#### Active sessions

- disconnecting 272
- restarting 272
- sending messages 272
- viewing 272

#### ADM Template file

- adding to a local system 236
- adding to Active Directory 237
- installing 236

#### ADM template files

- PCoIP session bandwidth settings 214
- PCoIP Session Variables 207
- View Agent Configuration 181
- View Client Configuration 187
- View Common Configuration 206
- View components 180
- View Server Configuration 205

#### where to find 181

#### administration

- configuring 39
- delegating 40

#### administrator groups

- creating 42
- managing 39, 42
- removing 43

#### administrator permissions

- adding 43
- deleting 44
- managing 43
- viewing 45

#### administrator privileges

- command line utilities 53
- common tasks 51
- desktop management 51
- general administration 53
- global 49
- internal 51
- object-specific 50
- persistent disk management 52
- pool management 51
- predefined 48
- understanding 39

#### user and administrator management 52

#### administrator roles

- adding custom 39, 47, 48
- managing custom 47
- modifying custom 47
- predefined 39, 48
- removing custom 48
- understanding 39

#### administrator users

- creating 42, 43
- managing 42

#### Administrators (Read only) role 48

#### Administrators role 48

#### Adobe Flash

- improving quality in the desktop 272
- quality modes 271
- reducing bandwidth 271
- setting quality modes 271
- setting throttling modes 271
- Terminal Services sessions 125, 272
- throttling modes 271

#### Agent Registration Administrators role 48

#### alarm settings, performance 206

#### allowCertCRLs property 168

#### Always on policy 140

#### application packages, capturing and storing 286

#### application repositories

- creating a network share 287
- load balancing 286
- problems registering 299
- problems scanning 299
- registering 287
removing 298
scanning 288
ASP.NET IIS registration tool, RSA key container 366
authentication
enabling for clients in kiosk mode 444
dvmadmin command 409
automated desktop pools
adding desktops manually 268
assigning multiple network labels 147
changing the pool size 267
creating 88, 90
customizing desktops in maintenance mode 131
deploying large pools 147
desktop settings 91, 132
desktop-naming example 130
maintenance mode 131
naming desktops manually 126, 128
power policies 143, 144
using a desktop-naming pattern 126
worksheet for creating 88
automatic Windows updates, disabling 76

B
backing up
configuration backup settings 353
scheduling backups 352
View configuration data 351
View Connection Server 26
bandwidth reduction, Adobe Flash 271
base images
determining the size 314
downloading from the Transfer Server repository 313
best practices, View Persona Management 240
blackout times
for disk space reclamation 116, 146
for View Storage Accelerator 116, 146
bridged networking for local desktops 331

C
caching proxy server
provisioning local desktops 332
setting up 335
CBRC
configuring for desktop pools 145
configuring for vCenter Server 20
certificate revocation checking enabling 165
group policy settings 187
troubleshooting for security server 395
certificates
accept the thumbprint 23
ignoring problems 187
updating on View Connection Server 367
certutil command 163
client accounts, adding for kiosk mode 443
client session policies
configuring global 176
configuring pool-level 176
configuring user-level 177
defined 175
general 177
inheritance 175
local 178
client sessions
global settings 26, 28
session timeouts 28
setting timeouts 26
client systems
checking out a desktop after a manual download 339
configuring in kiosk mode 439
configuring registry for HTTP caching 334
displaying information about kiosk mode 428, 445
displaying MAC addresses 442
manually downloading a local desktop 338
passing information to desktops 186
preparing Active Directory for kiosk mode 440
setting defaults for kiosk mode 441
setting permissions on manually copied desktop files 339
setting up in kiosk mode 439
cluster, more than eight hosts 147
command scripts, running on desktops 185
CommandsToRunOnConnect group policy setting 185
composite USB devices 199
compression
data transfers for local desktops 323
impact on data transfers 326
configuration data
exporting with vdmexport 353
importing with vdmimport 354
connection issues
between desktops and View Connection Server 390
between View Client and the PCoIP Secure Gateway 389
between View Client and View Connection Server 388
linked-clone desktops with static IP addresses 391
Connection Server service 360
collection ticket timeout 181
collections, troubleshooting 388
Console Interaction privilege 49
credentials 172
CRL checking
configuring 166
logging in 166
crlLocation property 166, 168
CSV output, vdmadmin command 410
Ctrl+Alt for ungrabbing the mouse pointer 307
custom administrator roles
creating 39
managing 47
modifying 47
removing 48
custom setup options, View Agent 57, 65
customer experience program
collecting data 368
desktop data 375
desktop pool data 372
global data 368
joining or withdrawing 36
security server data 372
Transfer Server data 378
vCenter data 377
View Connection Server data 369
View Transfer Server data 378
customization scripts
increasing QuickPrep timeout limits 84
using QuickPrep for linked-clone desktops 104,
105
customization specifications
creating 86
recomposing linked-clone desktops 106
customizing desktops, maintenance mode 131
deduplication
data transfers for local desktops 323
impact on data transfers 326
defragmentation, disabling on linked clones 75
deliberating administration 40
delta disks, storage overcommit 111
desktop management
deleting desktops 277
displaying desktops for unentitled users 427
displaying the first user of a desktop 432
exporting desktop information to a file 278
monitoring desktop status 274, 358
understanding 272
desktop pool creation
choosing a user assignment type 126
customizing in maintenance mode 131
deploying large pools 147
desktop-naming example 130
on more than 8 hosts 147
provisioning options 125
understanding 87
with Persona Management 239
desktop pool management
deleting desktop pools 269
deleting unmanaged desktops 282
disabling desktop pools 269
disabling provisioning 269
editable desktop pool settings 266
editing desktop pools 265
fixed desktop pool settings 266
understanding 265
desktop pool management
deleting desktop pools 269
deleting unmanaged desktops 282
disabling desktop pools 269
disabling provisioning 269
editable desktop pool settings 266
fixed desktop pool settings 266
understanding 265
desktop pool troubleshooting
cloning failure 393
creation problems 391
customization failure 394
failure due to configuration problems 392
failure due to missing customization specifications 391
failure due to permissions problems 392
failure due to vCenter being overloaded 394
free disk space problems 393
inability to connect to vCenter 393
inability to log in to vCenter 393
resource problems 393
timeout while customizing 394
vCenter status unknown 393
virtual machines stuck in Provisioning state 394
desktop recomposition
correcting an unsuccessful recomposition 257
linked-clone desktops 253, 254, 256
### preparing a parent virtual machine
- Sysprep
- desktop refresh, linked clones
- desktop sessions
  - disconnecting
  - restarting
  - viewing
- desktop settings
  - automated desktop pools
  - linked-clone desktops
  - manual desktop pools
- Terminal Server desktop pools

### desktop sources
- adding to a pool
- preparing for desktop deployment
- removing from a pool
- unregistering
- desktop status
  - locating desktops
  - physical computers
- terminal servers
- virtual machines
- desktop troubleshooting
  - connection issues
  - displaying orphaned desktops
  - displaying problem desktops
- repeated deletions
- using vSphere Web Client
- desktop UI, group policy settings
- attaching detached persistent disks
- deleting
- editing the pool or user
- recreating a desktop
- detecting LDAP entry collisions

### device families

### diagnostic information
- collecting
- collecting for View Composer
- collecting using the support tool
- using support scripts
- Diagnostic Policy Service, disabling
- dial-up network connection, checking out local desktops
- direct connections
  - configuring
  - local desktops
- Direct Interaction privilege
- disjoint namespaces
- disposable file redirection, paging-file size
- disposable-data disks, linked-clone desktops

### Do nothing policy

### domain filters
- configuring
- displaying
- example of excluding domains
- example of including domains

### domains
- enumerating trusted
- filter lists
- drivers, installed on client systems for local desktops

### E
- education resources
- Enable Pool privilege
- enableOCSP property
- enableRevocationChecking property
- encryption, of user credentials
- endpoint resource usage, configuring
- Enterprise NTAuth store, adding root certificates
- Entitle Pool privilege
- entitlements
  - adding to desktop pools
  - removing from desktop pools
  - restricting
  - reviewing
- ESXi hosts, using more than eight in a cluster

### events
- generating output in syslog format
- monitoring
- types and descriptions
- exclusion lists
- external URL, editing

### F
- filter lists, adding and removing domains
- Flexible Authentication
- floating-assignment pools
  - choosing a user assignment type
  - maintenance mode
- folder redirection, group policy settings
- folders
  - adding a desktop pool
  - creating
  - managing
  - organizing desktops and pools
  - removing
  - reviewing desktop pools
  - reviewing desktops
  - root
- Foreign Security Principals, updating
- Framework Component service
- FSPs, updating
Full (Read only) privilege 51

G
GINA
  chaining 3rd-party software dlls 404
  View Agent dll 404
Global Configuration and Policy Administrators
  (Read only) role 48
Global Configuration and Policy Administrators role 48
global policies, configuring 176
global settings
  client sessions 26, 28
  message security mode 30
glossary 9
GPOs
  creating for desktops 223
  creating for View component policies 179
gpvm utility, examining GPU resources 139
graphics, 3D renderer 136
group policies
  ADM template files 181
  applying to GPOs 222
  examples 222
  Terminal Services 221, 222
  View Agent configuration 181
  View Client configuration 187
  View common configuration 206
  View components 180
  View Connection Server 205
group policy settings
  adding to a local system 236
  adding to Active Directory 237
desktop UI settings 248
  folder redirection 246
logging 249
  manage user persona 244
  persona repository location 244
  roaming and synchronization 244
  View Persona Management 243
guest operating systems
  file system optimization 328
  installing 61
  optimizing performance 70, 71
  paging-file size 84
  preparing for desktop deployment 62
GUIDs
  displaying for View Connection Server group 414
  support in View Composer 102

H
health monitors, listing and displaying 415
heartbeat interval, local desktops 336, 337
host caching
  for desktop pools 145
  for vCenter Server 20
HTML access, configuring 32
HTML Access, opening port 33
HTTP, allowing for SSL off-loading 34
HTTP cache
  configuring a proxy server 335
  configuring client systems 334
  configuring View Connection Server 333
  configuring View LDAP 334
  provisioning local desktops 332
I
inclusion lists 423
individual desktops, creating 121
installation
  guest operating system 61
  silent 66
  silent installation options 67
  standalone View Persona Management 235
  View Agent 55, 64, 66
  intermediate certificates
    adding to intermediate certification authorities 164
    See also certificates
  Intermediate Certification Authorities policy 164
  Inventory Administrators (Read only) role 48
  Inventory Administrators role 48
IOPS
  benefits of disabling Windows 7 services 73
  benefits of disabling Windows 8 services 73
IP addresses
  overriding for View Agent 413
  troubleshooting for linked-cloned desktop connections 391
IPSec, security server connections 29

K
keyboard settings, PCoIP session variables 216
keytool utility 159
kiosk mode
  adding client accounts 443
  configuring 439
  connecting to desktops 446
  displaying information about clients 445
  displaying MAC address of client devices 442
  enabling authentication of clients 444
  managing client authentication 428
  preparing Active Directory 440
  setting defaults for clients 441
  setting up 439
  viewing and modifying client accounts 428

VMware, Inc.

VMware, Inc.
setting permissions on manually copied desktop files 339
SSO timeout limits 29
suspending data transfers 311
understanding management tasks 303
local desktop troubleshooting 340
local desktop use
benefits 303
checking out 307
checking out after a manual download 339
deleting local desktops 322
logging in with smart cards 157
rolling back a checked-out desktop 321
local memory usage, overriding 328
local mode, See local desktop
local mode only desktops 306
local mode policies 178
local sessions
privileges for managing 50, 51
rolling back 321, 437
viewing 380
location-based printing
configuring 218
group policy 218–220
registry key 218
TPVMGPOAcmap.dll file 218
locked.properties file
configuring CRL checking 166
configuring OCSP checking 167
configuring smart card authentication 160
configuring smart card certificate revocation 168
off-loading SSL connections 34
locking
remote desktops 437
View Transfer Server instances 437
log files
collecting for View Client 385
configuring in View Agent 411
configuring settings 206
displaying for View Connection Server 164
Log in as current user feature, group policy settings 187
logging, group policy settings 249
logging levels, View Agent 411
loopback processing
benefits 180
enabling 225
LSI20320-R controllers, installing driver 61
MAC addresses, displaying for client systems 442
Mac systems, using with View Administrator 14
maintenance mode
customizing desktops 131
entering 274
exiting 274
starting desktops 131
View Transfer Server 311
Manage Composer Pool Image privilege 50
Manage Global Configuration and Policies (Read only) privilege 51
Manage Global Configuration and Policies privilege 49
Manage Inventory (Read only) privilege 51
Manage Local Sessions privilege 50
Manage Persistent Disks privilege 50
Manage Pool privilege 50
Manage Reboot Operation privilege 50
Manage Remote Sessions privilege 50
Manage Roles and Permissions privilege 49
manage user persona
configuring 238
group policy settings 244
manual desktop pools
configuring a single desktop 121
creating 119, 121
desktop settings 122, 132
worksheet for creating 120
max concurrent power operations, configuration guidelines 22
Message Bus Component service 360
message security mode, global settings 30
messages, sending to desktop users 381
Microsoft Feeds Synchronization
disabling on Windows 7 79
disabling on Windows 8 78
Microsoft Terminal Services, creating desktop pool 123
Microsoft Terminal Services pools
Adobe Flash Throttling 125, 272
creating 124
Microsoft Windows Defender
disabling in Windows 7 78
disabling in Windows 8 78
Microsoft Windows Installer, properties for View Agent 68
migrating
linked-clone desktops 259
user profiles 229
View Composer to another computer 362
View Composer with an existing database 363
View Composer without linked clones 365
mouse grabbed inside desktop window 307
MSI packages
creating 286
invalid 301
multiple NICs, configuring for View Agent 70

N
naming desktop pools
example 130
manually specifying names 126, 128
providing a naming pattern 126
NAT on local desktops 331
NET Framework, migrating RSA key container 366
network connections
manually downloading desktops 337
troubleshooting 388
network share, guidelines for creating 233
NFS datastores, clusters with more than eight hosts 147
NICs 331
NTFS, optimizing data transfers 328

O
OCSP certificate revocation checking
configuring 167
logging in 166
ocspCRLFailover property 168
ocspSendNonce property 168
ocspSigningCert 168
ocspSigningCert property 167
ocspURL property 167, 168
Offline Desktop (Local Mode), See local desktop offline smart card authentication 157
online support 9
orphaned desktops, displaying 383, 427
OS disks
desktop refresh 251, 252
disabling Windows 7 services 73
disabling Windows 8 services 73
growth caused by Windows 7 services 73
growth caused by Windows 8 services 73
linked-clone desktops 119
storage overcommit 110
storage sizing formulas for editing pools 109
OUs
creating for kiosk mode clients 440
creating for View desktops 180, 223
output formats, vdmadmin command 410
overriding IP addresses for View Agent 413

P
package files
copying to a portable device 338
deleting from the Transfer Server repository 316
publishing in the Transfer Server repository 316
packages, displaying and setting the split limit 433
paging-file size, parent virtual machine 84
parent virtual machines
disabling defragmentation on Windows 7 75
disabling defragmentation on Windows 8 75
disabling hibernation 82
disabling Windows 7 services 73
preparing for View Composer 80
passwords 173
PCoIP Secure Gateway, connection problems 389
PCoIP Server, View Agent custom option 57, 65
PCoIP session variables
build-to-lossless feature 217
general session variables 208
group policy settings 207
keyboard settings 216
session bandwidth settings 214
PCoIP Smartcard, View Agent custom option 57, 65
pcoip.adm, ADM template files 181
performance alarms, configuring 206
performance optimization, guest operating system 70, 71
permissions
adding 43
deleting 44
viewing 41
persistent disks
attaching 261
creating 92
deleting detached disks 263
detaching 261
editing the pool or user 262
importing from a vSphere datastore 263
linked-clone desktops 119
Persona Management 242
recreating a desktop 262
storage sizing formulas for editing pools 109
understanding 260
View Composer 260
Persona Management
best practices 240
configuration overview 232
configuring a deployment 232
configuring and managing 227
creating desktop pools 239
enabling 238
migrating user profiles 229
setting the repository location 238
standalone installation 235
standalone laptops 242
standalone systems 228
View Agent installation option 234
View Composer persistent disks 242
Windows roaming profiles 231
with View Manager 227
persona repository location, group policy settings 244
physical computers
adding to a pool 281
desktop status 283
displaying information about 419
installing View Agent 55
managing 281
preparing for desktop delivery 55
removing from a pool 282
pointer grabbed inside desktop window 307
policies
Active Directory 179
automated pools 143
client session 175
client session inheritance 175
configuring for View 175
configuring persona management 227
displaying for unentitled users 427
displaying unentitled 383
general client session 177
global 176
Intermediate Certification Authorities 164
local mode 178
pool-level 176
power 140, 143
    Trusted Root Certification Authorities 163
user-level 177
pool size, changing 267
post-synchronization script, customizing linked-clone desktops 105
Power Off VM policy 140
power operations, setting concurrency limits 22
power policies
    automated desktop pools 143, 144
avoiding conflicts 144
desktops and pools 140
power-off script, customizing linked-clone desktops 105
pre-login messages, displaying to clients 28
predefined administrator roles 39
prefetch and superfetch, disabling 77
printing, location-based 218
privileges, See administrator privileges
problem desktops
displaying 381
troubleshooting with vSphere Web Client 382
viewing 380
professional services 9
proxy caches, setting the split limit for View Transfer Server 433
proxy.pac files, configuring View Client to use 187
Q
QuickPrep
customization errors 400
customization scripts 104, 105
increasing timeout limit for customization scripts 84
troubleshooting customization failure 399
View Composer 103, 104
R
RADIUS authentication
enabling 170
logging in 169
RDP, disabling access to desktops 139
read-only domain controllers, troubleshooting linked clones failing to join the domain 404
rebalancing linked-clone desktops
disk filenames after a rebalance 260
setting minimum ready desktops 117
recomposing desktops
correcting an unsuccessful recomposition 257
local desktops 255
setting minimum ready desktops 117
View Composer 253, 256
recomposing linked-clone desktops,
    Sysprep 106
refresh
    linked-clone desktops 251
setting minimum ready desktops 117
    View Composer 252
Register Agent privilege 49
registry backup (RegIdleBackup), disabling 78
Remote Desktop connections
    disabling RDP 139
    enabling 62
Remote Desktop Users group 62
remote desktops
    compared to local desktops 303
    configuring a secure tunnel connection 324
    creating 309
    locking and unlocking 437
    logging off 307
    setting replication policies 320
USB redirection problems 397
user-initiated rollback setting 178
remote repository, configuring 232
remote sessions
privileges for managing 50, 51
viewing 380
replication
configuring policies 319
deduplication and compression 323
initiating a request 321
reports, displaying 416
resolving LDAP entry collisions 438
restoredata, result codes 356
restoring, View configuration data 351, 354
restricted entitlements
assigning tags to desktop pools 153
configuring 152
examples 150
limitations 152
tag matching 151
understanding 150
result codes, restoredata operation 356
roaming and synchronizing, group policy settings 244
roaming profiles, See persona management
role-based delegated administration
best practices 53
configuring 39
roles, See administrator roles
root certificates
adding to the Enterprise NTAuth store 163
adding to trusted roots 163
exporting 159
importing to a server truststore file 159
obtaining 158
root folder 40
RSA Agent host node secret, resetting 171
RSA key container
migrating to View Composer 366
using NET Framework 366
RSA SecurID authentication
configuring 168
enabling 170
logging in 169
troubleshooting 172
SCOM, setting the name of a View Connection Server group 414
Script Host service 360
search exclusion lists 423
Security Gateway Component service 360
security server
connection problems to the PCoIP Secure Gateway 389
problems with certificate revocation checking 395
removing entry from configuration 432
troubleshooting pairing with View Connection Server 395
Security Server service 360
security servers
enabling smart card authentication 160
opening port for HTML Access 33
restricted entitlements limitations 152
services 360
updating certificates 367
security settings, group policy 187
sending messages to desktop users 381
services
security server hosts 360
stopping and starting 359
understanding 359
View Connection Server hosts 360
View Transfer Server hosts 361
sessions
disconnecting 272
restarting 272
sending messages 272
viewing 272
Setup Capture wizard, ThinApp 286
SIDs, support in View Composer 102
silent installation, View Agent 66
silent installation options 67
single sign-on
enabling for local desktop operations 29
group policy settings 181, 187
single sign-on (SSO) 172
smart card authentication
Active Directory preparation 162
certificate revocation checking 165
configuring 158, 160, 161
enabling single sign-on 187
offline smart card authentication 157
redirecting cards and readers 187
understanding 157
UPNs for smart card users 162
verifying configuration 164
smart card certificates, revoking 165
smart cards
exporting user certificates 159
using to authenticate 157
using with local desktops 157
solid-state disks, storing View Composer replicas 113
sparse disks
configuring for desktop pools 115
configuring for vCenter Server 19
split limit, displaying and setting for View Transfer Server 433
splitting composite USB devices 199
SSL
accept a certificate thumbprint 23
enabling for client connections 26, 29
importing certificates to View servers 33
local desktop operations 323, 324
off-loading to intermediate servers 33
setting external URLs for intermediate servers 34
SSL certificates, See certificates
SSO
enabling for offline desktop operations 29
enabling, disabling, setting timeout limits 28
group policy settings 181, 187
local desktops 29
storage, reclaiming disk space 19, 115
storage overcommit, linked clones 110, 111
Storage vMotion, migrating linked clones 259
support offerings 9
support requests
collecting log files 385
updating 387
support scripts
collecting diagnostic information 386
View Composer 385
support tool, using to collect diagnostic information 386
Suspend VM policy, on disconnect 142
sviconfig utility
restoring the database 355
result codes for restoredata 356
swap files, linked-clone desktops 80, 83
Syslog format, generating log messages 417
Sysprep
linked-clone desktops 103
recomposing linked-clone desktops 106
system health dashboard 380
System Restore, disabling 78
T
technical support resources 9
Terminal Server desktop pools
creating 123
desktop settings 124, 132
terminal servers
desktop status 283
installing View Agent 55
managing 281
preparing for desktop delivery 55
Terminal Services group policies 221, 222
text display issues, View Administrator 14
ThinApp applications
assigning 289–293
checking installation status 295
configuration walkthrough 302
configuring user profiles 241
displaying MSI package information 295
maintaining 296
packaging 286
problems assigning 300
problems installing 300
problems uninstalling 301
removing assignments 296, 297
removing from View Administrator 298
requirements 285
reviewing assignments 294
troubleshooting 299
upgrading 296
ThinApp Setup Capture wizard 286
ThinApp templates
assigning 293
creating 288
removing 298
third-party applications, support in View Composer 102
time synchronization
desktop and client system 187
guest OS and ESX host 62
timeout limit, QuickPrep customization scripts 84
TPVMGPoAcmA.dll file 218
Transfer Server Control Service 361
Transfer Server repository
configuring 314
copying packages to a portable device 338
deleting a package 316
determining the size of a base image 314
downloading system images 313
managing 313
migrating 317
publishing a package 316
recovering corrupted shared folder 318
recreating 318
status values 312
Transfer Server service 361
trusted domains, enumerating 205
Trusted Root Certification Authorities policy 163
trustKeyfile property 160
trustStoreType property 160
tunneled connections, local desktops 324
two-factor authentication 168, 172

U
unassigning users, dedicated-assignment pools 274
unentitled users
displaying 383
displaying desktops 427
Unix systems, using with View Administrator 14
Unknown username or bad password 428, 444
unlocking
remote desktops 437
View Transfer Server instances 437
unmanaged desktop sources
adding to a pool 281
defined 55
installing View Agent 55
preparing for desktop delivery 55
removing from a pool 282
unregistering 283
unregistering desktop sources 283
Update Service, disabling 76
updating linked-clone desktops
correcting an unsuccessful recomposition 257
desktop recomposition 253
UPHClean service, using with Persona Management 235
UPNs, smart card users 162
USB device families 204
USB device filters 201
USB devices, group policy settings 187
USB redirection
configuring in View Agent 57, 65
controlling using policies 198
troubleshooting failure 397
useCertAuth property 160, 164
user accounts, View Composer 15
user authentication, configuring 155
user persona, configuring policies 227
user profile path, configuring 232
user profile repository, guidelines for creating 233
user profiles
ThinApp sandbox folders 241
See also persona management
userPrincipalName attribute 162
users
displaying information about 434
displaying unentitled 383
sending messages 381
updating general user information 361

V
VAAI, creating linked clones 114
vCenter Server
configuring concurrent operations limits 21
configuring host caching 20
configuring sparse disks 19
vCenter Server instances
adding in View Administrator 14, 15
correcting conflicting unique IDs 25
removing in View Administrator 24
vdm_agent.adm 181
vdm_client.adm 181, 187
vdm_common.adm 181, 206
vdm_server.adm 181, 205
vdmadmin command
authentication 409
command options 410
introduction 407
output formats 410
syntax 409
View Administrator
logging in 12
managing a View deployment 11
navigating 13
overview 11
text display issues 14
tips for using 13
using the health dashboard 380
using with Linux, Unix, or Mac 14
View Agent
collecting diagnostic information 386
configuring logging levels 411
configuring multiple NICs 70
creating a Data Collection Tool bundle 384
custom setup options 57, 65
installing on a virtual machine 64
installing on unmanaged desktop sources 55
installing silently 66
overriding IP addresses 413
silent installation properties 68
with View Persona Management 234
View Client
collecting diagnostic information 386
configuring online help URL 187
connection problems to the PCoIP Secure Gateway 389
improving Adobe Flash quality 272
saving log files 385
troubleshooting 379
troubleshooting connection issues 388
troubleshooting USB redirection 397
using with kiosk clients 446
View Client with Local Mode, See local desktop
View components, maintaining 351
View Composer Agent
  View Agent custom option 65
  View Agent custom setup option 65
View Composer Array Integration, enabling for desktop pools 114
View Composer configuration
  concurrent operations limits 21
  configuring settings for vCenter Server 17
  creating a user account 15
  deleting base images 316
  domains 18
  publishing base images 313
  removing the service from vCenter Server 24
  support for unique SIDs 102
  volume activation 82
View Composer maintenance
  backing up configuration data 26, 351
  guidelines for migrating 363
  migrating an RSA key container 366
  migrating View Composer to another computer 362
  migrating with the existing database 363
  restoring configuration data 354
  restoring the database 355
  scheduling backups 352
View Composer persistent disks
  attaching 261
  deleting detached 263
  detaching 261
  editing the pool or user 262
  importing from vSphere 263
  management overview 260
  storage sizing formulas 109
  storage sizing formulas for editing pools 109
  understanding 260
View Composer troubleshooting
  collecting diagnostic information 385
  correcting an unsuccessful recomposition 257
  finding unused replicas 402
  overview 379
  provisioning error codes 400
  QuickPrep script failure 399
View Composer use
  choosing QuickPrep or Sysprep 103
  considerations for storing replicas on separate datastores 113
  creating data disks 119
  creating linked-clone pools 92, 100
  local datastores 112
  managing linked-clone desktops 251
  migrating linked-clone desktops 259
  preparing a parent virtual machine 79, 80
  preparing a parent virtual machine for recomposition 253
  publishing base images 316
  QuickPrep 104
  rebalancing linked-clone desktops 257, 258
  recomposing linked-clone desktops 254
  recreating a desktop with a detached persistent disk 262
  refreshing desktops 251
  storing replicas and linked clones on separate datastores 113
  understanding desktop recomposition 253, 256
  understanding desktop refresh operations 252
  worksheet for creating linked-clone pools 92
View Connection Server
  assigning tags for restricted entitlement 152
  backing up configuration data 26, 351
  changing the heartbeat interval 336
  collecting diagnostic information 386
  configuring 11
  configuring direct connections 31
  configuring for HTTP caching 333
  disabling 35
  editing the external URL 35
  exporting configuration data 353
  removing entry from configuration 432
  restoring configuration data 354
  scheduling backups 352
  services 359, 360
  setting names of groups 414
  troubleshooting connection issues 388, 390
View LDAP configuration data 36
View Connection Server configuration, server certificate 367
View LDAP
  configuration data 36
  limiting size of base image package files 334
  pae-mVDIOfflineUpdateFrequency attribute 336
View services, stopping and starting 359
View Storage Accelerator
  configuring for desktop pools 145
  configuring for vCenter Server 20
View Transfer Server configuration
  adding an instance 310
  configuring the repository 314
  configuring transfer policies 319
  determining the size of a base image 314
  locking and unlocking instances 437
  optimizing data transfers 323
  removing an instance 311
  setting replication policies 320
 VMware, Inc.
setting the split limit for publishing packages 433
synchronizing local desktops 309
understanding the Transfer Server repository 313
View Transfer Server management
managing the repository 313
migrating the repository 317
placing in maintenance mode 311
services on a View Transfer Server host 361
status values 312
View Transfer Server troubleshooting
bad health check 345
bad Transfer Server repository 344
checking out desktops 341
maintenance mode pending 343
missing Transfer Server repository 345
no Transfer Server repository configured 345
pending state 343
repository connection error 344
Transfer Server repository conflict 346
VM was modified 346
Web server down 346
ViewPM.adm, ADM template files 181
ViewPM.adm file
adding to a local system 236
adding to Active Directory 237
virtual machines
creating templates 85
custom configuration parameters 60
customization failures 394
desktop status 275
disabling Windows 7 services 73
disabling Windows 8 services 73
displaying information about 419
installing guest operating system 61
managing 265, 272
preparing for desktop deployment 59
reclaiming disk space 420
stuck in Provisioning state 394
Virtual Printing, View Agent custom option 65
virtual profiles, See persona management
VMFS datastores, clusters with more than eight hosts 147
VMware Server virtual machines, preparing for desktop delivery 55
VMware ThinApp
integrating with View Manager 285
using the Setup Capture wizard 286
VMware Tools, installing 62
VMware View with Local Mode, See local desktop
VMwareVDMDS service 360
volume activation, linked-clone desktops 82

W
Web Component service 360
Windows 7
3D rendering 136
benefits of disabling services 73
customization specifications 86
disabling customer experience improvement program 72
disabling defragmentation for linked clones 75
disabling hibernation 82
disabling Microsoft Feeds Synchronization 79
disabling prefetch and superfetch 77
disabling registry backup 78
disabling System Restore 78
disabling Windows Defender 78
disabling Windows Diagnostic Policy Service 77
disabling Windows Update Service 76
services that cause OS disk growth 73
volume activation with linked clones 82
Windows 8
benefits of disabling services 73
customization specifications 86
disabling customer experience improvement program 72
disabling defragmentation for linked clones 75
disabling hibernation 82
disabling Microsoft Feeds Synchronization 79
disabling prefetch and superfetch 77
disabling registry backup 78
disabling services 73
disabling System Restore 78
disabling Windows Defender 78
disabling Windows Diagnostic Policy Service 77
disabling Windows Update Service 76
services that cause OS disk growth 73
volume activation with linked clones 82
Windows roaming profiles, Persona Management 231
Windows Vista
disabling hibernation 82
volume activation with linked clones 82
Windows XP
disabling hibernation 82
troubleshooting GINA chaining 404
troubleshooting linked clones failing to join the domain 404

X
XML output, vdmadmin command 410