VMware Horizon Mirage
Administrator's Guide
Horizon Mirage 4.3

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

EN-001276-02
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 Mirage Administration 7

1 About the Horizon Mirage System Components 9

2 Activating Endpoints 13
   Installing the Horizon Mirage Client 13
   Centralizing Endpoints 15
   Working with Upload Policies 18
   Working with CVD Collections 21
   Working with Archived CVDs 22

3 End User Operations 27
   Client Status Information 27
   File-Level Restoration 28
   Directory-Level Restore 29
   Sync Now and Snooze 29

4 Configuring the File Portal 31
   Allow Access to CVD Files 31
   Configure User CVD Mapping 32
   Browse and View Files with the File Portal 32

5 Configuring the Horizon Mirage System 35
   Configure the System Settings 35
   CVD Snapshot Generation and Retention 38
   Configuring Secure Socket Layer Communication 39

6 Managing the Driver Library 41
   Driver Library Architecture 41
   Managing Driver Folders 42
   Managing Driver Profiles 44

7 Deploying Multiple Storage Volumes 47
   View Storage Volume Information 47
   Add Storage Volumes 48
   Edit Storage Volume Information 49
   Remove or Unmount Storage Volumes 49
   Mount Storage Volumes 50
   Block Storage Volumes 50
   Unblock Storage Volumes 50
   Maintain Storage Volumes 51
8 Using Branch Reflectors  53
   Branch Reflector Matching Process  53
   Select Clients To Be Branch Reflectors  54
   Enable Branch Reflectors  54
   Configure Defaults for Branch Reflectors  55
   Configure Specific Branch Reflector Values  55
   Disable Branch Reflectors  56
   Reject or Accept Peer Clients  56
   Suspend or Resume Server Network Operations  57
   Monitoring Branch Reflector Activity  57

9 Deploying Additional Horizon Mirage Servers  61
   Using Multiple Servers  61
   View Server Information  62
   Add New Servers  63
   Stop or Start the Server Service  63
   Remove Servers  64
   Integrating a Load Balancing Framework  64

10 Image Management Overview  67
   Base Layers and App Layers  67
   Layer Management Life Cycle  67
   Hardware Considerations with Base Layers  69
   Image Management Planning  69

11 Preparing a Reference Machine for Base Layer Capture  73
   Set Up the Reference Machine  73
   Reference Machine Data Considerations  74
   Reference Machine Software and Settings  74
   Recreate a Reference Machine from a Base Layer  75

12 Capturing Base Layers  77
   Working with Base Layer Rules  77
   Applying a Base Layer Override Policy  79
   Capture Base Layers  81
   Post-Base Layer Assignment or Provisioning Script  82

13 Capturing App Layers  85
   App Layer Capture Steps Overview  85
   Prepare a Reference Machine for App Layer Capture  86
   Performing the App Layer Capture  87
   What You Can Capture in an App Layer  90
   Capturing OEM App Layers  91
   Capture Multiple Layers on a Virtual Machine  91
   Create a Post-App Layer Deployment Script  92
22 Troubleshooting 141
   CVD Events History Timeline 141
   Using Event and Other System Logs 141
   Customize the Minimal Restore set 142
   Generate System Reports 143
   Generate System Reports Remotely 144

23 Advanced Administration Topics 145
   Horizon Mirage and SCCM 145
   Setting Up the SSL Certificate in Windows Server 146
   Using Microsoft Office 2010 in a Layer 148
   Managing Role-Based Access Control and Active Directory Groups 148
   Macros in Upload Policy Rules 150

24 Managing Horizon View Desktops with Horizon Mirage 153

Index 155
VMware Horizon Mirage Administration

The *Horizon Mirage Administrator’s Guide* provides information about how to deploy Horizon Mirage to your endpoints and configure the Horizon Mirage system. With Horizon Mirage, you can manage base layer and app layer images, desktop operations such as disaster recovery and hardware and operating system migrations, and monitoring, reporting, and troubleshooting.

**Intended Audience**

This information is intended for the Horizon Mirage administrator. The information is written for experienced Windows system administrators who are familiar with typical Windows Data Center environments such as Active Directory, SQL, and MMC.
VMware® Horizon Mirage™ software centralizes the entire desktop contents in the data center for management and protection purposes, distributes the running of desktop workloads to the endpoints, and optimizes the transfer of data between them.

The Horizon Mirage components integrate into a typical distributed infrastructure, with the following relationships between the system components:

- Horizon Mirage clients connect to a Horizon Mirage server, either directly or through a load balancer.
- The administrator connects to the system through the Horizon Mirage Management server.
- Horizon Mirage servers and the Management server share access to the back-end Horizon Mirage database and storage volumes. Any server can access any volume.

Figure 1-1. System Components
Horizon Mirage clients

Endpoint devices installed with the Horizon Mirage client can run a centralized virtual desktop (CVD) or convert an existing desktop to a CVD. See “Centralized Virtual Desktop (CVD),” on page 10.

The Horizon Mirage client software runs in the base operating system and makes sure the images at the endpoint and the CVD are synchronized. The client does not create or emulate a virtual machine. No virtual machines or hypervisors are required. The Horizon Mirage client software can run on any Type 1 or Type 2 hypervisor.

Horizon Mirage Management server

The Horizon Mirage Management server, located in the data center, is the main component that controls and manages the Horizon Mirage server cluster.

Horizon Mirage Management console

The Horizon Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints.

Through the Management console, the administrator configures and manages clients, base and app layers, and reference machines. The administrator uses the Management console to perform operations such as update and restore, and monitors the system operation through the dashboard and event logs.

Horizon Mirage Web Manager

The Horizon Mirage Web Manager enables help-desk personnel to respond to service queries, and the Dashboard feature assists the Protection manager role to ensure that user devices are protected. The Web Manager mirrors Horizon Mirage Management console functionality. For more information, see the Horizon Mirage Web Manager Guide.

Horizon Mirage Server

The Horizon Mirage servers, located in the data center, manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate monitoring and management communications. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations. It is good practice to keep the server on a dedicated machine or a virtual machine. However, a server can be co-hosted with the Management server.

The server machine must be dedicated for the Horizon Mirage server software to use. It must not be used for any other purposes. For hardware requirements and supported platforms, see the Horizon Mirage Installation Guide.

Centralized Virtual Desktop (CVD)

CVDs represent the complete contents of each PC. This data is migrated to the Horizon Mirage server and becomes the authoritative copy of the contents of each PC. You use the CVD to centrally manage, update, patch, back up, troubleshoot, restore, and audit the desktop in the data center, regardless of whether the endpoint is connected to the network. A CVD comprises the following components:

- Base layer defined by the administrator, which includes the operating system (OS) image plus core applications such as antivirus, firewall, and Microsoft Office. A base layer is used as a template for desktop content, cleared of specific identity information and made suitable for central deployment to a large group of endpoints.
- App layers defined by the administrator, which include sets of one or more departmental or line-of-business applications, and any updates or patches for already installed applications, suitable for deployment to large numbers of endpoints.

- Driver profile defined by the administrator, which specifies a group of drivers for use with specific hardware platforms. These drivers are applied to devices when the hardware platforms match the criteria that the administrator defines in the driver profile.

- User-installed applications and machine state, including unique identifier, hostname, any configuration changes to the machine registry, DLLs, and configuration files.

- Changes to data, applications, or the machine state made by end-user are propagated to the data center. Conversely, all changes that the administrator makes to the base layer or app layers in the data center are propagated to the endpoints. Administrators can identify data that does not need to be protected, such as MP3s, or other files that are considered local only to the endpoint.

**Horizon Mirage Reference Machine**

A Horizon Mirage reference machine is used to create a standard desktop base layer for a set of CVDs. This layer usually includes OS updates, service packs and patches, corporate applications for all target end-users to use, and corporate configurations and policies. A reference machine is also employed to capture app layers, which contain departmental or line-of-business applications and any updates or patches for already installed applications.

You can maintain and update reference machines over time over the LAN or WAN, using a Horizon Mirage reference CVD in the data center. You can use the reference CVD at any time as a source for base and app layer capture.

**Horizon Mirage Branch Reflector**

A Horizon Mirage branch reflector is a peering service role that you can enable on any endpoint device. A branch reflector can then serve adjacent clients in the process of downloading and updating base or app layers on the site, instead of the clients downloading directly from the Horizon Mirage server cluster. Using a branch reflector can significantly reduce bandwidth use during mass base or app layer updates or other base or app layer download scenarios. The branch reflector also assists downloading hardware drivers.

**Horizon Mirage File Portal**

End users can use appropriate login credentials and the Horizon Mirage file portal to access their data from any Web browser. The file portal front-end component runs on any server machines that have IIS 7.0 or later installed, and the back-end component runs on the Management server.

**Distributed Desktop Optimization**

The Distributed Desktop Optimization™ mechanism optimizes transport of data between the Horizon Mirage server and clients, making it feasible to support remote endpoints regardless of network speed or bandwidth. Distributed Desktop Optimization incorporates technologies that include read-write caching, file and block-level deduplication, network optimization, and desktop streaming over the WAN.
Activating Endpoints

The Horizon Mirage client software runs in the base operating system and verifies that the images at the endpoint and the CVD are synchronized. To prepare an endpoint for centralized management of the device data, you install the Horizon Mirage client on the device and activate the device by synchronizing it to a CVD on the Horizon Mirage server.

You must define Upload policies, which determine which files to synchronize, before endpoints are activated. The activation process selects an existing upload policy for the endpoint.

The client does not create or emulate a virtual machine. No virtual machines or hyper visors are required. The client can run on Type 1 or Type 2 hypervisors.

This chapter includes the following topics:
- “Installing the Horizon Mirage Client,” on page 13
- “Centralizing Endpoints,” on page 15
- “Working with Upload Policies,” on page 18
- “Working with CVD Collections,” on page 21
- “Working with Archived CVDs,” on page 22

Installing the Horizon Mirage Client

You can install the Horizon Mirage client installer using the Management console. Administrators can also push out the client installer silently, without disturbing user operations, by using command-line arguments.

The installation procedures apply to first-time installation of the client and to upgrading to a new version of the client.

When the installation is finished:
- the Horizon Mirage icon appears in the notification area, indicating that the client is pending assignment. Right-click actions are available from this icon.
- the Horizon Mirage client appears in Management console in the pending devices list.

Install the Horizon Mirage Client Using the Management Console

You can install the client using the Horizon Mirage Management console.

The client MSI Installer file is located in the Horizon Mirage installation package.

Prerequisites

1 Verify that you have administrative permissions.
2 Verify that your platform meets the software and hardware requirements.

3 Because you cannot place Horizon Mirage servers in the customer's DMZ premises, use a VPN to connect clients that will be used outside the network.

4 If the client will use SSL to connect to the server SSL must already be configured on the server.

**Procedure**

1 Double-click the client MSI Installer file, accept the terms and conditions of use, and click Next.

2 Select the server settings and click Next.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP or FQDN of server</td>
<td>Type the IP address or FQDN of the server you want this client to communicate with. You can also append a port to the server location if you do not want to use the default (port 8000).</td>
</tr>
<tr>
<td>Use SSL to connect to the server option</td>
<td>Select this option to enable SSL if your server is configured for SSL use, and type the required SSL port.</td>
</tr>
</tbody>
</table>

3 Click Install, and when the installation is finished, click Finish.

4 (Optional) Restart your computer.

For first-time installation, restarting assures better backup protection and enables streaming which promotes faster restore. For an upgrade, restarting promotes better performance.

After the Horizon Mirage client is installed, the endpoint appears in the Management console as Pending Assignment.

**What to do next**

Activate the device in the Management console and use a CVD on the server to assign it. This process synchronizes the device and centralizes management of the device data.

**Install the Horizon Mirage Client Silently**

The administrator can deploy the Horizon Mirage client installer silently, without disturbing user operations, by using command-line arguments.

**Prerequisites**

1 Verify that you have administrative permissions.

2 Verify that your platform meets the software and hardware requirements.

3 Because you cannot place Horizon Mirage servers in the customer's DMZ premises, use a VPN to connect clients that will be used outside the network.

4 If the client will use SSL to connect to the server SSL must already be configured on the server.

**Procedure**

1 Select Start > Run, type cmd, and click OK.
2 Type the required expression for your environment and press Enter.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 32-bit clients  | `<Mirage MSI path>\MirageClient.x86.buildnumber.msi SERVERIP=MirageServer /quiet`  
For the SERVERIP parameter, you can use a DNS FQDN or hostname instead of the server IP address. |
| 64-bit clients  | `<Mirage MSI path>\MirageClient.x64.buildnumber.msi SERVERIP=MirageServer /quiet` |

3 (Optional) If SSL needs to be enabled, type the following expression and press Enter:

```
<Mirage MSI path>\MirageClient.x86.buildnumber.msi SERVERIP=MirageServer:port USESSLTRANSPORT=true /quiet
```

4 (Optional) Restart your computer.

   For first-time installation, restarting the computer assures better backup protection and enables streaming which promotes faster restoration.

   For an upgrade, restarting promotes better performance.

When the installation is finished, the Horizon Mirage client appears in the Management console in the Pending Devices list.

**What to do next**

Verify that SSL is enabled on the Horizon Mirage server.

Activate the device in the Management console to assign the device to a CVD on the server. This process synchronizes the device and centralizes management of the device data. See “Centralizing Endpoints,” on page 15.

### Centralizing Endpoints

After you install the Horizon Mirage client, you centralize the device. Centralization activates it in the Management console and synchronizes it with, or assigns it to, a CVD on the Horizon Mirage server so that you can centrally manage the device data.

When Horizon Mirage is first introduced to an organization, each device must be backed up, creating a copy of it on the server, in the form of a Centralized Virtual Desktop or CVD. You can then centrally manage the device.

The endpoint with the client installed appears in the Management console as Pending Assignment, and is pending activation in the system.

You activate a pending device by using a centralization procedure, which either the end user can perform with the automatic procedure, or the administrator can perform with a manual procedure. The administrator option provides more control over the process, for example, allows a choice of upload policy, placement of CVDs on different volumes, and whether to assign a base layer.

You can also reject a device that you do not want to manage in the system. See “Reject Pending Devices,” on page 17.

- The user can use the desktop as usual while the centralization process runs in the background. This ability includes offline work. The client monitors user activities and network characteristics encountered by the desktop, such as speed, and adjusts its operation to optimize the user experience and performance.
After the server synchronization is completed, the Transaction log includes a successful endpoint centralization or provisioning entry. The desktop is protected and can be managed centrally at the data center.

End User Centralization Procedure

After you install the Horizon Mirage client, users can start the centralization of their own endpoint by logging in.

When a user logs in for the first time, Horizon Mirage centralizes the user’s endpoint.

Prerequisites

Verify that the administrator enabled CVD autocreation. CVD autocreation is disabled by default. See “Enable CVD Auto Creation,” on page 36.

Procedure

1. The user logs in using DOMAIN\user or user@DOMAIN.
2. The user provides user credentials.
3. If the prompt is closed or cancelled, the users can restart this process by right-clicking the Horizon Mirage icon in the notification area and selecting Create New CVD.

CVD autocreation starts.

Administrator Centralization Procedure

After the Horizon Mirage client is installed, the administrator can centralize the endpoint. Centralization performed by the administrator provides more control over the process, for example, allows a choice of upload policy, placement of CVDs on different volumes, and whether to assign a base layer.

You might want to add devices to a collection. A collection is a folder that aggregates CVDs that share a logical grouping, for example, Marketing CVDs. You can then implement relevant base layer changes with a single action on all CVDs in the collection. See “Working with CVD Collections,” on page 21.

Prerequisites

The devices to centralize must be in the Pending Devices queue.

Procedure

1. In the Horizon Mirage Management console, select Common Wizards > Centralize Endpoint.
   a. Use Search or filter to find the device or devices you want to assign and click Next. All devices in the filtered list will be centralized.
   b. Select the upload policy to use and click Next. If you do not make a selection, a default policy applies, as specified in the general system settings.
   c. Select a base layer to add to the endpoint and click Next. If you do not want to use a base layer for this endpoint, select Don’t use a base layer and click Next.
   d. Select one or more application layers to which you want to add to the device and click Next.

   Note: This step only appears when you have selected a base layer from the previous step.
e. Select a target storage volume to where you want to store the endpoint base layer and app layers and click Next. Alternatively, you can have Horizon Mirage choose the volume according to the sizes of the base layer and app layers by selecting Automatically choose a volume.

f. The Compatibility Check window displays whether or not the assigned CVDs connected to the endpoint passed the compatibility validation check. When the endpoint passes the validation, you can click Next to proceed.

- When there are potential problems the the CVDs, a warning window appears. You can select each item in the Mismatch List and the validation details and resolution are displayed on the bottom of the window. You can either fix the problem, or click Ignore to bypass the problem. Alternatively, you can click Ignore All to bypass all warning messages.

- When there are fatal errors that must be resolved to centralize the endpoint, a blocking window appears. You can select an error from the Mismatch List to view the Validation Details on the bottom of the window. You must resolve these issues before continuing. The Ignore and Ignore All buttons are unavailable.

2. Click Finish.

   The client starts the scanning phase according to the policy defined during the installation.

   After the scanning finishes, the device appears in the All CVDs panel.

3. (Optional) You can monitor the centralization progress.

   The notification area icon changes to show that the initialization process has started, and the console shows that the client has started an upload. When the initialization process finishes and server synchronization starts, the notification area icon shows the progress of the upload. The console also shows the upload progress in the Progress column of the CVD inventory list. The user can also view the detailed status of the upload operation by clicking the Horizon Mirage icon in the notification area.

Reject Pending Devices

You can reject a client device that is pending assignment that you do not want Horizon Mirage to manage.

If a device is rejected, the server does not honor its communication requests. The rejected device moves from the Pending Devices list to the Rejected list.

Procedure

1. In the Horizon Mirage Management console, expand the Inventory node and click Pending Devices.

2. Right-click the pending device to remove and select Reject.

3. Click Yes to confirm.

Reinstate Rejected Devices

You can remove a device from the Rejected list at any time to reinstate it.

If you remove a device from the Rejected list to reinstate it, its configuration remains valid. It will connect to the server and reappear in the Pending list the next time the client connects.

Procedure

- Right-click the device and select Remove.
Working with Upload Policies

An upload policy determines which files and directories to upload from the user endpoint to the CVD in the data center. You must define upload policies before you activate endpoints because the activation process selects an existing upload policy for the endpoint.

A CVD is assigned only one upload policy at a time.

The administrator creates upload policies by defining whether files are unprotected or local to the endpoint, or protected. Protected policies are uploaded to the Horizon Mirage server in the data center.

To simplify the task, you identify only files and directory names or patterns that are not uploaded to the CVD. The remaining files are considered part of the CVD and are protected.

The list of files that are not protected is defined by a set of rules and exceptions.

You define two upload policy areas, which the system uses according to the relevant system flow.

<table>
<thead>
<tr>
<th>Table 2-1. Upload Policy Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload Policy Area</strong></td>
</tr>
<tr>
<td>Unprotected area</td>
</tr>
<tr>
<td>User area</td>
</tr>
</tbody>
</table>

The upload policy that is applied to the CVD is a combination of the following items:

- A selected built-in factory policy that VMware provides to assist the administrator with first time deployment
- Administrator modifications to that policy to address specific backup and data protection needs

The built-in factory policy is a reference for further customization and includes all the mandatory rules that the system needs to function. The administrator cannot modify the mandatory rules.

Before you use a built-in policy, evaluate it to be sure it meets backup policy and data protection needs. The built-in policies, for example, do not upload .MP3 and .AVI files to the CVD.

You can use one of the following customizable built-in upload policies, to help manage mixed Horizon Mirage and Horizon View systems:

- **Horizon Mirage default upload policy** Use on Horizon Mirage servers that manage CVDs on distributed physical devices.
- **Horizon View optimized upload policy** Use on Horizon Mirage servers that manage CVDs on virtual machines. This upload policy is provided for convenience. It is identical to the Horizon Mirage default upload policy, except that the **Optimize for Horizon View** check box is selected.
View Upload Policies

You can view an upload policy to review its content and parameters.

**Table 2-2. Upload Policy Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Description</td>
<td>Name and description of the policy.</td>
</tr>
<tr>
<td>Upload change interval</td>
<td>Denotes how frequently the client attempts to synchronize with the server. The default is every 60 minutes. End users can override the policy in effect at an endpoint. See “Sync Now and Snooze,” on page 29. The Upload change interval affects the frequency of automatic CVD snapshot creation. See “CVD Snapshot Generation and Retention,” on page 38.</td>
</tr>
<tr>
<td>Protected volumes</td>
<td>Denotes which volumes to centralize from the endpoint to the CVD in the server. The system volume is included by default. You can add more volumes by using the assigned drive letters.</td>
</tr>
<tr>
<td>Protect EFS Files check box, selected by default</td>
<td>Includes all Encrypted File System (EFS) files in the protected upload set. The user encrypts files using the Windows Encrypted File System feature. When the files are download in a CVD restore or file level restore, the files are restored in their original encrypted state.</td>
</tr>
<tr>
<td>Optimize for Horizon View check box</td>
<td>Optimizes performance on servers that use Horizon View to manage virtual machines.</td>
</tr>
<tr>
<td>Unprotected Area tab</td>
<td>Defines the rules to unprotect files and directories.</td>
</tr>
<tr>
<td>Rules list</td>
<td>Paths that are explicitly unprotected by Horizon Mirage.</td>
</tr>
<tr>
<td>Rule Exceptions list</td>
<td>Paths that are exceptions to unprotect rules in the Rules list. Horizon Mirage protects exceptions to unprotect rules.</td>
</tr>
<tr>
<td>User Area tab</td>
<td>Defines the rules to unprotect files and directories defined as user files. These rules are used instead of Unprotected Area rules when certain system flows specifically refer to user files. The tab contains Rules and Rule Exception areas, used in the same way as in the Unprotected Area tab.</td>
</tr>
<tr>
<td>Show Factory Rules check box</td>
<td>Shows the Factory upload policy settings in the rules list, the Horizon Mirage mandatory settings that the administrator cannot change. The factory rules are dimmed in the rules list.</td>
</tr>
<tr>
<td>Export button</td>
<td>Exports policy rules to an XML file for editing and backup. Horizon Mirage factory rules are not exported, even if they appear in the policy window.</td>
</tr>
<tr>
<td>Import button</td>
<td>Imports policy rules from an XML file.</td>
</tr>
</tbody>
</table>

**Procedure**

1. In the Horizon Mirage Management console, expand the System Configuration node and click **Upload Policies**.
2. Double-click the policy to view.

**Add New Upload Policies**

When you add a new upload policy, the new policy is added to the respective node.

**Procedure**

1. In the Horizon Mirage Management console, expand the System Configuration node, right-click **Upload Policies**, and click **Add an Upload Policy**.
2 Type the policy name, description, and policy data.
3 Click OK to save the policy.

Edit Upload Policies

You can edit an upload policy in the Management console and distribute the revised policy.

You can also use an external editor to edit the policy. You export the policy file, edit it, and import it back to the Management console.

The new policy takes effect at the next update interval in which the client queries the server. The default is one hour and requires a full disk scan.

Before you distribute the revised policy to a group of CVDs, it is good practice to test it on a sample desktop.

Procedure
1 In the Horizon Mirage Management console, expand the System Configuration node, and Upload Policies, and double-click an upload policy.
2 Edit the policy data and click OK.
3 Indicate the scope of the update.
   Select a minor version, for example, 1.1, or a major version, for example, 2.0, and click OK.
   The new policy is added to the Management console with the new version number.
4 (Optional) To distribute the changed policy, right-click the policy with this policy version and select Update CVDs.

Add or Edit Upload Policy Rules

You can add or edit a policy rule or a rule exception in a policy. A rule defines directories or files that are not protected, and a rule exception defines entities within the scope of the rule that are protected.

When you formulate policy rules, you can use macros to assist specification of various Horizon Mirage directory paths addressed by the rules. For example, macros allow Horizon Mirage and the administrator to handle cases when some endpoints have Windows in c:\windows and some in d:\windows. Using macros and environment variables makes sure Horizon Mirage backups important files regardless of their specific location. For information about the macro specifications, see “Macros in Upload Policy Rules,” on page 150.

Procedure
1 In the Horizon Mirage Management console, expand the System Configuration node, select Upload Policies, and double-click the required upload policy.
2 Click Add or Edit next to the required Rule or Rule Exception area.
3 Type the directory path or select it from the drop-down menu.
   IMPORTANT Do not type a backslash (\) at the end of the path.
4 Specify a filter for this directory or a pattern for matching files under this directory.
   For example, to add a rule not to protect Windows search index files for all the users on the desktop, add the following rule:

   %anyuserprofile%\Application Data\Microsoft\Search\*

5 Click OK.
Working with CVD Collections

You can group in a collection folder CVDs that share a logical relation to other CVDs. Additionally, you can change an upload policy to a CVD collection with a single action.

For example, you can aggregate all CVDs of users in the marketing department to a folder under a collection called Marketing. Then you can change the upload policy that all the Marketing CVDs share all at once.

Horizon Mirage supports static and dynamic collections. You manually assign CVDs to a static collection, while CVD assignments to dynamic collections are calculated based on predefined filters every time an operation is applied to a collection.

A CVD can be a member of multiple collections. If different base layers or policies are applied to different collections and a CVD belongs to more than one, the last change applied takes effect.

Add Static Collections

You can add a static collection folder to the Collections node, to which you can add CVDs manually.

Procedure

1. In the Horizon Mirage Management console, expand the Inventory node, right-click Collections, and select Add a Collection.
2. Type a name and description for the collection.
4. Click OK.

Add CVDs to Static Collections

You can move CVDs to existing collection folders to organize them in logical groupings.

Procedure

1. In the Horizon Mirage Management console, expand the Inventory node and select All CVDs.
2. Select the Horizon Mirage clients to move to the collection, right-click, and select Manage CVD > Manage Collections.
3. Select the collection to which to move the CVDs.
4. Click OK.

Add Dynamic Collections

You can add a dynamic collection. CVD assignments to the dynamic collection are calculated based on predefined filters every time an operation is applied to the collection. You can define an unlimited number of rules for a dynamic collection.

Procedure

1. In the Horizon Mirage Management console, expand the Inventory node, right-click Collections, and select Add a Collection.
   a. Type the name and description for this dynamic collection.
   b. Select the Dynamic collection option.
c Select the filter to define the dynamic collection from the Column drop-down list.

d Click Apply to view the CVDs filtered into the collection. These CVDs appear in the lower pane.

2 Click OK.

Add Dynamic Collections by Using Active Directory

You can use Active Directory (AD) to add a dynamic CVD collection. You can add CVDs to the collection by Active Directory group, organizational unit, or domain. You can create a filter for multiple Active Directory elements, for example, filter CVDs whose users belong to the Human Resources AD group or to the Marketing AD group.

The Active Directory is updated whenever a device is authenticated. Active Directory information might change if the Active Directory is updated for that user or device.

Procedure

1 In the Horizon Mirage Management console tree, expand the Inventory node, right-click Collections, and select Add a Collection.
   a Type the name and description for this dynamic collection.
   b Select Dynamic Collection.
   c Set the filter to define the dynamic collection by Active Directory group, Active Directory organizational unit, or Active Directory domain.
   d Click Apply to view the CVDs filtered to the collection. These CVDs appear in the lower pane.

2 Click OK.

Working with Archived CVDs

You can archive a CVD to preserve its data, snapshots and operational history for long term retention, for example, when an employee is on leave or leaves the company. You can also reinstate an archived CVD and assign it to another endpoint. You can delete archived CVDs that are no longer required to free up space.

After you archive a CVD, it does not require a Horizon Mirage license.

Archive CVDs

You can transfer a CVD that is not immediately required to the CVD archive.

Procedure

1 In the Horizon Mirage Management console tree, expand the Inventory node, and select All CVDs.
2 Right-click the CVD to archive, and click Manage CVD.
3 Click Archive CVD.
   The CVD is transferred to the CVD Archive.

View CVDs in the Archive

You can view a list of the CVDs that you archived.

Procedure

◆ In the Horizon Mirage Management console tree, expand the Inventory node and select Archive.
Delete CVDs from the Archive

Archiving CVDs can take up disc space. You can delete archived CVDs that you do not need.

Procedure
1. In the Horizon Mirage Management console tree, expand the Inventory node and select Archive.
2. Select the archived CVD to delete.
3. Click the Delete from Inventory icon on the CVD Archive toolbar.

Move Archived CVDs to Another Volume

You can move a CVD to another storage volume, according to your disc organization requirements.

Procedure
1. In the Horizon Mirage Management console tree, expand the Inventory node and select Archive.
2. Right-click the archived CVD to move and select Move to a different volume.
3. Select the volume selection option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically choose a volume</td>
<td>Allows Horizon Mirage to select the volume.</td>
</tr>
<tr>
<td>Manually choose a volume</td>
<td>Decide where to move the archived CVD yourself. Then select the volume.</td>
</tr>
</tbody>
</table>
4. Click OK.

Assign an Archived CVD to a Device

You can reinstate an archives CVD to assign it to an endpoint device, for example, when an employee returns to the company from leave.

The device can be the original endpoint device or a new device that is a replacement for the original device.

The procedure is the same as for reassigning a CVD to a different device. See “Reassign a CVD to a Different Device,” on page 117.

In this procedure, you select one of the following restore options for the selected CVD and device:
Table 2-3. Restore a CVD to a Replacement Device - Wizard Restore Options

<table>
<thead>
<tr>
<th>Restore Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full System Restore, including OS, Applications, User Data and Settings.</td>
<td>Use this option for systems with Windows volume licenses or Windows OEM SLP licenses. The entire CVD is restored to the replacement device, including OS, applications, and user files. Any existing files on the replacement device are lost or overwritten.</td>
</tr>
<tr>
<td>Restore Applications, User Data and Settings</td>
<td>Use this option when replacing a device that has a different Windows OEM license. The OS of the replacement device must be the same as that of the CVD. Only applications and user data are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.</td>
</tr>
<tr>
<td>Only Restore User Data and Settings</td>
<td>Use this option to migrate users from Windows XP/Vista/Windows 7 machines to new Windows 7 machines. The OS of the replacement device must be the same as or newer than that of the CVD. Only user data and settings are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.</td>
</tr>
</tbody>
</table>

- User data in these options pertain to files and directories listed in the upload policies User area. See “Working with Upload Policies,” on page 18.
- If you migrate a CVD from a Windows XP or Vista device to a replacement device that has Windows 7, you can select only Full System Restore or Only Restore User Data and Settings. This is because Horizon Mirage does not transfer user-installed applications from a Windows XP/Vista to a Windows 7 system. Horizon Mirage cannot guarantee cross-OS compatibility.

Prerequisites

Install the Horizon Mirage client on the client machine as described in “Installing the Horizon Mirage Client,” on page 13.

Verify that the drive letters of the new endpoint and the CVD in the data center are compatible. If the drive letters are different, the system does not allow the restore operation to proceed.

Perform Sync Now on the endpoint before migrating it to a new client machine. This ensures that all data is saved to the data center before the migration takes place. See “Sync Now and Snooze,” on page 29.

The procedure enables you to select a domain for this endpoint to join after the restore operation. If you want to use the same credentials each time, perform the following:

1. In the Horizon Mirage Management console tree, right-click System Configuration and select Settings.
2. Select the General tab and then type the credentials you want to use for domain joining.
   - The join domain account must meet the appropriate security privilege requirements. See “General System Settings,” on page 35.

Procedure

1. In the Horizon Mirage Management console tree, expand the Inventory node and select Archive.
2. Right-click the archived CVD and select Assign to a Device.
3. Select the device where you want to migrate the CVD and click Next.
   - Only devices compatible with the selected CVD are listed.
4 Select a restore option.
   a Select a restore option for the selected CVD and device.
      You can maintain the current layer, if one applies, select a new base layer from the list, or proceed
      without a base layer.
   b If you selected **Full System Restore**, select the base layer.
   c Click Next.

5 (Optional) Specify CVD naming and domain options.
   a Change or define the hostname for a device being restored.
   b Select a domain for this endpoint to join after the restore operation. The current domain is shown
      by default.
      Type the OU and Domain or select them from the drop-down menus.
      The drop-down menus are populated with all known domains in the system. Each text box shows
      the required syntax pattern.

      | Option              | Description                                                                 |
      |---------------------|-----------------------------------------------------------------------------|
      | OU                  | Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com. |
      | Join Domain account | The join domain account must meet the appropriate security privilege requirements as defined in the system general settings. The account must have access to join the domain. This is not validated. |

   c Click Next.

6 Use the validation summary to compare the target device with the CVD. This summary alerts you to
   any potential problems that require additional attention.
   You cannot proceed until blocking problems are resolved.

7 Click **Next** and click **Finish**.
   The CVD is moved from the CVD Archive to the All CVDs view.

The migration process proceeds and takes place in two phases. See “End User Experience with Restore
Processes,” on page 115.
End User Operations

Certain operations can be performed by end users, independently of the administrator, such as accessing client status information, restoring files or directories from the CVD, and temporarily suspending or resuming the client to server synchronization process.

This chapter includes the following topics:
- “Client Status Information,” on page 27
- “File-Level Restoration,” on page 28
- “Directory-Level Restore,” on page 29
- “Sync Now and Snooze,” on page 29

Client Status Information

Users can view information about the Horizon Mirage client.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Horizon Mirage version</td>
</tr>
<tr>
<td>Server Address</td>
<td>IP address or FQDN of the Horizon Mirage server</td>
</tr>
<tr>
<td>Connection Status</td>
<td>Shows whether Horizon Mirage is in a Connected or Disconnected state</td>
</tr>
<tr>
<td>Last Upload Time</td>
<td>Last time that Horizon Mirage successfully completed an upload of data to the data center</td>
</tr>
<tr>
<td>Current Base Layer</td>
<td>Base layer that is currently applied to this endpoint</td>
</tr>
<tr>
<td>Current Action</td>
<td>Operation that is currently being performed on this endpoint</td>
</tr>
<tr>
<td>File Progress</td>
<td>File-level progress of the current transfer operation</td>
</tr>
<tr>
<td>Data Progress</td>
<td>Data-level progress of the current transfer operation</td>
</tr>
</tbody>
</table>

Access the Client Status

You can view information about the client, including the client’s version information, current connection status and current action.

Procedure
- Right-click the Horizon Mirage icon in the notification area and select Show Status. The client status information appears.
File-Level Restoration

Users can restore a previous version of an existing file or a deleted file from snapshots stored on the Horizon Mirage server.

The restore is based on files and directories included in CVD snapshots, in accordance with the upload policies currently in effect. See “Working with Upload Policies,” on page 18.

When the CVD contains Encrypted File System (EFS) files, the files are recovered in their original encrypted form. Only EFS files that the recovering user encrypted are restored from the CVD. Unauthorized files are filtered from the restore.

The file restore operation generates an audit event on the Horizon Mirage server for management and support purposes.

Files are restored with their original Access Control Lists (ACLs).

Restore a Previous File Version

You can restore a previous version of an existing file.

Prerequisites

Verify that you have access permissions for the location to which to write. If you do not, you are redirected to My Documents.

Procedure

1. Right-click a file in Windows Explorer and select Horizon Mirage Restore.
2. Select the archive file version to restore.
   - If the file exists, the File size and Modify time are updated with the file’s archive information.
3. Click Restore.
4. Browse to the required location and save the file.
   - The default path is the original file location.

Restore a Deleted File from the Horizon Mirage Recycle Bin

You can restore a deleted file from the Horizon Mirage Recycle Bin.

For example, you can restore a file that was deleted from the My Documents folder. The file is reinstated at a location that you select.

Prerequisites

Verify that you have access permissions for the location to which to write. If you do not, you are redirected to My Documents.

Procedure

1. In Windows Explorer, right-click the parent directory from where the file was deleted and select Horizon Mirage Recycle Bin.
2. Select the archive date from which to restore the file.
   - Horizon Mirage downloads the archive information and searches for the available deleted files.
3. Double-click the archive file to restore.
4. Click Restore.
5. Browse to the required location and save the file.
   The default path is the original file location.

**Directory-Level Restore**

Users can recover entire directories back to their endpoint. The recovery includes all files and subfolders that the directory contains.

**Prerequisites**

- Verify that the directories to be recovered exist in a snapshot saved in the data center.
- Verify that you have access permissions for the location to which you want to write. If you do not, you are redirected to My Documents.

**Procedure**

1. In Windows Explorer, right-click the parent directory from which the folder was deleted and select Horizon Mirage Restore.
2. Select the archive date from which to restore the folder.
   Horizon Mirage downloads the archive information and searches for the available deleted folders.
3. Double-click the archive folder to restore.
4. Click Restore.
5. Browse to the required location and save the file.
   The default path is the original file location.

**Sync Now and Snooze**

The Horizon Mirage client synchronizes the endpoint with the Horizon Mirage server at defined intervals. A user might want to override the defined interval and synchronize immediately, or temporarily suspend the client’s synchronization activities.

The client uses the endpoint processing power to synchronize the endpoint with the server and keep it up to date. This synchronization occurs at intervals that the upload policy upload change interval parameter defines. See “Working with Upload Policies,” on page 18.

The client uses a network client throttle mechanism to regulate the data transfer. When the client senses user activity, it reduces or suspends its synchronization process until the endpoint is idle.

A user can use the Sync Now feature to start synchronization outside the defined intervals. For example, when important changes are made to documents and the user wants to verify that they are backed up to the CVD.

A user who is operating over a limited or metered network link can use the Snooze feature to temporarily suspend the client’s background synchronization activities. Using Snooze to override the client’s synchronization with the server affects the timing of scheduled CVD snapshots. For more information about automatic snapshot creation, see “CVD Snapshot Generation and Retention,” on page 38.
Procedure

- Synchronize the endpoint or temporarily suspend the synchronization.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync Now</td>
<td>Right-click the <strong>Horizon Mirage</strong> icon in the notification area and select <strong>Sync Now</strong>.</td>
</tr>
<tr>
<td>Snooze</td>
<td>To activate Snooze, right-click the <strong>Horizon Mirage</strong> icon in the notification area and select <strong>Snooze</strong>. The user can snooze the client for 15 minutes, 2 hours, or 4 hours. After this time elapses, regularly scheduled synchronizations that the network client throttle mechanism regulates resume.</td>
</tr>
<tr>
<td></td>
<td>To exit the Snooze state, right-click the <strong>Horizon Mirage</strong> icon in the notification area and select <strong>Sync Now</strong>. This reactivates the automatic synchronization mechanism.</td>
</tr>
</tbody>
</table>
Users can use the Horizon Mirage file portal to browse and view files in their CVD.

In some situations, for example in an MSP environment, user devices cannot access the corporate domain. To enable users to access their files, an administrator maps a CVD that is centralized in the system to specific domain users. Users who are not on the domain can access their files through the file portal by using their domain account.

Users access these files from the data center directly, not from the endpoint, so the endpoint does not need to be accessible for file portal purposes.

This chapter includes the following topics:

- “Allow Access to CVD Files,” on page 31
- “Configure User CVD Mapping,” on page 32
- “Browse and View Files with the File Portal,” on page 32

### Allow Access to CVD Files

The administrator can enable or block user access to CVD files in the Horizon Mirage file portal.

The **Show Web Access** icon in the user’s notification area indicates that a file portal URL is defined.

Users cannot access the file portal if any of the following conditions are present:

- The file portal feature is disabled.
- The CVD is blocked for Web Access.
- The device is assigned as a reference CVD.
- The assigned user is in a workgroup, not in a domain, and a domain user account was not mapped to the workgroup.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Inventory** node and select **All CVDs**.
2. Right-click a CVD, and allow or block Web access.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To allow Web access</td>
<td>Select File Portal &gt; Allow File Portal.</td>
</tr>
<tr>
<td>To block Web access</td>
<td>Select File Portal &gt; Block File Portal.</td>
</tr>
</tbody>
</table>
Configure User CVD Mapping

In some situations, such as MSP environments, user's devices cannot access the corporate domain. An administrator can manually map a CVD that is centralized with Horizon Mirage to specific domain users. Users who are not on the domain can then access their files through the file portal by using their domain account.

Procedure
1. In the Horizon Mirage Management console tree, expand the Inventory node and select All CVDs.
2. Right-click the required CVD and select Properties.
3. Click the File Portal tab.
4. Type the user domain account in the text box to the right of the relevant Local User cell.
5. Click Save.

Browse and View Files with the File Portal

End users can use the file portal to browse and view any files in their CVD.

End users access the files from the data center, not from the endpoint, so the endpoint does not need to be accessible for the file portal purposes.

End users have Read Only access to the files and cannot modify or upload them.

End users can select files from any available CVD snapshot, which means they can access files that were previously deleted or previous version of files from their snapshots.

**NOTE** When the CVD contains Encrypted File System (EFS) files, only EFS files that the accessing user encrypted are visible on the CVD. Non-authorized files are filtered from the view.

You can view the set of user files and directories that can be excluded from restoration, as defined in the upload policies User area. See “Working with Upload Policies,” on page 18.

Prerequisites

- Verify that a file portal URL is configured in the Management server.
- Verify that the administrator configured the file portal correctly

Procedure
1. Access the file portal login.
   - In the notification area of an endpoint that has the Horizon Mirage client installed, right-click and select Show File Portal.
   - If a file portal URL is not configured in the Management server, you can also access by going to http://mirage-server-address/Explorer/.
2 Log in to the file portal for your environment.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Use your corporate Active Directory login.</td>
</tr>
<tr>
<td>Hosted MSP (with domain)</td>
<td>Your corporate Active Directory profile is automatically mapped to your MSP login as part of file portal activation. This happens the first time you login to a computer with an active Horizon Mirage client.</td>
</tr>
<tr>
<td>Hosted MSP (without domain)</td>
<td>If you are not a member of a domain, the local profile on the client is manually mapped to the MSP login. This configuration is similar to the Hosted MSP with domain option. The administrator can perform the mapping manually using the Horizon Mirage Management console.</td>
</tr>
</tbody>
</table>

You can browse and open your files.
You can apply settings to your Horizon Mirage installation that the administrator can configure, including the retention policy for snapshots. You can also configure the system to use Secure Sockets Layer (SSL) communication between the Horizon Mirage client and server.

This chapter includes the following topics:

- “Configure the System Settings,” on page 35
- “CVD Snapshot Generation and Retention,” on page 38
- “Configuring Secure Socket Layer Communication,” on page 39

Configure the System Settings

The administrator can configure Horizon Mirage system settings.

Procedure

1. In the Horizon Mirage Management console, right-click System Configuration and select Settings.
2. Make the required changes and click OK.

   The system configuration takes effect immediately.

General System Settings

You can define the standard options for the Horizon Mirage system.

You access these options through the system settings General tab. See “Configure the System Settings,” on page 35.
Table 5-1. General System Settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshots kept</td>
<td>Type the number of CVD snapshots the system must keep available for restoration, at <strong>hour, day, week, and month</strong> intervals. For more information about how these values are used in snapshot retention, see “CVD Snapshot Generation and Retention,” on page 38.</td>
</tr>
</tbody>
</table>
| Volumes          | This section configures the threshold percentages of data stored on a volume, which when reached, trigger a warning. This section configures the threshold percentages of data stored on a volume, which when reached, trigger a warning or critical events in the Events log. For more information about using multiple volumes, see Chapter 7, “Deploying Multiple Storage Volumes,” on page 47.  
- Volume capacity - warning threshold (%): Type the threshold percentage of data stored on a volume, which triggers a warning event when reached.  
- Volume capacity - critical threshold (%): Type the threshold percentage of data stored on a volume, which triggers a critical event when reached.  
- Volume capacity check interval (seconds): Type the elapsed time interval (in seconds) at which the system rechecks the level of data stored on the volume against the thresholds.  
- Driver Library and USMT files volume: To choose the volume to be addressed by the threshold checks, click Change and select the required volume. |
| CVDs             |  
- CVD size warning threshold (MB): Type the maximum CVD size. An event is generated in the Event Log when that size is reached.  
- Default Upload Policy: To choose the default upload policy used when an end user adds their CVD to the Horizon Mirage system, click Change and select the required policy. |
| Join Domain Account | User and Password: Account which authorizes joining the domain. The join domain account is used during migration operations. Note: The join domain account must have the following permissions - Reset Password, Write all properties, Delete, Create computer objects, and Delete computer objects. Permissions are set using the Advanced Security Settings for Computers dialog box for this object and all descendant objects. |

Enable CVD Auto Creation

You can enable end users to manually create a new CVD for their machine. This avoids the need for the administrator to intervene in the critical first phase of adding the machine to the Horizon Mirage system.

You can also define the message that the end user sees when the operation takes place. After this is configured, any device that connects to the Horizon Mirage system prompts the end user to add their CVD.

You access these options through the system setting **CVD Auto Creation** tab. See “Configure the System Settings,” on page 35.

**Note**  An end user can also initiate the CVD creation by right-clicking the **Horizon Mirage** icon in their notification area.

**Procedure**

1. In the Horizon Mirage Management console, right-click **System Configuration** and select **Settings**.
2. Select the **CVD Auto Creation** tab.
3. Select **Enable automatic CVD creation** to change the user message if needed.
4. Click **OK**.

Configure File Portal Settings

File portal settings are used to enable the VMware file portal.

**Procedure**

1. In the Horizon Mirage Management console, right-click **System Configuration** and select **Settings**.
2 Select the File Portal tab.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable File Portal</td>
<td>Select this checkbox to enable the file portal feature.</td>
</tr>
<tr>
<td>File Portal URL</td>
<td>Specify the path to the file portal. For example, http://&lt;address&gt;/Explorer,</td>
</tr>
<tr>
<td></td>
<td>where &lt;address&gt; is the host where the Horizon Mirage file portal is installed.</td>
</tr>
<tr>
<td>User message</td>
<td>Type the message that the user will see when prompted for activation.</td>
</tr>
</tbody>
</table>

3 Click OK.

**Import USMT Settings**

You can import the Microsoft User State Migration Tools (USMT) files that are required for various base layer operations.

USMT files are used for the following base layer operations:

- Migration to Windows 7 from another Windows version.
- Cross-hardware Windows 7 Migration.
- User profile and Data-only restores.

**Note** This feature supports only USMT 4.

**Procedure**

1 Find the USMT folder in the directories installed with the Windows Automated Installation Kit (AIK) software.
   You can download this software free of charge from Microsoft.
2 Copy the USMT folder and all subdirectories to your Horizon Mirage server.
3 Click the Import USMT button to perform the import.

**Branch Reflector Settings**

Branch reflector settings include default values of parameters governing the behavior of branch reflectors.

For the relevant procedures, see Chapter 8, “Using Branch Reflectors,” on page 53.

**License Settings**

License settings are used to add a license to Horizon Mirage or view existing licenses.

For the relevant procedures, see Add and View Licenses in the Horizon Mirage Installation Guide.
CVD Snapshot Generation and Retention

A CVD snapshot is a centrally retained point-in-time image of CVD content, including OS, applications and user data, that enables complete restoration of a specific endpoint or a specific file. The Horizon Mirage server generates snapshots and keeps generations of snapshots available according to a retention policy.

Automatic Snapshot Generation

After the first successful CVD upload to a device, the Horizon Mirage server attempts to synchronize with the device at regular intervals, and to create a CVD snapshot when the synchronization is successful. The frequency of the attempts is defined by the Upload Change Interval parameter, for example every 60 minutes. See “Working with Upload Policies,” on page 18.

The success of a synchronization, and the snapshot creation, depends on the server being able to access the device at the scheduled intervals. This is not always possible since the device might be closed or the Snooze feature might be in effect. See “Sync Now and Snooze,” on page 29.

Snapshots can also be generated independently of the Upload Change Interval timing, in the following cases:

- Before a base layer update. This allows an administrator to revert to the CVD state before the update if the update fails or is problematic, or after any migration.
- Before reverting to a snapshot. This keeps the current endpoint state available in case a rollback is required.
- Whenever the administrator performs a forced upload. See “Reconnect a Device to a CVD,” on page 115.

According to these circumstances, the interval between specific snapshots can be longer or shorter than the time defined by the Upload Change Interval parameter.

Snapshot Retention Policy

The system keeps historical snapshots according to a retention policy, and can be used to restore files on the device.

You define the snapshot retention in the Snapshots kept area of the System Configuration General tab. See “General System Settings,” on page 35. The system keeps a maximum number of CVD snapshots at hourly, daily, weekly, and monthly intervals.
Table 5-2. Categories for Kept Snapshots

<table>
<thead>
<tr>
<th>Retention category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of snapshots at 1 hour intervals</td>
<td>Number of consecutively generated snapshots that the system keeps. For example, the value 8 means that the system always keeps the latest 8 successful CVD snapshots in this category. Historical snapshots older than the latest 8 are discarded. However, if daily snapshot retention is defined, whenever a first snapshot of a new day is created, the oldest snapshot in the Hourly category becomes a candidate as the newest daily snapshot. The default number of Hourly snapshots is zero, meaning new snapshots are not kept as they are created. You can change this value.</td>
</tr>
<tr>
<td>Number of snapshots at 1 day intervals</td>
<td>Number of snapshots that the system keeps in the Daily category. For example, the value 7, the default, means that the system always keeps the earliest-created snapshot in each new calendar day, up to 7 snapshots in this category. If hourly snapshots are defined, the oldest snapshot in the hourly category becomes the newest daily snapshot. Historical snapshots older than the latest 7 in the daily category are discarded. However, if weekly snapshot retention is defined, whenever a first snapshot of a new week is created, the oldest daily snapshot becomes the newest weekly snapshot.</td>
</tr>
<tr>
<td>Number of snapshots at 1 week intervals</td>
<td>Number of snapshots that the system keeps in the Weekly category. For example, the value 3, the default, means that the system always keeps the earliest-created snapshot in each new calendar week, up to 3 snapshots in this category. Other aspects of the weekly snapshot retention follow the same pattern as daily snapshot retention.</td>
</tr>
<tr>
<td>Number of snapshots at 1 month intervals</td>
<td>Number of snapshots that the system keeps in the Monthly category. For example, the value 11, the default, means that the system always keeps the earliest-created snapshot in each new calendar month, up to 11 snapshots in this category. Other aspects of the monthly snapshot retention follow the same pattern as daily or weekly snapshot retention.</td>
</tr>
</tbody>
</table>

The intervals between snapshots retained in each category depend on the factors described in “Automatic Snapshot Generation,” on page 38, and how device availability affects the retention rollover timing. For this reason, the snapshots in the daily, weekly, and monthly retention categories can typically have time intervals of at least a day, week, or month between them.

Automatic snapshots taken before a base layer update, before reverting to a snapshot, or forced uploads are counted against the snapshot retention capacity. They cause the number of regular snapshots retained to decrease.

Configuring Secure Socket Layer Communication

Horizon Mirage supports Secure Socket Layer (SSL) communication between the Horizon Mirage client and server.

The SSL setup is included as part of the server installation process. If for any reason this operation was disabled, you can perform the SSL setup at any time as described in this procedure.

The setup involves the following steps:

1. Installing the SSL server certificate. See “Install the Server SSL Certificate,” on page 40.

If you enable SSL on the server, you must also enable SSL on clients.

**Note** For environments with multiple Horizon Mirage servers, you must enable SSL and install the SSL certificate for each server. See “Setting Up the SSL Certificate in Windows Server,” on page 146.
Install the Server SSL Certificate

To set up SSL on the Horizon Mirage server, you must obtain SSL certificate values and configure them on the server. SSL Certificates is a Windows feature.

Procedure

1. Access the certificate store of the local machine account to check the server SSL certificate details.
   a. Select Start > Run.
   b. Type certmgr.msc.
   c. Select Certificates > Personal > Certificates to navigate to your certificate.
2. If you do not have a certificate, create one with tools such as the Microsoft makecert, and import the result into the Certificate Manager.
3. Note the Certificate Subject and Issuer values.
   The certificate values appear in the details of the certificate you imported.

What to do next

Continue to the server configuration procedure to enter the SSL certificate values. See “Configure Horizon Mirage Servers for SSL,” on page 40.

Configure Horizon Mirage Servers for SSL

After you install the SSL Server certificate, you configure the Horizon Mirage server maximum CVD connections and transport settings.

Allocate a larger number of concurrent CVDs for high-end servers, or a smaller number for low-end servers. For more information about this modification, contact VMware Support.

Procedure

1. In the Horizon Mirage Management console tree, expand the System Configuration node and select Servers.
2. Right-click the required server and select Configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Connections</td>
<td>Type the maximum number of concurrent CVD connections. The range is from 1 to 2500.</td>
</tr>
<tr>
<td>Port</td>
<td>Change the port used for client-server communication. Either use the default port of 8000 or change the port. Changing the port might require adding firewall rules to open the port.</td>
</tr>
<tr>
<td>TCP or SSL</td>
<td>Change the connection type to SSL to have clients communicate with the server using SSL encryption. This is a global change.</td>
</tr>
</tbody>
</table>
3. If you selected SSL, enter the Certificate subject and Issuer values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Subject</td>
<td>Typically the FQDN of the Horizon Mirage server.</td>
</tr>
<tr>
<td>Certificate Issuer</td>
<td>Usually a known entity like VeriSign. Leave this blank if only one certificate is on this server.</td>
</tr>
</tbody>
</table>
4. Click OK.
Managing the Driver Library

You use the driver library to manage hardware-specific drivers in a separate repository, organized by hardware families.

You add drivers with an import wizard and view them in the driver library’s console.

You can configure the system to add the necessary driver library to the relevant endpoints based on matching rules between the library and the endpoint configuration.

The driver handling is unconnected to layers. Not having to include drivers in the layer results in smaller and more generic layers.

This chapter includes the following topics:

- “Driver Library Architecture,” on page 41
- “Managing Driver Folders,” on page 42
- “Managing Driver Profiles,” on page 44

Driver Library Architecture

The driver library copies drivers from the Horizon Mirage system to the endpoint. When Windows scans for hardware changes, these copied drivers are used by the Windows Plug and Play (PnP) mechanism, and the appropriate drivers are installed as required.

This diagram illustrates the driver library architecture and how rules associate drivers to endpoints.
Profile A contains drivers from driver folder 1 and 2. When the profile is analyzed, the drivers from those folders are applied to two endpoints.

Profile B contains drivers only from driver folder 2, which is also used by profile A. When the profile is analyzed, the drivers from that folder are applied to only one endpoint.

The Horizon Mirage system can have multiple driver folders, multiple driver profiles, and many endpoints.

A driver profile can contain drivers from multiple driver folders and multiple driver profiles can use a driver folder.

You can apply a driver profile to one, many, or no endpoints.

The driver library is used during the following operations:

- Centralization
- Migration
- Hardware migration and restore
- Machine cleanup
- Base layer update
- Set driver library

Managing Driver Folders

Hardware drivers are imported and stored in driver folders in the Horizon Mirage system.

You can add driver folders to the root All folder, or create subfolders. You can also have Horizon Mirage mirror your current Driver Store folder structure.

The driver library has the following capabilities:

- You can group drivers by folder, for example, by common model. You can associate a driver with several folders.
- A folder can contain other folders, in a recursive hierarchy.
- You can enable or disable drivers within a folder, without deleting them.
- To view a device driver’s details, right-click any driver and select Properties.

**NOTE** For best results, obtain drivers directly from vendor Web sites, or restore media.
Create Driver Folders

You can create folders to hold related hardware drivers.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Driver Library** node.
2. Right-click **Folders** or any driver folder and select **Add folder**.
3. Type a folder name and click **OK**.

Change Driver Folders

You can rename or remove folders, or add hardware drivers to folders.

When you remove a folder, the drivers remain intact. The folder is a logical grouping of drivers that are stored on the system.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Driver Library** node and right-click any driver folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename the folder</td>
<td>Click <strong>Rename Folder</strong>, type the new name and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Remove the folder</td>
<td>Click <strong>Remove Folder</strong>, and click <strong>Yes</strong> to confirm.</td>
</tr>
<tr>
<td>Add drivers to the folder</td>
<td>Click <strong>Add drivers</strong>, select a driver and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

Import Drivers to Folders

You can import hardware drivers to driver folders to assist organization and accessibility.

You can have Horizon Mirage mirror your current **Driver Store** folder structure by selecting the **Keep original folder hierarchy** check box.

**Prerequisites**

- Verify that the Horizon Mirage Management server has access to the UNC path where the drivers are stored.
- Verify that you extracted drivers from the archive.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Driver Library** node, right-click any driver folder and select **Import drivers**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNC path</td>
<td>Type the UNC path where the drivers are stored. The path is scanned recursively.</td>
</tr>
<tr>
<td>Keep original folder hierarchy</td>
<td>Recreates the folder structure on your driver store in the Horizon Mirage system.</td>
</tr>
</tbody>
</table>

2. Click **OK**.
Add Drivers from the All Folder

The All folder in the driver library contains all the drivers in the library. You can add selected drivers from the All folder to one or more selected folders.

Procedure

1. In the Horizon Mirage Management console tree, expand the Driver Library node.
2. Select the All folder, right-click one or more drivers, and select Add drivers to folder.
3. Select individual folders in the tree.
4. Click OK.

Managing Driver Profiles

The driver library also contains driver profiles. A driver profile is used to select the driver folders to publish to a particular hardware model or set.

A driver profile can select one or more driver folders.

Driver profile rules check if a driver applies to a particular hardware, and can select one or more matching driver profiles for a device.

Create or Edit Driver Profiles

You can define driver profiles and the rules that apply to them. The rules are used during Horizon Mirage operations to validate the endpoints that use the profiles and check which profiles to apply to specific hardware.

Procedure

1. In the Horizon Mirage Management console tree, expand the Driver Library node, right-click Profiles, and select Add.
2. On the General tab, type a profile name and select the check boxes of drivers to apply in this profile.
   For example, if you are building a profile for a Dell Latitude E6410, select all the driver folders that apply to that hardware family.
3. On the Rules tab, use the drop-down menus to create specific rules for hardware families.
   For example, set the Vendor to Dell, and select the appropriate OS type.
4. Click Apply to test the result set that is returned by these rules.
5. Continue to fine-tune the rules until the result set is accurate.
6. Click OK.

What to do next

After you define rules, no more work is necessary for them to function. If devices that meet these criteria already exist in the Horizon Mirage system, you must start a driver profile update on those systems.

Apply Driver Profiles

You can apply newly created rules and profiles to already centralized endpoints.

The drivers are stored in one of the Horizon Mirage storage volumes in the MirageStorage directory, and deduplication is applied. If you have multiple volumes, you can change the volume where the driver library is stored by editing the system configuration settings.
This operation is not needed for clients added to the Horizon Mirage system after the driver library was configured. It is performed on those clients when an operation is performed that can use the driver library, including image updates, CVD restores, and so on.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Inventory** node and click **All CVDs**.
2. Right-click one or more CVDs, or a collection, and select **Apply Driver Library**.
3. (Optional) Right-click a CVD and select **Properties** to view the assigned driver profiles of a CVD.

   The driver library download progress appears in the desktop status window, the task list of the Management console, and the transaction logs.

   - A profile is selected for each device according to the rules.
   - Devices that match more than one profile receive a driver store that contains a merged view of all the matching profiles.
   - A warning or event, or both, is generated for devices that have no matching driver store.
Horizon Mirage provides multiple storage volume support to help manage volume congestion.

Each storage volume can contain base layers, app layers, and CVDs. CVDs are assigned to a storage volume when they are created. The storage volumes must be shared by the servers where Network-attached storage (NAS) permissions must be in place.

For more information about the relation between multiple servers and storage volumes, see “Using Multiple Servers,” on page 61.

This chapter includes the following topics:
- “View Storage Volume Information,” on page 47
- “Add Storage Volumes,” on page 48
- “Edit Storage Volume Information,” on page 49
- “Remove or Unmount Storage Volumes,” on page 49
- “Mount Storage Volumes,” on page 50
- “Block Storage Volumes,” on page 50
- “Unblock Storage Volumes,” on page 50
- “Maintain Storage Volumes,” on page 51

View Storage Volume Information

You can view information about all the storage volumes connected to the Horizon Mirage Management system.

You can view certain information about each storage volume, such as volume state, location, description, metrics, and status.

Table 7-1. Horizon Mirage Storage Volume Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique volume identification number set by the Horizon Mirage Management system.</td>
</tr>
<tr>
<td>Name</td>
<td>Volume name assigned when the volume was added.</td>
</tr>
</tbody>
</table>
Table 7-1. Horizon Mirage Storage Volume Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume State</td>
<td>Current state of the storage volume.</td>
</tr>
<tr>
<td></td>
<td>- Mounted. Volume is reachable and accessible.</td>
</tr>
<tr>
<td></td>
<td>- Malfunctioned. Volume is currently unreachable and inaccessible. CVDs and base layers on this volume cannot be accessed or used until the volume status is restored to Mounted. A manual action is needed to correct the problem. Run an SIS volume integrity check before returning the volume to the active state. See “Maintain Storage Volumes,” on page 51.</td>
</tr>
<tr>
<td></td>
<td>- Unmounted. Volume was temporarily disconnected by the administrator using the Unmount Volume function. See “Remove or Unmount Storage Volumes,” on page 49.</td>
</tr>
<tr>
<td></td>
<td>- Removing. Volume is in the process of removal from the system.</td>
</tr>
<tr>
<td>Path</td>
<td>UNC or local path where the volume resides.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the storage volume assigned when the volume was added. You can edit the volume information. See “Edit Storage Volume Information,” on page 49.</td>
</tr>
<tr>
<td>Capacity (GB)</td>
<td>Storage volume capacity in gigabytes.</td>
</tr>
<tr>
<td>Free Space (GB)</td>
<td>Amount of free space in gigabytes available on the storage volume.</td>
</tr>
<tr>
<td>Number of CVDs</td>
<td>Number of CVDs stored on the storage volume.</td>
</tr>
<tr>
<td>Number of Base Layers</td>
<td>Number of base layers and base layer versions stored on the storage volume.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the storage volume.</td>
</tr>
<tr>
<td></td>
<td>- (blank). The storage volume is available.</td>
</tr>
<tr>
<td></td>
<td>- Blocked. The storage volume is not used when creating new CVDs and base layers, but continues to serve existing stored entities. See “Block Storage Volumes,” on page 50.</td>
</tr>
</tbody>
</table>

Procedure

◆ In the Management console tree, expand the System Configuration node and select Volumes.

Add Storage Volumes

You can add storage volumes to the Horizon Mirage system.

When you add a new volume, the system checks that the path exists, the volume is empty, and the volume supports alternative data streams.

Prerequisites

Verify that the following conditions are met:

- The user account that manages the Horizon Mirage system has access permissions to the new volume.
- The volume has sufficient privileges for the Management server and the Horizon Mirage server cluster to access the required volume.
- The server service accesses the volume using the user credentials. In a CIFS (clustered) environment, the volume must be shared.
Procedure
1 In the Horizon Mirage Management console tree, expand the **System Configuration** node, right-click **Volumes** and select **Add a Volume**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name of the storage volume.</td>
</tr>
<tr>
<td>Path</td>
<td>Type the server UNC path of the volume where the volume resides.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the storage volume.</td>
</tr>
</tbody>
</table>

2 Click OK.

**Edit Storage Volume Information**
You can edit the volume name, description, and the UNC path in the storage volume information.

Procedure
1 In the Horizon Mirage Management console tree, expand the **System Configuration** node and select **Volumes**.
2 Right-click the required volume and select **Edit Volume Info**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Edit the volume name and the UNC path as needed.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description of the volume, if needed.</td>
</tr>
</tbody>
</table>

3 Click OK.

**Remove or Unmount Storage Volumes**
You can remove a storage volume from the Horizon Mirage system or unmount it.

Removing a volume deletes a storage volume from the system.

Unmounting a volume places the volume in a nonoperational status but retains the CVD and base layer data on the volume. Verify that the volume is unmounted before you perform maintenance operations such as integrity checks. The Volume State in the Volumes window is Unmounted.

**Prerequisites**
Verify that the selected volume is empty and does not contain CVDs or base layers. The remove operation fails if CVDs or base layers still reside on the volume.

Procedure
1 In the Horizon Mirage Management console tree, expand the **System Configuration** node and select **Volumes**.
2 Right-click the required volume and select **Remove Volume** or **Unmount Volume**.
3 Click **Yes** to confirm.
Mount Storage Volumes

You can activate an unmounted storage volume that is ready for reactivation.

Prerequisites

If the volume is in the Malfunctioned state, run the SIS integrity check before starting. See “Maintain Storage Volumes,” on page 51.

Procedure

1. In the Horizon Mirage Management console tree, expand the System Configuration node and select Volumes.
2. Right-click the required volume and select Mount.
   The Mount option is available when the Volume state is Unmounted.
3. Click Yes to confirm.

Block Storage Volumes

You can block a storage volume to prevent it from being used when new CVDs or base layers are being created.

Blocking a storage volume is useful when the volume reaches a volume capacity threshold or to stop populating it with new CVDs or base layers. Blocking a volume does not affect access or updates to existing CVDs and base layers on the volume.

IMPORTANT You cannot move a CVD or a base layer to a blocked volume. You can move a CVD or a base layer from a blocked volume.

Procedure

1. In the Horizon Mirage Management console tree, expand the System Configuration node and select Volumes.
2. Right-click the required volume and select Block.
3. Click Yes to confirm.
   The Volume Status column in the Volumes window shows Blocked.

Unblock Storage Volumes

You can unblock a volume that is currently blocked. The volume can then accept new CVDs and base layers and existing data can be updated.

Procedure

1. In the Horizon Mirage Management console tree, expand the System Configuration node and select Volumes.
2. Right-click the required volume and select Unblock.
3. Click Yes to confirm.
**Maintain Storage Volumes**

When a storage volume reaches a certain capacity, Horizon Mirage blocks operations such as writing to a storage volume.

When this occurs, you can:

- Increase the storage capacity by adding additional storage volumes to the Horizon Mirage Management console. Click **System Configuration > Volumes** to add storage volumes.

- Change the storage capacity of existing volumes in the Horizon Mirage Management console. Click **System Configuration > Volumes** to manage storage volumes.

- Delete CVDs from a storage volume.

- Move CVDs to another storage volume.

You can configure Horizon Mirage system settings for storage volume thresholds and alerts to enable you to trigger events in the events log. For more information, see “Configure the System Settings,” on page 35.

Additionally, inconsistencies may occur after a volume malfunction, such as following a network disconnect or storage access error. Performing a Single-Instance Storage (SIS) integrity procedure may help find and fix them.

When a volume state has changed to Malfunctioned, such as following a network disconnect or a storage access error, it is good practice to schedule a Single-Instance Storage (SIS) integrity procedure before mounting the volume on the system.

The SIS Integrity script is located in the *Wanova.Server.Tools.zip* file.

This procedure might take several hours to complete depending on the number of files on the volume. CVDs residing on the volume are suspended and base layers stored on the volume are not accessible during that time.

The SIS integrity procedure can also be run from *C:\Program Files\Wanova\Mirage Server*.

**Prerequisites**

Verify that the volume is unmounted before performing any maintenance operations such as integrity checks. See “Remove or Unmount Storage Volumes,” on page 49.

**Procedure**

1. Unmount the volume using the **Unmount** option.

2. Run the SIS Integrity script from a Horizon Mirage server.
   a. Open the command window.
   b. Type
      ```
      C:\Program Files\Wanova\Mirage Server>Wanova.Server.Tools.exe SisIntegrity -full volume path
      ```
      For example:
      ```
      SisIntegrity -full \apollo\vol100\MirageStorage
      ```

   An SIS integrity check summary appears when the SIS Integrity script is completed.
Using Horizon Mirage branch reflectors promotes efficient distribution to branch offices and remote sites where multiple users share the WAN link to the data center. You can enable the branch reflector peering service on endpoint devices that are installed with a Horizon Mirage client.

The branch reflector downloads base layer images, app layers, driver files, and USMT files from the Horizon Mirage server and makes them available for transfer to other Horizon Mirage clients in the site. Only files that reside on the branch reflector machine’s disk are transferred and files are not requested from the Horizon Mirage server at all.

In this way, files are downloaded to the branch reflector only once, and common files across base layers become readily available to other clients without duplicate downloads.

This chapter includes the following topics:

- “Branch Reflector Matching Process,” on page 53
- “Select Clients To Be Branch Reflectors,” on page 54
- “Enable Branch Reflectors,” on page 54
- “Configure Defaults for Branch Reflectors,” on page 55
- “Configure Specific Branch Reflector Values,” on page 55
- “Disable Branch Reflectors,” on page 56
- “Reject or Accept Peer Clients,” on page 56
- “Suspend or Resume Server Network Operations,” on page 57
- “Monitoring Branch Reflector Activity,” on page 57

**Branch Reflector Matching Process**

You can enable one or more branch reflectors per site. Client endpoints detect enabled branch reflectors on the same or different sites.

The Horizon Mirage IP detection and proximity algorithm finds a matching branch reflector using the following process:

1. The algorithm first verifies that a potential branch reflector is in the same subnet as the client.
2. If the branch reflector is in a different subnet, the algorithm checks if the branch reflector is configured to service the client subnet.
See “Configure Specific Branch Reflector Values,” on page 55.

Alternatively, the algorithm can use the client site information to check that the branch reflector is in the same Active Directory site as the client.

See “Configure Defaults for Branch Reflectors,” on page 55.

3 The algorithm checks that the latency between the branch reflector and the client is within the threshold.

See “Configure Defaults for Branch Reflectors,” on page 55.

4 If a client and branch reflector match is found that satisfies these conditions, the client connects to the branch reflector to download a base layer. Otherwise, the client repeats the matching process with the next branch reflector.

5 If no match is found or all suitable branch reflectors are currently unavailable, the client connects to the server directly.

Alternatively, to keep network traffic as low as possible, you can select Always Prefer Branch Reflector to force clients to continually repeat the matching process until a suitable branch reflector becomes available. See “Configure Defaults for Branch Reflectors,” on page 55.

In this case, the client connects to the Horizon Mirage server only if no branch reflectors are defined for the specific endpoint.

You can see the results of the Horizon Mirage IP detection and proximity algorithm for a selected CVD. See “Show Potential Branch Reflectors,” on page 59.

Select Clients To Be Branch Reflectors

You can select any Horizon Mirage client endpoint to function as a branch reflector, in addition to serving a user. Alternatively, you can designate a branch reflector to a dedicated host to support larger populations. A branch reflector can run on any operating system compatible with Horizon Mirage clients.

Prerequisites

Clients that serve as branch reflectors must satisfy the following conditions:

- Connect the device that will serve as a branch reflector to a switched LAN rather than to a wireless network.
- Verify that enough disk space is available to store the base layers of the connected endpoint devices.
- Verify that port 8001 on the branch reflector host is open to allow incoming connections from peer endpoint devices.
- If the branch reflector endpoint also serves as a general purpose desktop for an interactive user, use a dual-core CPU and 2GB RAM.

Enable Branch Reflectors

You enable branch reflectors to make them available to be selected by the Horizon Mirage IP detection and proximity algorithm for distribution to clients.

You can disable an enabled branch reflector. See “Disable Branch Reflectors,” on page 56.

Procedure

1 In the Horizon Mirage Management console tree, expand the Inventory node and select Assigned Devices.
2 Right-click an endpoint device and select **Branch Reflector > Enable Branch Reflector**.
   When a device is enabled as a branch reflector, it is listed in the Branch Reflectors window, as well as remaining on the Device Inventory window.

3 (Optional) Select **System Configuration > Branch Reflectors** to view which devices are enabled as branch reflectors.

### Configure Defaults for Branch Reflectors

You can set default values of parameters that govern the behavior of branch reflectors.

The current Maximum Connections and Cache Size values apply to newly defined branch reflectors. You can correct them individually for selected branch reflectors. See “Configure Specific Branch Reflector Values,” on page 55.

Other parameters in this window apply system-wide to all branch reflectors, existing or new.

#### Prerequisites

Verify that the branch reflector endpoint has enough disk space to support the **Default Cache Size** value, in addition to its other use as a general purpose desktop.

#### Procedure

1 In the Horizon Mirage Management console tree, right-click **System Configuration** and click **Settings**.
2 Click the **Branch Reflector** tab and configure the required default values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Maximum Connections</td>
<td>Type the maximum number of endpoint devices that can simultaneously connect to the branch reflector.</td>
</tr>
<tr>
<td>Default Cache Size (GB)</td>
<td>Type the cache size that the branch reflector allocated.</td>
</tr>
<tr>
<td>Required Proximity (msec)</td>
<td>Type the maximum time, for example 50 ms, for a branch reflector to answer a ping before an endpoint considers downloading through the branch reflector. The endpoint downloads from the server if no branch reflectors satisfy the specified proximity.</td>
</tr>
<tr>
<td>Use Active Directory Sites</td>
<td>Horizon Mirage uses subnet and physical proximity information to choose branch reflectors. Select this check box to use Active Directory site information to determine to which branch reflector to connect.</td>
</tr>
<tr>
<td>Always Prefer Branch Reflector</td>
<td>To keep network traffic as low as possible, select this option to force clients to continually repeat the matching process until a suitable branch reflector becomes available. In this case, a client connects to the Horizon Mirage server only if no branch reflectors are defined. If the option is not selected, and no match is found or suitable branch reflectors are currently unavailable, the client connects to the Horizon Mirage server directly as a last resort.</td>
</tr>
</tbody>
</table>

3 Click **OK**.

### Configure Specific Branch Reflector Values

Newly created branch reflectors are assigned default parameter values. You can adjust some of these values for individual branch reflectors.

Default values apply to the Maximum Connections, Cache Size, and Additional Networks parameters for newly created branch reflectors. See “Configure Defaults for Branch Reflectors,” on page 55. You can adjust these values for a selected branch reflector.
Prerequisites
Verify that the branch reflector endpoint has enough disk space for the indicated cache size, in addition to its other use as a general purpose desktop.

Procedure
1 In the Horizon Mirage Management console tree, right-click System Configuration, select Settings, and click the Branch Reflectors tab.
2 Right-click the branch reflector device and select Branch Reflector > Configure.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Connections</td>
<td>Type the maximum number of endpoint devices that can connect to the branch reflector at the same time.</td>
</tr>
<tr>
<td>Cache Size (GB)</td>
<td>Type the cache size in gigabytes that the branch reflector has allocated.</td>
</tr>
<tr>
<td>Additional Networks</td>
<td>Type the networks where the branch reflector is authorized to service client endpoints in addition to its own local subnets.</td>
</tr>
</tbody>
</table>

3 Click OK. The branch reflector configuration settings take effect immediately. You do not need to restart the branch reflector client.

Disable Branch Reflectors
You can disable the branch reflector peering service at any time.
When a branch reflector is disabled, the device is deleted from the Branch Reflectors list. But it continues to be available because an endpoint device remains as a regular Horizon Mirage endpoint in the device inventory.
When a branch reflector is disabled, its base layer cache is deleted.

Procedure
1 In the Horizon Mirage Management console tree, right-click System Configuration, select Settings, and click the Branch Reflectors tab.
2 Right-click the branch reflector device and select Branch Reflector > Disable Branch Reflector.

Reject or Accept Peer Clients
When the branch reflector is operating slowly or is using excessive bandwidth, you can stop providing service to its peer clients. You can resume providing service to the peer clients of a paused branch reflector at any time.
When you use the Reject Peers feature, the branch reflector is not deleted from the Branch Reflectors list. The branch reflector cache is preserved.
You can use the Accept Peers feature to resume providing service to the peer clients of a paused branch reflector.

Procedure
1 In the Horizon Mirage Management console tree, right-click System Configuration, select Settings, and click the Branch Reflectors tab.
Right-click the branch reflector device and reject or accept the peer clients.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reject peer clients</td>
<td>Select Branch Reflector &gt; Reject Peers.</td>
</tr>
<tr>
<td></td>
<td>The branch reflector service status is set to Paused.</td>
</tr>
<tr>
<td>Accept peer clients</td>
<td>Select Branch Reflector &gt; Accept Peers.</td>
</tr>
<tr>
<td></td>
<td>The branch reflector status is set to Enabled.</td>
</tr>
</tbody>
</table>

**Suspend or Resume Server Network Operations**

You can suspend network communications with the Horizon Mirage server for the branch reflectors and for regular endpoint devices. Suspending network operations for a branch reflector still allows peer clients to download layer files from the branch reflector cache, but the branch reflector cannot download new files from the server.

When you resume network operations, the branch reflector or the individual endpoint device can communicate with the Horizon Mirage server cluster.

**Procedure**

1. In the Horizon Mirage Management console tree, right-click **System Configuration**, select **Settings**, and click the **Branch Reflectors** tab.
2. Right-click the branch reflector device and select **Suspend Network Operations** or **Resume Network Operations**.
3. (Optional) Select **Connection State** from the column headings drop-down menu to view which branch reflectors are connected or suspended in the Branch Reflectors window.

**Monitoring Branch Reflector Activity**

You can monitor branch reflector and associated peer client base layer download activity. You can also show which branch reflectors are potentially available to a client, and the branch reflector to which it is currently connected, if any.

**View CVD Activity and Branch Reflector Association**

You can view the CVD current activity and associated upload and download progress and transfer speed.

The All CVDs window shows the following information.

- CVD current activity
- Percent completed of associated upload and download progress
- Rate of transfer speed in KBps

For more information, see “Show Potential Branch Reflectors,” on page 59.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Inventory** node and select **All CVDs**.
2. Right-click a CVD in the list and select **Device > Go to Branch Reflectors**.
View Branch Reflector and Peer Client Information

You can view information about branch reflectors and their connected peer clients.

The Branch Reflectors window shows the following information about peer client activity.

**Downloading Peers**
Shows how many peer clients connected to a branch reflector are downloading the base layer from this branch reflector.

**Waiting Peers**
Shows how many peer clients connected to a branch reflector are waiting to download.

Endpoints in excess of the maximum number of simultaneously downloading client peers allowed for this branch reflector are rejected and receive their download from another branch reflector or directly from the server. If you observe that the number of downloading peers is constantly close to the Maximum Connections, consider either increasing the Maximum Connections value or configuring another client in the site as a branch reflector.

The Connected Peers window shows the following information about connected peers clients:

- Peer client identifiers
- Peer client current activity, for example, waiting and downloading, and the progress of that activity.

**Procedure**

1. In the Horizon Mirage Management console tree, right-click **System Configuration**, and select **Settings**, and click the **Branch Reflectors** tab.
2. Right-click a branch reflector and select **Branch Reflector > Show Connected Peers**.

Monitor Branch Reflector and Peer Client Transactions

You can track branch reflector and peer client activity related to base layer, and how much data was acquired from a branch reflector by a peer client.

The Transaction Log window shows the following branch reflector and peer client activity related to base layer download.

- A branch reflector downloading the base layer.
- An endpoint in which a peer client has updated its image. The properties of the Update Base Layer transaction show how much data was downloaded from the branch reflector and how much data was downloaded directly from the Horizon Mirage server.

The Transaction Properties window shows how much data was acquired from a branch reflector by a peer client, for example, how much data the endpoint transaction downloaded from the branch reflector, and how much from the server.

**Procedure**

- To view the Transaction log, in the Horizon Mirage Management console tree, expand the **Logs** node and select **Transaction Log**.
- To view transaction properties, right-click a transaction line and select **Update Base Layer transaction > Properties**.
Show Potential Branch Reflectors

You can show which branch reflectors are potentially available to a selected client.

The Potential Branch Reflector window lists the branch reflectors that can potentially serve a selected client, in the order defined by the Horizon Mirage IP detection and proximity algorithm. See “Branch Reflector Matching Process,” on page 53. It also provides information about the branch reflector to which the CVD is currently connected.

**Table 8-1. Potential Branch Reflectors Window Information**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serving column</td>
<td>Green V denotes the branch connector is currently selected for the CVD by the Horizon Mirage IP Selection and Proximity algorithm.</td>
</tr>
<tr>
<td>Connection Status icon</td>
<td>Branch reflector's connection status with the server, and whether the branch reflector is currently connected, disconnected, suspended, or resumed.</td>
</tr>
<tr>
<td>Connected Peers and Waiting Peers</td>
<td>See “View Branch Reflector and Peer Client Information,” on page 58</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>Maximum connections to peer devices defined for the branch reflector. See “Configure Specific Branch Reflector Values,” on page 55</td>
</tr>
<tr>
<td>Last Connection Time</td>
<td>A branch reflector’s last connection time to the server.</td>
</tr>
</tbody>
</table>

The **Show in Branch Reflectors View** button opens the Branch Reflectors window with the potential branch reflectors for the CVD filtered in. See “View Branch Reflector and Peer Client Information,” on page 58.

**Procedure**

1. In the Horizon Mirage Management console tree, expand the **Inventory** node and select **Assigned Devices**.
2. Right-click a CVD in the list and select **Branch Reflector > Show Potential Branch Reflectors**.
Deploying Additional Horizon Mirage Servers

Horizon Mirage provides multiple storage volume support. Enterprise organizations with large numbers of endpoint devices can add servers to the system, providing better access and efficiency where a single server is not sufficient to keep up with data storage requirements.

This chapter includes the following topics:

- “Using Multiple Servers,” on page 61
- “View Server Information,” on page 62
- “Add New Servers,” on page 63
- “Stop or Start the Server Service,” on page 63
- “Remove Servers,” on page 64
- “Integrating a Load Balancing Framework,” on page 64

Using Multiple Servers

You can use the Horizon Mirage Management server and the console to control and manage the multiple servers.

An enterprise data center can configure multiple servers in a cluster. Each Horizon Mirage server, or cluster node, supports up to 1500 CVDs, depending on its actual system specifications. You can control the number of CVDs permitted on each server with the server configuration Maximum Connections option. See “Configure Horizon Mirage Servers for SSL,” on page 40.

Load balancers are used in conjunction with the Horizon Mirage system to direct client connections to available servers. For more information about load balancing in the Horizon Mirage system, see “Integrating a Load Balancing Framework,” on page 64. Any server that uses the Horizon Mirage file portal requires an IIS 7.0 installation.

Every server connects to every storage volume and the Horizon Mirage database. Network-attached storage (NAS) permissions must be in place.

The diagram shows how multiple servers in a cluster connect to clients via the system and load balancers. Each server shares all storage volumes and the Horizon Mirage database.
View Server Information

You can view information about the servers connected to the Horizon Mirage Management system. The Servers window provides information about servers in the system.

Table 9-1. Horizon Mirage Servers Window Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Unique server identification number configured by the Horizon Mirage Management system.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the server. Up Indicates the server is available and running. Down indicates that the server is not available.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the server machine.</td>
</tr>
<tr>
<td>Status duration</td>
<td>Amount of time that the server has been in the same status.</td>
</tr>
<tr>
<td>Connections</td>
<td>Number of CVDs currently connected to the server.</td>
</tr>
</tbody>
</table>

* VMware Horizon Mirage file portal requires IIS7.0 installed on the Horizon Mirage servers.
Table 9-1. Horizon Mirage Servers Window Information (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Connections</td>
<td>Maximum number of concurrent CVD connections allowed on the server. You can use the server configuration to configure this setting. See “Configure Horizon Mirage Servers for SSL,” on page 40. Use the default setting. Different server specifications allow changing this setting. For best results, consult with VMware Support before changing the default settings.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Indicates if this server is configured to have clients connect using SSL. This is a global configuration.</td>
</tr>
<tr>
<td>Port:</td>
<td>Port over which the Horizon Mirage server is configured to communicate with clients.</td>
</tr>
<tr>
<td>CPU</td>
<td>Average percentage of CPU running for this server over a 15 minute period.</td>
</tr>
<tr>
<td>Used memory (committed)</td>
<td>Average amount of memory in megabytes used for the server over a 15 minute period.</td>
</tr>
<tr>
<td>Physical Memory</td>
<td>Amount of physical memory allocated for the server.</td>
</tr>
</tbody>
</table>

Procedure

◆ In the Horizon Mirage Management console tree, expand the System Configuration node and select Servers.

Add New Servers

You can install multiple Horizon Mirage servers on the Horizon Mirage Management system. When the server is installed, it registers itself with the Horizon Mirage Management server and appears in the servers list.

See Install the Server in the Horizon Mirage Installation Guide.

Procedure

1. Double-click the Mirage.server.x64.buildnumber.msi file.
   The server installation starts.
2. Repeat the process for each server to install on the Horizon Mirage Management system.

Stop or Start the Server Service

When you need to perform server maintenance or backup, you can stop and start a server service.

See also “Suspend or Resume Server Network Operations,” on page 57.

Procedure

◆ In the Horizon Mirage Management console tree, expand the System Configuration node and select Servers.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To stop the server service</td>
<td>Right-click the server and select Stop Server Service. Click Yes to confirm.</td>
</tr>
<tr>
<td>To start the server service</td>
<td>Right-click the server and select Start Server Service. The server status is Up.</td>
</tr>
</tbody>
</table>
Remove Servers

You can remove a Horizon Mirage server from the Horizon Mirage Management system.
Removing a server does not uninstall the server, but removes only the server from the system. It does not remove CVD data from the shared storage volumes. You must uninstall a server manually.

Procedure

1. In the Horizon Mirage Management console tree, expand the System Configuration node and select Servers.
2. Right-click the server to remove and select Remove.
3. Click Yes to confirm.

Integrating a Load Balancing Framework

Administrators can use a load balancing framework, called VMware Watchdog, to integrate with existing load balancer servers and communicate state changes to them.

The VMware Watchdog service periodically checks if a specific server is running and can receive new connections.

Table 9-2. Horizon Mirage Server States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alive</td>
<td>Signals that a server is running and is available to receive new client connections.</td>
</tr>
<tr>
<td>Full</td>
<td>Signals that a server has reached the maximum number of concurrent connections. The service is still running, but new client connections are not accepted.</td>
</tr>
<tr>
<td>Dead</td>
<td>Signals that a Horizon Mirage server service is not responding or is not operational.</td>
</tr>
</tbody>
</table>

When the server state changes, VMware Watchdog calls an external command to communicate the state change to the load balancer. You can customize and configure the command to match the particular type of load balancer deployed in the data center. See “VMware Watchdog Service Configuration,” on page 64.

By default, the Watchdog service is initially disabled. You must start the service for it to function.

The Watchdog log file is located at C:\ProgramData\Wanova Mirage\Watchdog\Watchdog.txt.

VMware Watchdog Service Configuration

You can configure which service and port the VMware Watchdog service monitors, the time interval (in milliseconds), and the load balancing command to run when switching to any state.

You do this in the Watchdog configuration file, Wanova Watchdog.exe.xml, located in the C:\Program Files\Wanova\Mirage server directory.

You use a default script, called NLBControl.vbs, to work with the Microsoft Network Load Balancer (NLB). This script configures Microsoft Cluster (NLB) according to the system state. It contains a list of actions for enabling or disabling traffic for a specific server.

You then use the Watchdog configuration file Wanova Watchdog.exe.xml to configure the Horizon Mirage server host use the NLBControl.vbs script.

For each Horizon Mirage server, replace the IP address with the dedicated IP address of the server node as registered with the cluster manager.

Some NLB parameters are configurable through the XML file. The PollTimeMs, ServiceName, and ListenPort commands are relevant for all load balancing scripts.
After you edit XML file settings, you must restart the VMware Watchdog service.

**Note** Any time that you configure an NLB port rule, you must configure it to listen on all the cluster virtual IP (VIP) addresses and not just on a specific VIP address. This configuration is required for the default script to work.

### Table 9-3. NBL Parameters in the Watchdog.exe XML File

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
</table>
| PollTimeMs         | Polling frequency (in milliseconds)                                         | `<setting name="PollTimeMs" serializeAs="String">  
<value>5000</value>`                                                       |
| ServiceName        | VMware server service name                                                  | `<setting name="ServiceName" serializeAs="String">  
<value>VMware Horizon Mirage Server Service</value>`                     |
| ListenPort         | Listening port                                                             | `<setting name="ListenPort" serializeAs="String">  
<value>8000</value>`                                                      |
| OnAliveProcess     | Commands to run when the Horizon Mirage server is open to receive new connections | `<setting name="OnAliveProcess" serializeAs="String">  
<value>cscript.exe</value>`                                               |
| OnAliveArgs        | Arguments used for the OnAliveProcess commands                              | `<setting name="OnAliveArgs" serializeAs="String">  
<value>nlbcontrol.vbs 10.10.10.10 enable -1 </value>`                   |
| OnDeadProcess      | Commands to run when the Horizon Mirage server is down                      | `<setting name="OnDeadProcess" serializeAs="String">  
<value>cscript.exe</value>`                                               |
| OnDeadArgs         | Arguments used for the OnDeadProcess commands                               | `<setting name="OnDeadArgs" serializeAs="String">  
<value>NlbControl.vbs 10.10.10.10 disable -1</value>`                   |
| OnFullProcess      | Commands to run when the Horizon Mirage server cannot receive new connections | `<setting name="OnFullProcess" serializeAs="String">  
<value>cscript.exe</value>`                                               |
| OnFullArgs         | Arguments used for the OnFullProcess commands                               | `<setting name="OnFullArgs" serializeAs="String">  
<value>NlbControl.vbs 10.10.10.10 drain -1</value>`                     |
Horizon Mirage extends the image layer concept to image updates. Layers are not implemented just once during initial deployment. Separate app layers are used to distribute more specialized applications to specific groups of users.

The Horizon Mirage approach to image management involves a layer life cycle, which includes base layer and app layer preparation, capture, update, and assignment processes used to synchronize endpoints.

This chapter includes the following topics:

- “Base Layers and App Layers,” on page 67
- “Layer Management Life Cycle,” on page 67
- “Hardware Considerations with Base Layers,” on page 69
- “Image Management Planning,” on page 69

**Base Layers and App Layers**

A base layer is a template for common desktop content, cleared of specific identity information and made suitable for mass deployment to endpoints. You can also define app layers, separate from the common base layer, to distribute more specific applications to groups of users.

The base layer includes the operating system, service packs and patches, as well as core enterprise applications and their settings.

An app layer can include a single application, or a suite of applications. You can deploy app layers with other app layers on any compatible endpoint.

App layers require a base layer to be present on an endpoint, but the base layer and any app layers can be updated independently of each other.

The App layer assignment process is wizard driven and similar to base layer assignment. App layer options are listed under separate nodes in CVD views, in parallel with base layer action nodes.

The base layer can still include applications directly. App layers are not needed in organizations where everyone uses the same applications.

**Layer Management Life Cycle**

The base layer or app layer life cycle begins with a reference machine, where the administrator creates and maintains the layer content.

The layer management life cycle involves layer capture from a reference machine, layer assignment to endpoints, and CVD synchronization.
Figure 10-1. Layer Management Life Cycle

1. You manage and revise the base layer and app layer contents on a reference machine, through operations such as adding core or specific applications or patching the OS. See Chapter 11, “Preparing a Reference Machine for Base Layer Capture,” on page 73.

2. You perform a base layer or app layer capture from the reference machine using the Horizon Mirage Management console. Horizon Mirage collects the data from the reference machine to create the layer, which is generalized for mass deployment. You give the layer a name and version. You can make multiple captures from the same reference machine, and store them in the Horizon Mirage server’s layer repositories. See Chapter 12, “Capturing Base Layers,” on page 77, and Chapter 13, “Capturing App Layers,” on page 85.

3. You initiate base layer or app layer assignment, or update, from the Management console.
   - This operation first distributes and stores the revised layer at each endpoint, ready to be applied.
   - It then swaps the old base or app layer on the endpoint with the new one, thereby assigning the layer to that endpoint. The base layer, or specific applications in the app layer, are instantiated on the endpoint.

   See “Assign a Base Layer to CVDs,” on page 97 and “Assign an App Layer to CVDs,” on page 104.

4. The resulting changes in an endpoint are propagated back to the endpoint’s CVD on the server. After the CVD is synchronized with the latest changes, the layer update operation for that endpoint is completed.

   Each endpoint operates at its own pace, and this phase ends at different times for different desktops depending on network connectivity and whether the desktop is online or offline.

When you next update the base layer or an app layer, the process begins again by generating a new version of the layer.

The management life cycle for base layers is policy driven. For example, the Upload policy that belongs to the reference CVD contains system rules that determine which elements of the reference machine are not included in the base layer. Similarly, the Base Layer Rules policy determines which elements of the base layer are not downloaded to endpoints. Both policies contain system-defined defaults, which are typically sufficient for standard deployments. You can also add custom rules to the policy. See “Working with Base Layer Rules,” on page 77.
Hardware Considerations with Base Layers
You can create generic base layers for use on hardware families with the Horizon Mirage driver library feature. You can maintain a minimum number of generic base layers and use driver profiles to apply the appropriate hardware drivers.

Virtual Machine Support
A common Horizon Mirage situation is reassigning a CVD from a physical machine to a virtual machine, and the reverse. You can then download a CVD to a workbench virtual machine at the data center for troubleshooting purposes.

Most virtualization platforms include integration components to enhance the experience of working on a virtual machine, for example, VMware Tools. These components are also part of a virtual machine base layer.

Use a separate base layer for the virtual machine, especially if the integration features are part of the base layer, for example, VMware Tools.

Special Case Hardware Drivers
Certain hardware drivers include installation programs that make them incompatible for pre-installation in a base layer, for example, Bluetooth Driver installation and Wireless-over-USB. You can install these drivers using a special script that Horizon Mirage starts after a base layer is applied. Horizon Mirage then reports failures to the management service at the data center.

Image Management Planning
When you build a reference machine, choose the core software to include in the base layer carefully, as this software is distributed with the base layer to all end users.


See also “Reference Machine Software and Settings,” on page 74.

System-level Software
For best results, include the following applications in the base layer:

- Antivirus and security products such as anti-malware
- VPN or other connectivity software, such as iPass
- Firewalls
- Windows components and frameworks, for example, .NET, Java
- Global Windowa configuration and settings changes

System-level software is sensitive to conflicting software, so it is important that endpoints do not receive conflicting software through other distribution methods. If a certain type of system-level software, for example, antivirus is distributed with a base layer, do not distribute different versions of the same software or conflicting software through other software distribution mechanisms, and the reverse.

Include the organization VPN, antivirus, firewall applications, and the driver store in the minimal restore set.
Software Licensing

The base layer generally includes core applications that an organization uses, while more specialized applications are typically distributed with app layers. Verify that the software is suitable for mass distribution and uses a volume license that does not require machine-specific identification or individual manual activation.

Certain applications are protected by hardware-based identification methods or a unique license key that resides on the endpoint, for example, in a license file, and must not be distributed with the base or app layer or installed on the reference machine. The user can still install these applications on the endpoint or through software distribution solutions that target individual endpoints.

Most enterprise software is protected by a floating, or volume, license, which eliminates this problem.

User-specific Software

On the reference machine, install software as administrator, and if the option exists, install for All Users. Exclude user profiles on the reference machine from the base layer so that you do not distribute them. Do not distribute software installed exclusively for a specific user, because it might not function properly.

Example: The Google Chrome default installation is to the current user profile. Make sure to install it for All Users if it is to be included in the base layer.

To ensure the presence of an application shortcut on the end user’s desktop or Programs menu, verify that the shortcut is correctly created when the application is installed on the reference machine. If it is not, create the shortcut manually in the All Users profile.

Applications that set up and use local user accounts or local groups, or both, might not function well on endpoints when the base layer is applied to them. Consequently, you must exclude definitions of local user accounts and local groups from the base layer.

OEM Software

Many hardware vendors include special software to enhance the user experience of their platforms. These applications can support specific hardware buttons, connection management and power management capabilities, and so on.

To include special software as part of the base layer, use the base layer only for compatible hardware. Do not preinstall hardware-specific software on a single base layer that you want to use for multiple incompatible hardware platforms.

Use App layering for OEM software.

Endpoint Security Software

Horizon Mirage does not distribute software that changes the Master Boot Record (MBR). Full Disk Encryption software usually modifies the MBR, so this type of software cannot be delivered with a base layer. Such software can still be installed on individual endpoints through an external delivery mechanism or during first-time provisioning.

Examples of Disk Encryption software that use preboot authentication are Checkpoint Full Disk Encryption, PGFdisk, Sophos SafeGuard and McAfee Endpoint Encryption.

Certain security software products take measures to protect their software and do not allow other processes to modify their files. Software of this type cannot be updated through Horizon Mirage. Instead, use the security vendor-recommended update process to implement central control and management of that software. Horizon Mirage does not interfere with or manipulate the operation of these security products, and does not override the security measures they provide.
BitLocker Support

Microsoft BitLocker, in Windows 7, performs full-disk encryption and is fully compatible with Horizon Mirage. The state of BitLocker is maintained and managed on each endpoint and does not propagate to the Horizon Mirage CVD in the data center.

After you use BootUSB to do bare metal restore, the BitLocker state is not preserved and the machine is not encrypted.

The following BitLocker scenarios apply:

- If BitLocker is enabled on the target endpoint, it remains enabled after Horizon Mirage restore, base layer update, or rebase operations, regardless of the BitLocker configuration in the original endpoint on which the CVD was running, or on the reference machine from which the base layer was captured.

- Similarly, if BitLocker is disabled on the target endpoint, it remains disabled after Horizon Mirage restore, base layer update, or rebase operations.

**IMPORTANT** When you build a Windows 7 base layer for migration purposes, verify that BitLocker is disabled on the reference machine. Otherwise the migration operations cannot be completed.
Preparing a Reference Machine for Base Layer Capture

A reference machine is used to create a standard desktop base layer for a set of CVDs. A base layer on the reference machine usually includes operating system updates, service packs and patches, corporate applications for all target users to use, and corporate configuration and policies.

The reference machine used for app layer capture does not generally require advance preparation. Certain guidelines apply for special circumstances. A base layer does not have to be present on the reference machine for app layer capture purposes. For more information, see “Prepare a Reference Machine for App Layer Capture,” on page 86 and “Recreate a Reference Machine from a Base Layer,” on page 75.

This chapter includes the following topics:

- “Set Up the Reference Machine,” on page 73
- “Reference Machine Data Considerations,” on page 74
- “Reference Machine Software and Settings,” on page 74
- “Recreate a Reference Machine from a Base Layer,” on page 75

Set Up the Reference Machine

You assign a pending device as a reference CVD and configure it with applications and settings for a base layer that applies to a set of endpoints. After the reference machine is built and configured, the installed Horizon Mirage client uploads its content to an assigned reference CVD, which is used to capture a base layer.

A pending device that is assigned as a reference machine is moved from the Pending Devices list to the Reference CVDs view. See “Layer Management Life Cycle,” on page 67

**CAUTION** Files and settings from the reference machine are captured in the base layer, which are then distributed to a large number of endpoint desktops. To avoid unintended consequences, make sure the configuration is appropriate for mass distribution.

**Procedure**

1. In the Management console tree, expand the Inventory node and select Pending Devices.
2. Right-click the reference machine to be assigned and select Create a new Reference CVD.
3. Select the required upload policy and click Next.
4 Select a base layer and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t Use a Base Layer</td>
<td>For first-time use, when no base layer exists.</td>
</tr>
<tr>
<td>Select Base Layer from List</td>
<td>Select this option to select an existing base layer to apply updates and modify content.</td>
</tr>
</tbody>
</table>

5 Select a volume and click **Next**.

6 Click **Finish**.

The device is moved from the Pending Devices list to the Reference CVDs view.

After the reference machine is configured with applications and settings for a base layer, you can use it to capture a base layer.

**Reference Machine Data Considerations**

A base layer consists of all the files in the reference CVD, excluding a list of files and registry entries specified in the Base Layer Rules policy. The excluded items are the factory policy combined with user-customized base layer rules.

All the data placed on the reference machine is downloaded as part of a base layer. Keep the following considerations in mind when you use reference machines.

- Directories that reside directly under the root (C:\) are by default included in the base layer. Do not leave directories in the root that you do not want in the base layer.
- Avoid storing unnecessary data on the reference machine. Unnecessary data can consume excessive disk space on the endpoints.
- Verify that the Documents and Settings directory does not contain abandoned user profile directories. If an old user directory exists under the Documents and Settings directory and no user profile is registered for it in the system, the system considers it a regular directory and treats it as part of the base layer.

You can exclude specific areas of the reference machine from the base layer. See “**Working with Base Layer Rules**,” on page 77.

**Reference Machine Software and Settings**

The software installed on the reference machine becomes part of the base layer that you capture. When you deploy the base layer to other endpoints, those software and settings are delivered to those endpoints as well.

**Software Considerations**

Consider the following items before you decide on the software to include in your base layers:

- Do not include software that is licensed specifically to individual pieces of hardware, or whose licenses are tied to the hardware.
- If the reference machine contains OEM software, you can deploy that base layer only to endpoints of the same hardware family. This restriction is because OEM software is tied to specific hardware vendors, makes and models.
- The following items are examples of core corporate software that is typically the most commonly included software in a base layer:
  - Antivirus
VPN client
Microsoft Office
Corporate applications to be used by all target users

Departmental applications should generally be distributed through app layers.
You can install disk encryption software on the reference machine, but it must not be part of the base layer. Always deploy disk encryption software to the endpoints after.

For additional software considerations, see “Image Management Planning,” on page 69.

System-Wide Settings
System-wide settings are transferred from the reference machine to all machines that receive the base layer.

- Check which settings are required and configure them accordingly.
- In special cases, you can add specific exclusion rules to the Base Layer Rules policy. See “Working with Base Layer Rules,” on page 77.
- For more detailed control outside the base layer configuration, you can use Active Directory Group Policy Objects (GPOs) to configure settings.

Examples of settings in the reference machine are power management, remote desktop settings, and service startup options.

Domain Membership and Login Settings
If the target endpoints assigned to the base layer are members of a domain, verify that the following conditions are in place:

- The reference machine used for this base layer is a member of the same domain. Otherwise, users of the target endpoints are prevented from logging in to the domain and only local users can log in.
- The Net Login service is set to start automatically.

Recreate a Reference Machine from a Base Layer
When you want to update a base layer, but the reference machine that was used to create the original base layer is not available, you can recreate the original reference machine from the existing base layer.

Procedure
1. In the Horizon Mirage Management console, expand the Image Composer node and select the Base Layers tab.
2. Right-click the base layer and select Create Reference CVD from layer.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending device</td>
<td>Select a pending device and click Next.</td>
</tr>
<tr>
<td>Upload policy</td>
<td>Select an Upload policy and click Next.</td>
</tr>
</tbody>
</table>

3. Click Finish.
What to do next

Use a Horizon Mirage Restore operation to download and apply the image of the original reference machine to a selected device to serve as a new reference machine. See “Restoring to a CVD After Hard Drive Replacement or Device Loss,” on page 108. You then update or install core applications and apply security updates on the new reference machine before you capture a new base layer using the existing reference CVD.
Capturing Base Layers

After you set up the base layer for a reference machine, you can capture a base layer from it so that endpoints can be updated with that content.

The base layer capture process creates a point-in-time snapshot of the data and state of the live reference machine, generalized for mass deployment.

For more about the base layer deployment process, see “Layer Management Life Cycle,” on page 67.

A similar process is employed to capture app layers. See Chapter 13, “Capturing App Layers,” on page 85.

You can use a custom post-base layer script called post_core_update.bat to perform certain actions after the base layer update. See “Post-Base Layer Assignment or Provisioning Script,” on page 82.

This chapter includes the following topics:
- “Working with Base Layer Rules,” on page 77
- “Applying a Base Layer Override Policy,” on page 79
- “Capture Base Layers,” on page 81
- “Post-Base Layer Assignment or Provisioning Script,” on page 82

Working with Base Layer Rules

By default, the entire reference machine content is applied to the base layer. You can define rules to exclude specific content on the reference machine from being captured for the base layer, but include specified subsets of that content.

The system employs a built-in default rule set for production use. You can define a draft rule set, or edit a rule set. You can test a draft rule set, and when you are satisfied, define it as the default. Only the rule set currently defined as the default applies for base layer capture purposes.

When a draft rule set is being tested, only the selected CVD is affected. Other CVDs still use the default rule set, so the production environment is not affected.

You can also define Override policies to prevent specific endpoint content from being overwritten by the base layer. See “Applying a Base Layer Override Policy,” on page 79.

View Layer Rule Sets

You can select a rule set to view its details.

Procedure

1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Right-click a layer rule set and select Properties.
A read-only Layer Rules Details window shows the rule details.

Create a Rule Set based on an Existing Rule Set

You can create a copy of a selected rule set with its original details and a new name. You can edit the contents of the rule set. A new Draft layer rule set is listed in the Layer Rules list.

Procedure

1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Right-click a layer rule set and select Clone.
3. (Optional) Select the Show factory rules checkbox if you want to view the Horizon Mirage mandatory settings that the administrator cannot change. Factory rules are dimmed in the rules list.
4. Configure Do Not Download rules and rule exceptions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules list</td>
<td>Defines the files and directories on the reference machine that must not be applied to the CVD.</td>
</tr>
<tr>
<td>Rule Exceptions list</td>
<td>Lists specific files and directories within the directories to be excluded that must be applied.</td>
</tr>
</tbody>
</table>

For example:

C:\Windows* in the Rules list will exclude all Windows directories and files.

You can then apply only certain system DLLs in C:\Windows by typing specific paths in the Rule Exceptions list, such as: c:\Windows\system32\myapp.dll.

All files not matching a rule in the Rules list are applied to the CVD.

5. When you are finished working with this rule set, click OK.

What to do next

Consider whether override policies are needed to prevent specific problems. See “Applying a Base Layer Override Policy,” on page 79.

Test the rule set as a draft on several base layers. See “Test a Draft Layer Rule Set on a Test Machine,” on page 78.

When you are satisfied with the changes, you can define the new layer rule set as the Default rule set. See “Set the Default Rule Set,” on page 79.

Test a Draft Layer Rule Set on a Test Machine

It is good practice to test a rule set as a draft on several base layers.

When a draft rule set is being tested, only the selected CVD is affected. Other CVDs still use the default rule set, so the production environment is not affected.
Prerequisites
You can only test rule sets with Draft status. To test changes to the Default rule set, first create a clone of that rule set with the changes you want for testing purposes, then define that new rule set as the Default if the testing is satisfactory. See “Create a Rule Set based on an Existing Rule Set,” on page 78.

Procedure
1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Right-click the layer rule set to test and select Test Rules Draft.
3. Select the CVD on which you want to test the selected layer rules and click Next.
4. Select the base layer to use for the test.
5. Click Finish.

Test the Default Rule Set
You can only test rule sets with Draft status. To test changes to the Default rule set, first create a clone of that rule set with the changes you want for testing purposes, then define that new rule set as the Default if the testing is satisfactory.

Set the Default Rule Set
When you make changes to a rule set or create a rule set and you are satisfied with the changes, you can define the new layer rule set as the Default rule set.

Procedure
1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Right-click a Draft rule set and select Set As Default.

   The rule set has the status Default and replaces the previous default rule set for base layer capture purposes.

Applying a Base Layer Override Policy
You can define an override policy that allows the base layer to distribute a file only if the file does not exist in the CVD. You can also define an override policy for registry values and registry keys.

An override policy overcomes problems that can arise when base layers are updated, making it possible for certain CVD files to remain the same across base layer updates.

Add a Base Layer Override Rule Set
You can add a Do Not Override by Layer rule. This rule allows the base layer to distribute a file only if it does not exist in the CVD, and makes it possible for certain CVD files to remain the same across base layer updates.

The same syntax apply as for layer rule sets. See “Create a Rule Set based on an Existing Rule Set,” on page 78.

Procedure
1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Select a base layer rule set.

   The same syntax apply as for layer rule sets.
3 Scroll to and configure the **Do Not Override By Layer** rules and rule exceptions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rules list</td>
<td>Defines the files and directories on the reference machine that must not be applied to the CVD.</td>
</tr>
<tr>
<td>Rule Exceptions list</td>
<td>Lists specific files and directories within the directories to be excluded that must be applied.</td>
</tr>
</tbody>
</table>

All files not matching a rule in the Rules list are applied.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
</table>
| Add a new rule or a rule exception | a Click Add next to the relevant list.  
                             | b Type the rule or exception details, and click **OK**. |
| Edit a rule or rule exception | a Select the rule or rule exception line.  
                             | b Click **Edit** next to the relevant list.  
                             | c Correct the rule or exception details, and click **OK**. |
| Remove a rule or exception | Select the rule or exception line and click **Remove** next to the relevant list. |

4 When you are finished working with this rule set, click **OK**.

**Base Layer Override Examples**

You can construct base layer override policies to overcome problems that can arise when base layers are updated.

**Avoid Incompatibility When CVD and Base Layer Applications Share a Component**

A base layer update can cause a shared component to be unusable by an application that does not support the new component version.

Microsoft Office and Microsoft Visual Studio have a common shared component. Office is part of the base layer but Visual Studio is user-installed and part of the layer that maintains user-installed applications and user machine information.

Visual Studio includes a newer version of the shared component that is backwards compatible with Office, but the Office component version is too outdated for Visual Studio.

Without an override policy, every base layer update that occurs after Visual Studio is installed might corrupt the Visual Studio installation.

**Procedure**

1 In the Horizon Mirage Management console, expand the **Image Composer** node and select **Layer Rules**.
2 Add the path of the component to the Do Not Override By Layer policy section.

The following behavior is enforced:

- If the user first installs Visual Studio and then receives Office with a base layer update, Horizon Mirage recognizes that the component file already exists and does not override it, leaving the newer version.
- If the user first receives the base layer update, the component file does not exist and is downloaded as part of Office. If the user then installs Visual Studio, the newer version of the shared file is installed, and Office and Visual Studio function properly.
Avoid Losing Customizations at Initial Provisioning of a Global Configuration File

A base layer update can cause local customization of shared files to be lost.

Lotus Notes has a configuration file that is placed under the Program Files directory that is shared across all users. The base layer must initially provision the file for Lotus Notes to function properly. However, the file is then modified locally to maintain the user configuration.

Without a base layer override policy, each base layer update or Enforce All Layers operation causes user customization to be lost.

Procedure

1. In the Horizon Mirage Management console, expand the Image Composer node and select Layer Rules.
2. Add the configuration file path to the Do Not Override By Layer policy section.

The base layer version of the file is provisioned to users who receive Lotus Notes for the first time, but is not delivered to existing Lotus Notes users.

Overriding Registry Values and Keys

You can apply a base layer override policy for setting registry values and registry keys.

Overriding Registry Values

Registry values behave similarly to files.

- If a registry value exists, it is not overwritten.
- If the registry value does not exist, its content is distributed with the base layer.

Overriding Registry Keys

Registry keys behave uniquely.

- If a registry key path is included in the Do Not Override By Layer policy section, and the key exists in the CVD and the base layer, the key, including its subkeys and values, is skipped entirely in the base layer update.
- If the key does not exist in the CVD, it is handled normally and delivered with all of its subkeys and values with the base layer.

Capture Base Layers

After the reference machine is centralized to a reference CVD on the Horizon Mirage server, you can capture a new base layer from that reference CVD. You can capture the base layer from either an existing reference CVD, or a new reference CVD as a new source of layer capture.

Prerequisites

When you create a base layer to be used in a Windows 7 migration, make sure Windows 7 base layer migration requirements are satisfied. See “Set up the Windows 7 Base Layer for Migration,” on page 122.

Procedure

1. In the Horizon Mirage Management console, select Common Wizards > Capture Base Layer.
2 Select the capture type, and an existing CVD or pending device, and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use an existing reference CVD</strong></td>
<td>a Select to capture a base layer from an existing CVD.</td>
</tr>
<tr>
<td></td>
<td>b Select the reference CVD from which you want to capture the base layer.</td>
</tr>
<tr>
<td><strong>Create a new reference CVD</strong></td>
<td>a Select this to create a new source of layer capture.</td>
</tr>
<tr>
<td></td>
<td>b Select the pending device and the upload policy to use for this reference CVD.</td>
</tr>
</tbody>
</table>

3 Select the base layer capture action to perform and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Create a new layer</strong></td>
<td>Select this option and specify the new base layer details.</td>
</tr>
<tr>
<td><strong>Update an existing layer</strong></td>
<td>Select this option and the base layer to update.</td>
</tr>
</tbody>
</table>

4 Fix validation problems, click **Refresh** to make sure they are resolved, and click **Next**.

5 Specify your Microsoft Office 2010 license files and click **Next**.

6 Click **Finish** to start the capture process.

7 Click **Yes** to switch to the task list view where you can monitor the progress of the capture task.

When the task is finished, the base layer is moved to the Base Layers list under the **Image Composer** node and you can apply the capture to endpoints. See Chapter 14, “Assigning Base Layers,” on page 93.

### Post-Base Layer Assignment or Provisioning Script

You can include a custom post-base layer script in the base layer capture. This script performs certain actions required after a base layer update, such as installing software that must be run on the individual endpoint, or updating or removing hardware drivers that might already exist on the endpoint. You can also use a post-base layer script following a base layer provisioning operation.

Software required to be run on the individual endpoint can include hardware-specific software that is compatible with only certain endpoints.

The client installation includes a default sample script that does not perform post-base layer script actions.

The client continues to run the post-base layer script at every startup, until the first upload following the base layer update is finished. This ensures that the state of the CVD on the server includes the result of the post-base layer script. This process is also done for every enforce base layer operation.

**CAUTION** The script must include the relevant checks and conditional clauses so that any parts that require one-time execution are not run again.

### Prerequisites

The post-base layer script file and auxiliary files used or called by the script are captured as part of the base layer and distributed to the endpoints. Verify that the auxiliary files are placed in the same directory as the script or another directory that is captured in the base layer.
Procedure

1. After a base layer update operation, create a file called `post_core_update.bat` under the `%ProgramData%\Wanova\Mirage Service` directory.

   OR

   After a base layer provisioning operation, create a file called `post.provisioning.bat` under the `%ProgramData%\Wanova\Mirage Service` directory.

2. Edit the file on the reference machine to perform the required post-deployment actions on the endpoint.

   To monitor the execution of the post-base layer script, the client reports events to the central management service if the script returns an error value other than zero.
Capturing App Layers

You can provide sets of more specialized applications to specific users through app layers, independent of the core applications that are generally distributed with the common base layer.

You can capture an app layer with a single application, or a suite of applications from the same vendor. You can flexibly create app layers to include applications relevant for a specific department or group. You can combine app layers with other app layers and deploy them on any compatible endpoint.

You define and deliver app layers by capturing an app layer, then updating them to endpoints. See Chapter 15, “Assigning App Layers,” on page 103.

The app layer capture process creates a point-in-time snapshot of designated applications installed on a live reference machine, which is generalized for mass deployment.

You can use a CVD as the reference CVD for app layer purposes. A base layer does not need to be present on the reference machine.


This chapter includes the following topics:

- “App Layer Capture Steps Overview,” on page 85
- “Prepare a Reference Machine for App Layer Capture,” on page 86
- “Performing the App Layer Capture,” on page 87
- “What You Can Capture in an App Layer,” on page 90
- “Capturing OEM App Layers,” on page 91
- “Capture Multiple Layers on a Virtual Machine,” on page 91
- “Create a Post-App Layer Deployment Script,” on page 92

App Layer Capture Steps Overview

Capturing a single app layer involves several procedures.

For information about capturing multiple app layers, see “Capture Multiple Layers on a Virtual Machine,” on page 91.

Prepare the Reference Machine

A standard reference machine is required for capturing an app layer. A virtual machine is suitable for capturing most applications.

See “Prepare a Reference Machine for App Layer Capture,” on page 86.
Capture the Pre-install State

After the reference machine is ready, capture the preinstallation state of the machine.

See “Start an App Layer Capture,” on page 87.

Install the Applications

When the pre-installation state of the machine is captured, you install the applications to be captured, apply any application updates and patches, and customize global settings or configurations.

- “Install Applications on the Reference Machine,” on page 88
- “What You Can Capture in an App Layer,” on page 90
- “Capturing OEM App Layers,” on page 91
- “Application Upgrades,” on page 86

Capture the Post-Install State

After applications are installed, updated and configured, complete the capture. This process uploads the app layer to the Horizon Mirage server and adds it to the list of available app layers in the Management console. For more information, see “Post-Scan and Layer Creation,” on page 89.

Test the App Layer Deployment

Before you deploy app layers to many endpoints, test each captured app layer by deploying it to a selected sample of target endpoints to verify that the applications work as expected on these endpoints after deployment.

Deploy the App Layer

After testing is completed, the app layer is ready for deployment to any selected collection of target endpoints. See Chapter 15, “Assigning App Layers,” on page 103.

Application Upgrades

When a new version of an application is available, you can replace the existing app layer with a new layer.

1. Capture the upgraded application in an app layer, together with any other applications or updates required at that time. As described in this procedure, start with a clean reference machine and capture the installed new application.

2. After you have a new app layer, update the layers to replace the old app layer with the new app layer. See Chapter 15, “Assigning App Layers,” on page 103.

Prepare a Reference Machine for App Layer Capture

The reference machine for app layer capture should have a standard installation of the required operating system. Other advance preparation is not required. Certain guidelines apply for special circumstances.

Prerequisites

Verify that the following conditions exist for special circumstances:

- A virtual machine is created for capturing all except hardware-specific app layers.
- The reference machine has a standard installation of the required OS, for example, Windows XP, Windows 7 32-bit or Windows 7 64-bit.
App layers are deployed to compatible OS versions. You must capture app layers separately for Windows XP, Windows 7 32-bit, and Windows 7 64-bit. An app layer captured on Windows XP cannot be deployed on a Windows 7 (32-bit or 64-bit) machine, and the reverse. An app layer captured on Windows 7 32-bit cannot be deployed to Windows 7 64-bit, and the reverse.

Avoid software in the standard state of the reference machine that have the following characteristics:

- Can cause changes to be made to the machine while you are installing the applications.
- Is auto-updating. If you cannot avoid auto-updating software, try to disable the auto-update feature of any pre-existing software. For example, turn off automatic Windows Update installation and automatic anti-virus definition updates.

If you plan to capture a .NET-based application that uses a version of .NET not included in the standard Windows OS you installed, install the required .NET framework in the clean reference machine before you start the capture and install your application. Deliver the .NET framework itself through the base layer, if possible.

Verify that the standard reference machine is similar in content to the base layers used throughout the organization, for example, with the same Windows service pack version and .NET framework version as the base layer.

Procedure

1. Install the Horizon Mirage client on the reference machine.

   The virtual machine device state is Pending Assignment in the Management console.

2. Restart the reference machine.

   Restarting assures best scan performance when you are capturing app layers.

What to do next

Continue to capture the pre-install state of the machine. See “Start an App Layer Capture,” on page 87.

Performing the App Layer Capture

The app layer capture process starts with a pre-scan of the reference machine, installing the applications, and a post-scan.

- The pre-scan creates an image of the reference machine before the required applications are installed. See “Start an App Layer Capture,” on page 87.

- The application installation installs the required applications on the reference machine that was selected in the pre-scan. See “Install Applications on the Reference Machine,” on page 88.

- The post-scan creates an image of the reference machine after the required applications are installed. The system then detects all changes following the installation and starts the capture process. See “Post-Scan and Layer Creation,” on page 89.

Start an App Layer Capture

The pre-scan step creates an image of the reference machine before the required applications are installed. Follow the prompts to remove any validation warnings or errors.

Prerequisites

You can use any CVD as the reference CVD for app layer purposes.

The Horizon Mirage client is installed on a clean reference machine.

A base layer does not need to be present on the reference machine.
Procedure

1. In the Horizon Mirage Management console, select Common Wizards > Capture Layer.
2. Select a pending device from which to capture an app layer and click Next.
3. Select an upload policy and click Next.
   If you do not make an Upload policy selection, a default upload policy value applies.
4. Follow the prompts to remove validation warnings or errors and click Next.
   The validations ensure that the machine is ready for capture.
5. Click Finish to start the Pre-scan capture process.
   A message appears asking if you want to switch to the task list view to follow the progress of the capture task in the Task list.

When the task is complete, the app layer is moved to the App Layers list under the Image Composer node. The pre-scan processing starts. A progress window shows the Pre-Install State Capture progress. Alerts show the process stage.

The Task Monitoring window shows a Capture App Layer task, from which you can monitor the operation progress and status.

NOTE If you miss the message, check that the red recording icon appears on the Horizon Mirage icon before you start installing applications.

What to do next

When the Finished capturing pre-installation system state message appears, you can install applications to the reference machine. See “Install Applications on the Reference Machine,” on page 88.

Install Applications on the Reference Machine

The application installation step installs the required applications on a reference machine.

After the pre-scan step is completed, the client notifies you that you can install applications.

CAUTION Any file or registry change that you make inside the captured area will be part of the app layer and applied to endpoints when you deliver the app layer. The Horizon Mirage policy can configure this area. Avoid putting sensitive information in the reference machine used for capturing app layers that you do not want to distribute to other devices.


Prerequisites

- Horizon Mirage does not capture application installations or configuration changes made for specific user profiles for an app layer. Whenever applications such as Google Chrome give options to install or set shortcuts for either a specific user or globally for all users, always choose the all users option so that these installations and configurations are captured as part of the app layer.

- When you install applications, do not make any changes that are not wanted in the capture. For example:
  - Avoid installing software updates or applications that you do not want to capture.
  - Avoid launching other applications or Windows components that the installation process of the application you want to capture does not require.
  - Avoid hardware changes, domain membership changes, and other configurations that are not required.
Avoid GPO scripts running on the machine during the recording phase.

To reduce conflicts between vendors, install applications of the same vendor in the same single-app layer.

Whenever possible, install software that can be volume-licensed and does not require hardware-bound licensing and activation. Delivering hardware-bound licensed applications through app layers usually triggers reactivation of the software on the endpoints.

**Procedure**

1. Install all of the applications required to be captured for the app layer on the reference machine.
   
   This process includes applying application updates and patches to the installed applications, and customizing global settings and configurations.
   
   The CVD remains in a Recording mode until processing is started, which signals that application installations were completed.
   
   If the reference machine is rebooted for any reason, the console reminds you that recording is still in progress and that you should complete application installation.

2. **What to do next**

   After all the required applications are installed and tested on the reference machine, you can perform a post scan and create a layer. See “Post-Scan and Layer Creation,” on page 89.

**Post-Scan and Layer Creation**

After the scan, you create an image of the reference machine, after the required applications are installed. The process then detects all changes following the installation and starts the final capture.

**Prerequisites**

All application, update, and configuration changes must be successfully finished, including machine restarts that the application installer requires.

**Procedure**

1. In a Reference CVD view, select the reference CVD where you installed the applications to be captured.
2. Right-click the reference CVD and select **Finalize App Layer Capture**.
3. Verify the list of applications to be captured and click **Next**.
4. (Optional) Select the **Show Updates checkbox** to display hot fixes for Windows that were installed in the recording phase.
5. Select the type of capture and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new layer</td>
<td>Specify the new app layer details.</td>
</tr>
<tr>
<td>Update an existing layer</td>
<td>Select the app layer to update. Selected by default if the installed application upgrade codes indicate the new app layer is an update of an existing App Layer. You can change the selection.</td>
</tr>
</tbody>
</table>

6. Follow the prompts to remove validation warnings or errors and click **Next**.
7. If Microsoft Office 2010 is installed, define your Office license files and click **Next**.
8. Click **Next** again and click **Finish** to start the capture conclusion processing.

The Horizon Mirage client indicates the progress of the post-scan.
The Task list shows that the task is completed. The new app layer appears in the App Layers list.

**What to do next**

You can now apply the capture to endpoints. See Chapter 15, “Assigning App Layers,” on page 103.

**What You Can Capture in an App Layer**

You can capture a wide range of entities as part of an app layer.

**Supported Entities**

An app layer can contain the following entities:

- A single application or a set of applications
- Any updates or patches related to the installed applications
- Global application configurations and settings
- Any custom set of files and registry entries

For example, an app layer can contain Adobe Reader, Microsoft Visio 2010 or the entire Microsoft Office 2010 suite. An app layer can also be used to capture OEM software, such as the Dell software suite, including drivers and utilities.

---

**Note** When an update, patch, or service pack becomes available for an application in the app layer, you must capture a new complete app layer with the original application and the update installed in the application software.

Horizon Mirage can additionally contain the following elements:

- Windows services
- Kernel drivers
- Shell integration components or shell extensions
- Browser plug-ins
- COM objects
- Global .NET assemblies
- OS language packs

**Unsupported Entities**

The following components are not supported for delivery as part of Horizon Mirage app layers:

- User accounts and groups, both local and domain users, and user-specific changes
- OS components or OS-bundled applications, for example, the .NET framework, Windows updates, Internet Explorer, and Windows Media Player
- Windows license

---

**Note** You can deliver OS components or OS-bundled applications and the Windows license as part of a base layer instead.
Partially Supported Entities

The following applications are partially supported for delivery as app layers:

- Disk encryption software
- Applications that make changes to the Master Boot Record or to disk blocks
- Kaspersky Internet Security
- Microsoft SQL Server

Recommended for Base Layer Only

Install the following applications in the base layer and not in app layers:

- Windows security applications, for example anti-virus, anti-malware, and firewalls
- VPN or other connectivity software, such as iPass
- Windows components and frameworks, for example .NET, Java
- Global Windows configuration and settings changes

Capturing OEM App Layers

You must follow certain guidelines when you capture hardware-specific software.

Follow these guidelines to successfully capture hardware-specific software, such as Dell or HP application and driver suite.

- Some vendors provide a single OEM application suite that is compatible with many or most of their hardware models. Use this suite for the OEM layer capture.
- If the vendor only provides an OEM suite that is relevant for a specific hardware model or model line, install the OEM software on the hardware model for which it is intended or on a compatible model.
- Horizon Mirage provides the following ways to deliver OEM device drivers to target endpoints.
  - Through the driver library. For more information about how to deliver device drivers to specific hardware models in a rule-based manner, see Chapter 6, “Managing the Driver Library,” on page 41.
  - Through base or app layers. In this method, you either install or place all relevant device driver packages in the reference machine, in a path that is also defined in the Windows DevicePath registry value. You can also install the corresponding OEM applications in the same reference machine. You then capture a base or app layer from the reference machine. You can use this layer to deploy OEM applications and drivers to any endpoint of the matching hardware models.

Capture Multiple Layers on a Virtual Machine

When you need to capture multiple app layers, it is useful to use a single virtual machine.

Procedure

1. Create a standard reference machine on a virtual machine, install the Horizon Mirage client, and centralize the device to a reference CVD.

2. In the Management console, use the Start App Layer Capture option to take a snapshot of the clean pre-install state.

3. Install the applications.
4 In the Management console, use the **Finalize App Layer Capture** option to complete the creation of the app layer.

5 Wait until the app layer appears in the App Layers view of the Management console.

6 Revert the virtual machine to the Clean State snapshot.

7 Wait for the device status to become Pending Assignment.

8 Repeat Step 3 to Step 7 to capture the next app layer.

## Create a Post-App Layer Deployment Script

In rare cases, you might need the client to run a custom script after the app layer is deployed, for example, to apply a specific application license after it is installed through an app layer. This script is captured as part of the app layer.

**Procedure**

1 Start the App Layer Capture wizard to complete a prescan of the reference machine.

2 Install the application to be captured.

3 Give your script a unique name with this pattern: `post_layer_update_*.bat`
   
   For example: `post_layer_update_myappv2_license.bat`

4 Copy the script to `%programdata%\Wanova\Mirage Service`.
   
   This path usually translates to:
   
   - `c:\ProgramData\Wanova\Mirage Service` (Windows 7)
   - `c:\Documents and Settings\All Users\Application Data\Wanova\Mirage Service` (Windows XP)

5 Run the Finalize App Layer Capture wizard to complete the postscan and the creation of the app layer.

6 After the app layer is deployed to an endpoint, Horizon Mirage starts your script.
Assigning Base Layers

After a base layer capture is completed, the revised base layer is distributed and stored at each endpoint desktop, then applied, or assigned, at each endpoint.

Assigning a base layer to an endpoint, or collection of endpoints, applies the contents of the base layer to the designated endpoints. Any applications, updates, or patches built in the base layer also reside on the endpoint device. See “Assign a Base Layer to CVDs,” on page 97.

Similar processes are employed to assign applications associated with app layers to endpoints. See “Assign an App Layer to CVDs,” on page 104.

For more about the base layer deployment process, see “Layer Management Life Cycle,” on page 67.

This chapter includes the following topics:
- “Detect Potential Effects of the Layer Change,” on page 93
- “Testing the Base Layer Before Distributing it to Endpoints,” on page 96
- “Assign a Base Layer to CVDs,” on page 97
- “Assign a Previous Layer Version,” on page 99
- “Monitor Layer Assignments,” on page 99
- “Correct Software Conflicts By Using a Transitional Base Layer,” on page 100
- “Fix Broken Layers on Endpoints (Enforce Layers),” on page 100
- “Base Layer Provisioning,” on page 101

Detect Potential Effects of the Layer Change

Before you apply a new base layer or replacing app layers, or both, for a CVD or collection of CVDs, you can run a report that describes the potential effects of the layer changes on the CVDs. This report can help you plan the layer update process and resolve in advance conflicts that might result from mismatches in layer contents on the selected CVDs.

The Comparison report is generated in HTML format and opened in your default Web browser. You can use Microsoft Excel to view the report and filter data. See “Comparison Report Format,” on page 95.
Procedure

1. Choose the base layer to use in the analysis.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No change to the target base layer</td>
<td>Analyzes only app layer changes.</td>
</tr>
<tr>
<td>Select base layer from list</td>
<td>a Choose to apply a new base layer to all the selected CVDs.</td>
</tr>
<tr>
<td></td>
<td>b Select the required base layer.</td>
</tr>
<tr>
<td></td>
<td>If the selected CVDs have different base layers, this option standardizes the base layer over all the CVDs.</td>
</tr>
</tbody>
</table>

2. Choose the app layers to use in the analysis.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Layers panel</td>
<td>Lists the available app layers that are not currently used by any of the selected CVDs. When Show only latest layers is selected, older versions of any software are suppressed from the view.</td>
</tr>
<tr>
<td>Assigned layers panel</td>
<td>Lists the app layers currently used by some or all the selected CVDs. Black lines denote app layers used by all the CVDs, gray lines denote app layers used by only some of the CVDs.</td>
</tr>
</tbody>
</table>

3. Select what to analyze.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze only a base layer change without app layer changes:</td>
<td>Click Finish without making any changes in this page.</td>
</tr>
<tr>
<td>Add app layers to all the selected CVDs:</td>
<td>Select lines in the Available Layers panel and click the right arrow.</td>
</tr>
<tr>
<td>Remove app layers from all the selected CVDs where they are used:</td>
<td>Select lines in the Available Layers panel and click the right arrow.</td>
</tr>
</tbody>
</table>

4. Click Finish.

The HTML report is generated and opened in your default Web browser.

What to do next

Review the listed changes and adjust the reference machine to avoid unintended consequences. In the case of downgrades, consider upgrading the relevant software to avoid software being downgraded on endpoints or CVDs excluded from the assignment.

Compare Base Layers to Each Other

You can produce a comparison report that compares one or more base layers with another base layer.

The comparison report describes the differences between the contents of one or more base layers and a selected base layer. This report uses the same format as in "Detect Potential Effects of the Layer Change," on page 93, but in terms of base layers instead of CVDs.

Procedure

1. Select one or more base layers in the base layers view, right-click, and select Compare Programs with Layer.
2 Choose the base layer to use in the analysis.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No change to the target base layer</strong></td>
<td>Analyzes only app layer changes.</td>
</tr>
<tr>
<td><strong>Select base layer from list</strong></td>
<td>a Select to apply a new base layer to all the selected CVDs.</td>
</tr>
<tr>
<td></td>
<td>b Select the required base layer.</td>
</tr>
<tr>
<td></td>
<td>If the selected CVDs have different base layers, this option standardizes</td>
</tr>
<tr>
<td></td>
<td>the base layer over all the CVDs.</td>
</tr>
</tbody>
</table>

3 Choose the app layers to use in the analysis.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Available Layers panel</strong></td>
<td>Lists the available app layers that are not currently used by any of the selected CVDs. When <strong>Show only latest layers</strong> is selected, older versions of any software are suppressed from the view.</td>
</tr>
<tr>
<td><strong>Assigned layers panel</strong></td>
<td>Lists the app layers currently used by some or all the selected CVDs. Black lines denote app layers used by all the CVDs, gray lines denote app layers used by only some of the CVDs.</td>
</tr>
</tbody>
</table>

4 Select what to analyze.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analyze only a base layer change</strong></td>
<td>Click <strong>Finish</strong> without making any changes in this page.</td>
</tr>
<tr>
<td>without app layer changes:</td>
<td></td>
</tr>
<tr>
<td><strong>Add app layers to all the selected</strong></td>
<td>Select lines in the Available Layers panel and click the right arrow.</td>
</tr>
<tr>
<td><strong>CVDs:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Remove app layers from all the</strong></td>
<td>Select lines in the Available Layers panel and click the right arrow.</td>
</tr>
<tr>
<td>selected CVDs where they are used:**</td>
<td></td>
</tr>
</tbody>
</table>

5 Click **Finish**.

The HTML report is generated and opened in your default Web browser.

**What to do next**

Review the listed changes and adjust the reference machine to avoid unintended consequences. In the case of downgrades, consider upgrading the relevant software to avoid software being downgraded on endpoints or CVDs excluded from the assignment.

**Comparison Report Format**

The Comparison report summarizes the changes in the programs installed on the selected endpoints resulting from planned changes in their assigned layers.

You run the Comparison report for a selection of CVDs, pending devices, or a collection, as described in "Detect Potential Effects of the Layer Change," on page 93.

The report lists the layering operations to be performed and simulates the resulting user program list changes. The layering operations can include the following operations, in any combination:

- Base layer change or assignment
- Single or multiple app layer assignments or removals
- Enforcement or reinstallation of the current layers
- Enforcement with removal of user installed applications
This report is one of several Layer Dry-Run reports available from the Management Console Reports feature. See “Layer Dry Run Reports,” on page 134.

The report includes general information, user-installed application conflicts, and managed application changes sections.

**General Information**

**Table 14-1. General Information Section Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated By</td>
<td>Username of the administrator who generated the report.</td>
</tr>
<tr>
<td>New Base Layer</td>
<td>Base layer requested to be assigned, if any.</td>
</tr>
<tr>
<td>Added App Layers</td>
<td>App layers requested to be assigned, if any.</td>
</tr>
<tr>
<td>Removed App Layers</td>
<td>App layers requested to be removed, if any.</td>
</tr>
<tr>
<td>Enforced</td>
<td>Indicates whether the administrator asked to enforce the content of the layers.</td>
</tr>
</tbody>
</table>

**User Installed Application Conflicts**

User-installed application conflicts generate tables that summarize any conflict that the layer operation would involve, such as upgrade or downgrade, on programs installed or changed by users. Tables vary according to scope of changes. These conflicts cannot be anticipated from previous layering operations.

**Table 14-2. User Installed Application Conflicts Tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>Programs to be installed. Applies to Managed Application Changes section only.</td>
</tr>
<tr>
<td>Removed</td>
<td>Programs to be removed.</td>
</tr>
<tr>
<td>Downgraded</td>
<td>Programs to be downgraded.</td>
</tr>
<tr>
<td>Upgraded</td>
<td>Programs to be installed or upgraded to a new version.</td>
</tr>
</tbody>
</table>

**Managed Application Changes**

Managed application changes tables summarize the changes resulting from the layer operation on programs managed with Horizon Mirage layers. Tables vary according to scope of changes.

**Table 14-3. Managed Application Changes Tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed</td>
<td>Programs to be installed. Applies to Managed Application Changes section only.</td>
</tr>
<tr>
<td>Removed</td>
<td>Programs to be removed.</td>
</tr>
<tr>
<td>Downgraded</td>
<td>Programs to be downgraded.</td>
</tr>
<tr>
<td>Upgraded</td>
<td>Programs to be installed or upgraded to a new version.</td>
</tr>
</tbody>
</table>

**Testing the Base Layer Before Distributing it to Endpoints**

Because base layer updates include operating system and other critical component updates, test a new base layer before distributing it to endpoints.

After you capture a base layer, select a sample group of endpoints and distribute the base layer to them to verify that no problems exist.
If the base layer is used with multiple hardware platforms, test one sample per platform. Also do a test
distribution of a base layer to a typical user machine with user-installed applications to verify that the
overall update results are satisfactory before you distribute to multiple endpoints.

The Base Layer Rules policy is used during first-time deployment to identify the parts of the endpoint that
the base layer manages, and the parts to be left unmanaged at the endpoint. In an initial distribution, no
previous base layer exists to compare against, so Horizon Mirage does not remove existing software from
the endpoints before applying the base layer.

**Assign a Base Layer to CVDs**

After a base layer is updated at the server and tested on at least one CVD, you can assign it to individual or
multiple CVDs.

If collections are defined, you can assign the new base layer to all the CVDs in a collection in one step. See

The download to the endpoint transfers only new files and incremental changes to existing files of the target
endpoint.

When a file exists in a base layer, it overwrites the corresponding file in the target endpoint, unless one of
the following conditions apply:

- The file is defined in the **Do Not Download** rules in the Layer Rules.
- The file is defined in the **Unprotected Area** in the CVD Policy Details.

When software or system registry keys and values exist in the base layer, they overwrite the corresponding
registry keys in the target endpoint, unless the registry entry is defined in the Registry Keys To Exclude in the
**System Hive** or **Software Hive** tabs in the Layer Rules.

User profiles, for example c:\users\john, and any corresponding user registry hives are not overwritten by
the base layer update operation.

The process swaps the old base layer with the new one, assigning the base layer to the endpoint and
instantiating the endpoint. The changes in an endpoint are propagated back to the endpoint CVD on the
server.

Before a new or updated base layer is applied, the Horizon Mirage server takes a CVD snapshot so that it
can roll back in case of post-update problems.

Before and during base layer download, Horizon Mirage verifies that enough disk space is available to
proceed with the operation.

The same interfaces are used to apply or modify a base layer for multiple CVDs, or a collection.

You can upgrade an existing base layer or app layers to all CVDs that are already assigned with previous

During the assignment process, certain system aspects are validated.

<table>
<thead>
<tr>
<th>Table 14-4. Assignment Validations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Aspect</strong></td>
</tr>
<tr>
<td>Operating System</td>
</tr>
<tr>
<td>Computer Type</td>
</tr>
</tbody>
</table>
Table 14-4. Assignment Validations (Continued)

<table>
<thead>
<tr>
<th>System Aspect</th>
<th>Validation Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor and Model Name</td>
<td>The system checks that the base layer and the CVDs are from the same computer vendor. A warning appears if they are different. If the base layer was prepared to support the different vendor types, you can approve and continue.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>The system checks that the CVDs include the required drive letter in the base layer. If the CVDs do not have the appropriate drive letters, the system blocks these CVDs from receiving the base layer.</td>
</tr>
</tbody>
</table>

Prerequisites

Assign a base layer to a CVD only after endpoint centralization is completed for that CVD and its content is protected in the server. You can revert to the previous CVD state.

Procedure

1. In the Horizon Mirage Management console tree, select **Common Wizards > Assign Base Layer**
2. Select individual or multiple CVDs, or a collection of CVDs to update, click **Select** and click **Next** when you are finished.
   - The selected CVD details appear in the bottom pane.
3. Select the base layer with which you want to update the CVDs and click **Next**.
   - The details of a base layer appear in the bottom pane.
4. Correct mismatches between the base layer and the selected CVDs if needed.
   - Ignore any warnings that are not applicable. The following system aspects are validated.
5. Click **Finish**.
   - An update task is created. The client periodically checks the server for updates to download as part of its regular processing.

The administrator procedure is finished.

When the client next connects, download and swap operations take place, which ask the user to restart. Allow some time for the changes to download.

Cancel a Base Layer Assignment in Progress

You can discontinue a base layer assignment that is not yet finished.

Procedure

1. In the Management console tree, expand the **Inventory** node and select **All CVDs** or **Collections**.
2. Right-click the CVD or collection for which you want to cancel the base layer update.
3. Select **Layers > Cancel Pending Layers**.

Monitor the Layer Assignment Progress

After a layer is assigned to a number of CVDs, you can monitor the update process.

The layer deployment view displays the current status of the layer deployment progress.
Table 14-5. Assignment Progress States

<table>
<thead>
<tr>
<th>Progress State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>The layer was assigned to the CVD, but has not begun downloading to the endpoint.</td>
</tr>
<tr>
<td>Throttled</td>
<td>The endpoint tried to download the layer from the Horizon Mirage server and was rejected because of server resource throttling.</td>
</tr>
<tr>
<td>Downloading</td>
<td>The endpoint is downloading the layer.</td>
</tr>
<tr>
<td>Committing</td>
<td>The layer was downloaded and installed successfully by the endpoint and the client is now updating the CVD with the new content.</td>
</tr>
<tr>
<td>Blocked</td>
<td>The layer was blocked, and was not downloaded to the endpoint.</td>
</tr>
<tr>
<td>Canceled</td>
<td>The layer download process was canceled by the administrator.</td>
</tr>
<tr>
<td>Rejected</td>
<td>The layer was downloaded to the endpoint and failed the validation check on the endpoint.</td>
</tr>
<tr>
<td>Done</td>
<td>The layer update operation was completed.</td>
</tr>
</tbody>
</table>

Procedure

1. In the Horizon Mirage Management console, select the Task Monitoring node.
2. Right-click the specific layer task, and select View assignments.
   
   The specific layer update or assignment view appears.

Assign a Previous Layer Version

You can upgrade an existing base layer or app layers in all CVDs to which previous versions of those layers are already assigned. Programs in a CVD that are at the same version as in the layer are not reinstalled and not enforced.

The operation status is Update Layer, similar to a regular Update Layers operation.

Procedure

1. In the Management console tree, expand the Image Composer node and select Base Layers or App Layers.
2. Select the base layer or app layers with which you want to update all CVDs with previous versions of those layers.
3. Right-click and select Update CVDs to this layer version.

Monitor Layer Assignments

You can view and monitor which endpoints have certain layers assigned to them.

You can monitor layer assignment progress through the Layer Assignments window. The Task Monitoring window shows the overall status and the task progress.

Procedure

1. From the Horizon Mirage Management console, select a monitoring method.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To monitor all of your current layer assignments</td>
<td>Expand the Image Composer node and select Layer Assignments.</td>
</tr>
<tr>
<td>To monitor the progress of a base layer provisioning download to a specific device</td>
<td>Expand the Image Composer node, select Layer Assignments, right-click a CVD, and select Layers &gt; View assignments.</td>
</tr>
</tbody>
</table>
Correct Software Conflicts By Using a Transitional Base Layer

Before you apply a base layer, verify that software to be deployed by the base layer does not conflict with locally installed software, for example, an antivirus product on the base layer and on an endpoint are different.

You can perform an ad-hoc cleanup using a transitional base layer to remove conflicting software.

Procedure
1. Use the problematic endpoint as a reference machine to capture a temporary transitional base layer with the conflicting software.
2. Apply the transitional base layer to the endpoint and any similar endpoints.
3. Replace the temporary base layer by applying the base layer of choice, which replaces the conflicting software.

The initial rollout flow with a transitional base layer includes the following aspects:
1. Any application that is included in the transition base layer becomes a managed application when the transition base layer is assigned.
2. Managed applications undergo an update or removal process upon subsequent base layer update operations.
3. New base layers are constructed and endpoints are updated with the new base layer.

Fix Broken Layers on Endpoints (Enforce Layers)

Users and applications might make changes to files and registry settings that were provisioned through a base layer or app layer. Sometimes these changes create problems with the desktop operation. In most cases, you can resolve the problem by enforcing the layer originally assigned to the CVD.

The Horizon Mirage client downloads only the relevant files and registry settings required to realign the CVD with the original layer. User profiles, documents, and installed applications that do not conflict with the layer content are preserved.

Enforcing all layers can also be set to remove user-installed applications residing in the Machine Area of the CVD. This ability is useful, for example, for fixing a problematic CVD in which all layer applications do not function because of overwritten or corrupted system files. Removing user applications deletes Machine Area files and registry keys that are not in the current base layer, with the exception of files defined in the User Area policy.

Procedure
1. In the Management console tree, expand the Inventory node and select All CVDs.
2. Right-click the relevant CVD and select Enforce All Layers.
3 Select an enforce option.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preserve user applications</td>
<td>Keeps the user-installed applications on the CVD.</td>
</tr>
<tr>
<td>Remove user applications</td>
<td>Deletes user-installed applications from the CVD.</td>
</tr>
</tbody>
</table>

4 Click OK.

**Base Layer Provisioning**

When Horizon Mirage is already implemented, you can prepare new devices to be part of the organization using base layer provisioning.

The base layer provisioning process first cleans up the device files and applies an existing base layer as a common template. The device is then freshly imaged, and assigned to and synchronized with a newly created CVD.

After the Horizon Mirage client is installed on the new device, the Pending Devices panel shows the device as pending assignment, in the same way as when Centralize Endpoint applies. See “Centralizing Endpoints,” on page 15.

The user can use the desktop, including offline work and network transitions, as usual after the Centralization processing associated with the Provisioning operation starts. The Horizon Mirage client monitors user activities and adjusts its operation to optimize the user experience and performance.

After the server synchronization is completed, the Transaction log shows a successful endpoint centralization or provisioning entry. The desktop is protected and can be managed centrally at the data center.

You can use a custom post-base layer script called post_provisioning.bat to perform certain actions after the base layer provisioning. See “Post-Base Layer Assignment or Provisioning Script,” on page 82.

Base layer provisioning is supported for only Windows 7 base layers.

**Procedure**

1 In the Horizon Mirage Management console, select **Common Wizards > Base Layer Provisioning**.
   a Select the base layer that you want to provision with, and click Next.
   b Select the device or devices you want to assign, and click Next.
   c Select an upload policy and click Next. If you do not select an upload policy, a default policy defined in the system general setting applies.
   d Select the device name, set the domain, and click Next.
2 Click Next and click Finish.

When the initialization process is complete, the device starts downloading the base layer, performs a restart operation, and applies the base layer image. Then server synchronization starts. After the provisioning is finished, the device appears in the All CVDs view.

**What to do next**

You can monitor the provisioning progress. See “Monitor Layer Assignments,” on page 99.

The console shows the upload progress in the Progress column of the CVD inventory list.

The user can click the **Horizon Mirage** icon in the notification area to view the detailed status of the upload operation.
Assigning App Layers

After an app layer capture is completed, you can distribute and apply (assign) the revised app layer to each endpoint desktop.

Assigning app layers means applying their contents to an endpoint, or collection of endpoints, so that all the changes or modifications to the applications reside on the endpoint devices. See “Assign an App Layer to CVDs,” on page 104

For more information about app layers, see “Base Layers and App Layers,” on page 67.

For more information about the layer deployment process, see “Layer Management Life Cycle,” on page 67.

This chapter includes the following topics:

- “Detect Potential Effects of the App Layer Change,” on page 103
- “Testing App Layers Before Distributing it to Endpoints,” on page 103
- “Assign an App Layer to CVDs,” on page 104
- “Monitor App Layer Assignments,” on page 105

Detect Potential Effects of the App Layer Change

Before applying a new base layer or app layers, or both, to a CVD or collection of CVDs, you can run a report that describes the potential effects of the base layer or app layer changes on the CVD contents.

The Comparison report can help you plan the layer update process and resolve in advance conflicts that might result from mismatches in the layer contents on the selected CVDs.

For more information, see “Detect Potential Effects of the Layer Change,” on page 93 and “Comparison Report Format,” on page 95.

Testing App Layers Before Distributing it to Endpoints

It is good practice before you distribute an app layer widely to verify that it was captured properly and all intended settings are in place.

Before distributing to multiple endpoints, test-distribute an app layer to some sample user machines with user-installed applications to verify that the overall update results are satisfactory.
Assign an App Layer to CVDs

After an app layer is updated at the server and tested on at least one CVD, you can assign it to individual or multiple CVDs.

If Collections are defined, you can assign the new app layer to all the CVDs in a collection in one step. See “Working with CVD Collections,” on page 21.

The assignment process swaps the old app layer with the new one, thereby assigning the app layer to the endpoint and instantiating the applications to the endpoint. The changes in the endpoint are propagated back to the endpoint’s CVD on the server.

The download to the endpoint transfers only new files and incremental changes to existing files of the target endpoint.

Before a new or updated app layer is applied, the Horizon Mirage server takes a CVD snapshot so that it can roll back if any post-update problem arises.

Before and during app layer download, the system verifies that enough disk space is available to proceed with the operation.

The same interfaces are used to apply or modify app layers for multiple CVDs, or a collection.

**Note** You can upgrade an existing base layer or app layers to all CVDs that are already assigned with previous versions of those layers. See “Assign a Previous Layer Version,” on page 99.

**Prerequisites**

Verify that endpoint centralization is completed for that CVD and its content is protected in the server. You can revert to the previous CVD state.

Verify that the software to be deployed by the app layer does not conflict with locally installed applications. See “Correct Software Conflicts By Using a Transitional Base Layer,” on page 100.

**Note** App layer assignment requires a base layer to be present on the endpoints.

**Procedure**

1. In the Horizon Mirage Management console, select **Common Wizards > Update App Layer**.
2. Select individual or multiple CVDs, or a collection of CVDs that you want to update, and click **Select**. When you are finished, click **Next**.
3. Select the app layers with which you want to update the CVDs.

   The app layer details appear in the bottom pane.

   You select a layer in the Available Layers pane and click the right arrow to move it to the Assigned Layers pane. To remove a layer, select it in the Assigned Layers pane and click the left arrow.

   Layers shown in gray indicate that they are already assigned to some CVDs.
Correct mismatches between the app layer and the selected CVDs if needed. The following system aspects are validated. Ignore any warnings that are not applicable.

<table>
<thead>
<tr>
<th>System Aspect</th>
<th>Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>The system verifies that the CVD and the new app layer have the same OS and type (32- or 64-bit). If they are different, the system blocks those CVDs from receiving the app layer.</td>
</tr>
<tr>
<td>Drive Letters</td>
<td>The system verifies that the CVDs include the required drive letter in the app layer. If the CVDs do not have the appropriate drive letters, the system blocks these CVDs from receiving the app layer.</td>
</tr>
</tbody>
</table>

Click Finish.

An update task is created. The Horizon Mirage client periodically checks the server for updates to download as part of its regular processing.

This completes the administrator procedure.

When the client next connects, download and swap operations take place, which ask the user to restart. Allow some time for the changes to download.

Cancel an App Layer Assignment in Progress

You can discontinue an app layer update that is not yet completed.

Procedure

1. In the Management console tree, expand the Inventory node and select All CVDs or Collections.
2. Right-click the CVD or collection for which you want to cancel the app layer update.

Monitoring the App Layer Assignment Progress

After an app layer has been assigned to a number of CVDs, you can monitor the update process through the App Layer Deployment view.

The same method applies as for base layer assignment monitoring. See “Monitor the Layer Assignment Progress,” on page 98.

Monitor App Layer Assignments

You can see which endpoints have certain layers assigned to them. There are several ways to review and monitor currently running assignments.

The same methods apply as for base layer monitoring. See “Monitor Layer Assignments,” on page 99.
You can restore device files to a previous CVD snapshot, or restore a device from a CVD following hard drive replacement, file corruption, or format, or when the device is replaced.

Horizon Mirage provides disaster recovery in two key ways:

- Restore files or the entire desktop to a previous CVD snapshot on an existing device. Files and directories are included in CVD snapshots in accordance with the upload policies currently in effect. See “Working with Upload Policies,” on page 18.
- Restore the hard drive on an existing or a replacement device:
  - Restore a CVD to the same device after a hard-drive replacement, file corruption, or format.
  - Restore the CVD to a replacement device.

When the CVD contains Encrypted File System (EFS) files, the files are recovered in their original encrypted form.

**Note** For better deduplication in the revert-to snapshot, the end user must be logged in during the restore Prefetch operation if the CVD contains EFS files.

This chapter includes the following topics:

- “Restore a Device to a CVD Snapshot,” on page 107
- “Restoring to a CVD After Hard Drive Replacement or Device Loss,” on page 108
- “Working with Bootable USB Keys,” on page 111
- “Reconnect a Device to a CVD,” on page 115
- “End User Experience with Restore Processes,” on page 115

**Restore a Device to a CVD Snapshot**

You can use a CVD snapshot to restore a specific file or a complete endpoint on an existing device.

Horizon Mirage automatically creates CVD snapshots at regular intervals, and preserves them based on a retention policy, making them available for restoration purposes as needed. See “CVD Snapshot Generation and Retention,” on page 38.

You can use a selected CVD snapshot to restore a specific file or a complete endpoint on an existing device. The reversion can be between same operating system, for example, Windows 7 to Windows 7, or cross-operating systems, for example, Windows 7 to Windows XP/Vista.
Procedure

1. In the Horizon Mirage Management console tree, expand the Inventory node and select the All CVDs node.

2. Right-click the CVD that you want to restore to a previous snapshot and click Revert to Snapshot.

3. Choose the revert options:
   - Select the snapshot date to which you want to revert.
   - Restore System Only check box (selected by default): This restores system files only, including the base layer, user-installed applications and user machine settings. The user area content is not affected and any new files in the user area are not erased.

   The option behavior depends if the reversion you are performing is to same OS or cross-OS.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If to the same OS, for example, Windows 7 to Windows 7:</td>
<td>Deselect this check box if you want to restore the entire CVD, including the User area, from the CVD snapshot. If the checkbox is deselected, any application, setting, or document in the current CVD that does not exist in the snapshot is erased from the endpoint.</td>
</tr>
<tr>
<td>If to a different OS, for example, Windows 7 to Windows XP/Vista:</td>
<td>This checkbox is deselected and dimmed so the entire CVD, including the User area, is always restored from the CVD snapshot.</td>
</tr>
</tbody>
</table>

4. Complete the domain details. This applies only for Cross-OS reversions.
   - Fill in the domain details needed for the device to rejoin the domain.
   - Type the Domain and OU or select them from the drop-down menus.

5. Click Next and Finish.

Restoring to a CVD After Hard Drive Replacement or Device Loss

If the hard drive on an endpoint is replaced, corrupted, or formatted, or the user machine was lost and a new machine was supplied, you must restore the CVD to the device or a replacement device.

You must set up the device with at least a basic OS image that complies with Horizon Mirage software requirements. See Software Requirements in the Horizon Mirage Installation Guide.

You do not have to specifically identify the endpoint and locate the CVD in the console. The server recognizes the endpoint’s GUID in the device BIOS and finds the associated CVD.

Use one of the following restore procedures to restore a CVD:

- “Restore to CVD After Hard Drive Replacement, Corruption, or Format,” on page 108
- “Restore a CVD to a Replacement Device,” on page 109

Restore to CVD After Hard Drive Replacement, Corruption, or Format

You can restore a CVD after hard-drive replacement, file corruption or format.

Prerequisites

Install the Horizon Mirage client on the client machine. See “Installing the Horizon Mirage Client,” on page 13.
Procedure

1. In the Horizon Mirage Management console, select **Common Wizards > Disaster Recovery**.
2. Select **Replace Hard Disk** and click **OK**.
3. Select the device you want to use for the restore operation and click **Next**.
   Only devices that are recognized as connected to CVDs and are pending restore are listed.
4. Select a restore option.
   - Select the **Restore System Only** check box (default) to restore system files only, including the base layer, user-installed applications and user machine settings.
     The user area content is not affected and any new files in the user area are not erased.
   - Deselect the check box if you want to restore the entire CVD, including the user area, from the CVD snapshot.
     Any application, setting, or document in the current CVD that does not exist in the snapshot is erased from the endpoint.
5. Click **Next** and **Finish**.

**Restore a CVD to a Replacement Device**

You can restore a CVD to a replacement device.

In this procedure, you select one of the following restore options for the selected CVD and device:

<table>
<thead>
<tr>
<th>Table 16-1. Restore a CVD to a Replacement Device - Wizard Restore Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Option</strong></td>
</tr>
<tr>
<td>Full System Restore, including OS, Applications, User Data and Settings</td>
</tr>
<tr>
<td>Restore Applications, User Data and Settings</td>
</tr>
<tr>
<td>Only Restore User Data and Settings</td>
</tr>
</tbody>
</table>

- User data in these options pertain to files and directories listed in the upload policies User area. See “Working with Upload Policies,” on page 18.
- If you migrate a CVD from a Windows XP or Vista device to a replacement device that has Windows 7, you can select only Full System Restore or Only Restore User Data and Settings. This is because Horizon Mirage does not transfer user-installed applications from a Windows XP/Vista to a Windows 7 system. Horizon Mirage cannot guarantee cross-OS compatibility.

When a CVD is migrated from Windows XP or Vista to Windows 7, the system streams down to the endpoint after the CVD has been migrated so that the end user can resume work without waiting for all of the user data to be downloaded first.
If a Windows 7 endpoint is selected to be restored to a Windows XP or Vista CVD, that Windows 7 endpoint becomes a Windows XP or Vista device.

**NOTE** You can also migrate users from Windows XP or Windows 7 machines to new Windows 7 machines. See “Migrate to Windows 7 Replacement Devices,” on page 126. In this case, select **Only Restore User Data and Settings** as the restore option.

**Prerequisites**

Install the Horizon Mirage client on the client machine. See “Installing the Horizon Mirage Client,” on page 13.

The procedure enables you to select a domain for this endpoint to join after the restore operation. If you want to use the same credentials each time, perform the following:

1. In the Horizon Mirage Management console tree, right-click **System Configuration** and select **Settings**.
2. Select the **General** tab and then type the credentials you want to use for domain joining.

   The join domain account must meet the appropriate security privilege requirements. See “**General System Settings**,” on page 35.

**Procedure**

1. In the Management console, select **Common Wizards > Disaster Recovery**.
2. Select **Replace the user machine** and click **OK**.
3. Select the device where you want to restore the CVD. Only devices to which the CVD can be restored are listed and click **Next**.
4. Select a restore option.
   a. Select a restore option for the selected CVD and device.
      You can maintain the current layer, if one applies, select a new base layer from the list, or proceed without a base layer.
   b. If you selected **Full System Restore**, select the base layer.
   c. Click **Next**.
5. **(Optional)** Specify CVD naming and domain options.
   a. Change or define the hostname for a device being restored.
   b. Select a domain for this endpoint to join after the restore operation. The current domain is shown by default.

      Type the OU and Domain or select them from the drop-down menus.

      The drop-down menus are populated with all known domains in the system. Each text box shows the required syntax pattern.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU</td>
<td>Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com.</td>
</tr>
<tr>
<td>Join Domain account</td>
<td>The join domain account must meet the appropriate security privilege requirements as defined in the system general settings. The account must have access to join the domain. This is not validated.</td>
</tr>
</tbody>
</table>

c. Click **Next**.
6 Use the Validation Summary to compare the target device with the CVD. This summary alerts you to any potential problems that require additional attention. You cannot proceed until blocking problems are resolved.

7 Click **Next** and click **Finish**.

The migration process proceeds and takes place in two phases. See “End User Experience with Restore Processes,” on page 115.

**Working with Bootable USB Keys**

Horizon Mirage bootable USB media can assist you with recovery operations and system imaging. After it is created, the bootable USB key contains a clean install of Windows 7 Professional or Enterprise Edition. The Horizon Mirage client is also installed and pre-configured to connect to your Horizon Mirage server when the client machine restarts.

You can customize the Bootable USB key to accommodate different hardware platforms and additional pre- and post-Windows installation actions, for example, joining the new system to the required domain or renaming the system. The following are the most common use scenarios:

- Restoring a device which can no longer boot to Windows.
- Restoring or reimaging a remote device in the field.
- Provisioning or imaging a fresh Windows installation on an existing machine quickly.

Deploying the Windows image with the Horizon Mirage bootable USB key generally takes 15 to 30 minutes.

The following components are required:

- Windows 7 Professional or Enterprise Edition machine.
  This is represented in this guide as Drive C.
- Horizon Mirage bootable USB Scripts provided by VMware.
- Windows 7 Professional or Enterprise Edition DVD or ISO file.
  This is represented in this guide as Drive D.
- An 8 Gigabyte USB Drive
  This is represented in this guide as Drive U.
- Horizon Mirage client MSI installer file x86 or x64 version.
  You can find current clients on the Horizon Mirage support downloads page.
- (Optional) Drivers for the end point hardware
- Network drivers are highly recommended.
- All other drivers are available through the Driver Library feature within the Horizon Mirage server.

**Limitations**

- The Windows 7 installation is not activated and does not include a product key. Windows 7 allows working with a non-activated machine for a few days. You can work around this limitation by editing the autounattend.xml file.
- Some antivirus products (for example, Trend Micro) are known to prevent copying "autorun.inf" to removable disks. As the process of creating a bootable USB disk requires copying such a file, you must disable Trend Micro while creating the USB disk using this utility.
If you try to install Horizon Mirage with an SSL-enabled server, the newly deployed client machine might not be able to connect to the server, as it is not yet a member of the domain. In such a case, add a custom action on the USB disk to add the client machine to the domain.

**Windows XP Bootable USB Keys**

Horizon Mirage does not officially support a bootable USB key for Windows XP. To restore a bare metal Windows XP device, use your Windows 7 Bootable USB Key, and then use Horizon Mirage to restore the device to a previous Windows XP snapshot.

**Create the Bootable USB Key**

You can create a folder or drive or virtual-drive on a USB disk containing the Windows 7 installation folders.

**Prerequisites**

- The drive letter “U” must be available to create the bootable USB disk. The creation scripts do not warn you if it is already in use.

**IMPORTANT** The process formats the entire USB drive!

- When using an ISO file for Windows 7 installation, extract the content of the ISO file by one of the following methods:
  - Use .ISO image file software to download and save the .ISO image file to a CD-R or a DVD-R.
  - Virtually mount and access ISO files as a virtual device.
  - Extract the .ISO files to your hard drive.

Obtain the USB scripts BootUSB.zip file from VMware support.

**Procedure**

1. On your workstation, create the folder C:\BootUSB.
2. Create two subdirectories in C:\BootUSB. One called **Drivers** and one called **MirageClient**.
3. Extract the VMware Boot USB Scripts from the BootUSB.zip file to the root of the C:\BootUSB folder. Do not modify the file structure or add sub-directories.
4. Open the C:\BootUSB\MirageClient folder and copy the Horizon Mirage client installation MSI to this folder.
5. Find any hardware drivers you need for the new hardware and copy them to the C:\BootUSB\Drivers folder.
6. Insert the Windows 7 Pro DVD to your DVD Drive.
   Alternatively, you can mount your Windows 7 ISO file. This speeds up bootable USB key creation.
7. Insert the USB Key and wait until Plug and Play detection completes.
8. Run a Command Prompt window as an administrator and type `cd C:\BootUSB` and press Enter.
9. Type `win7usb.cmd` and press Enter.

   A list of the available disks and their disk number are displayed. Look for the disk number of your USB drive, which you can identify by the size value.
10 Run the complete command with the following syntax:

```
win7usb.cmd win7 dvd path msi path server address use ssl transport (true/false) usb disk number Drivers folder (optional)
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>win7 dvd path</code></td>
<td>Path to the Windows 7 DVD or folder containing Windows 7 installation files (folder containing the contents of the Windows 7 DVD).</td>
</tr>
<tr>
<td><code>msi path</code></td>
<td>Path of a Horizon Mirage client msi.</td>
</tr>
<tr>
<td><code>server address</code></td>
<td>IP address for your Horizon Mirage server for client devices to connect.</td>
</tr>
<tr>
<td><code>Use SSL transport</code></td>
<td>Whether this client will connect uses SSL (Use true or false).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The Horizon Mirage server must already be configured for the SSL for this to be turned on.</td>
</tr>
<tr>
<td><code>usb disk number</code></td>
<td>Number of the USB disk to format. A list of connected disk numbers is displayed upon invocation.</td>
</tr>
<tr>
<td><code>Drivers folder</code></td>
<td>This is where any hardware drivers you need on your new device are stored, from which you can add them to the bootable USB key. This parameter is optional.</td>
</tr>
</tbody>
</table>

The exact string for each endpoint will be different. This is an example of how a typical string might look:

```
C:\BootUSB>win7usb.cmd D:\
C:\BootUSB\MirageClient\MirageClient.x86.45071.msi
  192.168.11.203 false 2 C:\BootUSB\Drivers
```

assuming:

- Windows 7 DVD is in the D: drive
- Horizon Mirage client’s exact path and filename
- IP or FQDN of the Horizon Mirage server is 192.168.11.203
- SSL is turned off
- USB Key is listed as disk #2
- Endpoint drivers are in C:\BootUSB\Drivers

11 The USB disk is prepared. When the USB key creation is completed, you can customize it in additional ways. For example, you can have it install additional software, or embed hardware drivers).

**How to Install Windows with the Bootable USB Key**

You can use the bootable USB key to install Windows on a device.

**Prerequisites**

Do not unplug the USB disk until this process is fully completed and you have Windows and Horizon Mirage installed on your Windows 7 system.

**Procedure**

1. Perform a one-time boot from the USB disk by choosing the correct option in the startup menu.

   For example, most Dell laptops use the F12 key. Windows 7 begins loading.

   The process is very similar to a clean install of Windows 7.
2. Install Windows.

Prompts can vary according to the version of Windows you are installing and Windows installations, if any, currently on the endpoint.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version of Windows</strong></td>
<td>Select a Professional or Enterprise edition. Horizon Mirage does not support Home editions.</td>
</tr>
<tr>
<td><strong>Upgrade and custom (advanced)</strong></td>
<td>Select the Custom (advanced) option.</td>
</tr>
</tbody>
</table>
| **Partition**                 | Select a partition in which to install the new copy of Windows. Formatting the partition is optional.  
**NOTE** VMware software does not modify any existing partition tables. |

Windows now installs. No further user intervention is required.

In the process, the target machine restarts several times to complete the Windows install. This is normal.

3. After the installation is complete, log in with the following login information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>The default user is TEST.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>The password is: password</td>
</tr>
<tr>
<td><strong>Administrator password</strong></td>
<td>The default administrator password is: passwd1!</td>
</tr>
</tbody>
</table>

**NOTE** You can change these passwords by editing the account values in the autounattend.xml file found on the USB Key. You can use the System Image Manager (SIM) tool that comes with the Windows Automated Installation Kit (AIK) to do this.

After you login for the first time, the target machine is ready to use but might perform additional Windows operations in the background.

### Customize Your Bootable USB Key

After the Bootable USB is created, you can customize and configure it to suit your site or location.

You can use a number of files that for this purpose without having to rebuild the Bootable USB key in the process. Unless specified otherwise, these files are located in: `USB_ROOT\sources\$oem}\$$\setup\Wanova\`

<table>
<thead>
<tr>
<th><strong>Table 16-2. Customization Files</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Name</strong></td>
</tr>
<tr>
<td>InstallClient.cmd</td>
</tr>
<tr>
<td>SetupComplete.cmd</td>
</tr>
<tr>
<td>MirageClient.msi</td>
</tr>
<tr>
<td>Autounattend.xml</td>
</tr>
</tbody>
</table>
Procedure

1. (Optional) Add Boot-critical drivers to the Bootable USB by putting them in `<USB DRIVE>:\$WinPEDrivers$`.
   Do this only if the Windows 7 installation cannot proceed due to missing a critical driver, for example, a missing disk controller, preventing the installation from detecting the hard drive.

2. Copy the contents of `<USB DRIVE>:\sources\$oem$\$1\MirageDrivers` to the local folder `C:\MirageDrivers`.
   The Windows 7 installation will search and use drivers located in the folder “MirageDrivers” on the root of any drive.

3. (Optional) You can customize the Windows 7 installation further in the following ways:
   a. Copy the contents of `<USB DRIVE>:\sources\$oem$\$` to the Windows folder on the installation drive, e.g. `C:\Windows`.
   b. Copy the contents of `<USB DRIVE>:\sources\$oem$\$1` to the installation drive, e.g. `C:\`.

Reconnect a Device to a CVD

You can reconnect a device that has lost its synchronization for any reason to its CVD. After the Force Upload operation, you can then continue backing up incremental changes as before.

You can connect an Assignment Pending device to an existing CVD and upload the current device data to the CVD through a **Force Upload** process.

Procedure

1. In the Horizon Mirage Management console, expand the **Inventory** node and select **Pending Devices**.
2. Select the device, right-click and select **Force Upload**.
   The device then synchronizes all its data to the CVD. Local client changes take precedence (“win”) over CVD changes.

End User Experience with Restore Processes

End users can start working as soon as a subset of data is resident on their endpoints. An end user or application request for a file that is not yet downloaded, takes priority over background transfers. When the file finishes downloading, the system notifies the end user that the file is available.

Restore processes take place in two phases: Restore Prefetch and Restore Streaming.

**Restore Prefetch**

The server downloads the minimal set of files and configuration required for the endpoint to boot to the CVD and connect to the network. This is called the Minimal Restore Set. End users can start working as soon as this subset of data is resident on their endpoints.

**Restore Streaming**

After the Minimal Restore Set is downloaded and reboot is completed, the server begins streaming the remaining CVD content to the endpoint in the background while the end user works. If the user or application request a file that is not yet downloaded, this request takes priority over background transfers.

The end user can view the streaming status of each downloading file by right-clicking the **Horizon Mirage** icon in the notification area and clicking **Show Streaming Status**.
When an end user opens a file which is not yet fully downloaded, the system notifies the user that the file is currently downloading. When the file finishes downloading, the system notifies the end user that the file is available.

The system might advise the end user to wait until the connection is reestablished.

CVD files which have not yet been streamed to the endpoint appear in Windows Explorer with the Offline icon overlay. This indicates that the files exist on a remote storage medium and that accessing them involves a network download delay.
Migrating Users to Different Hardware

You can move a user from one device to another, for example, when new hardware is purchased. This can be done one at a time or as a mass hardware migration including many user machines.

This chapter includes the following topics:

- “Reassign a CVD to a Different Device,” on page 117
- “Perform a Mass Hardware Migration,” on page 119

Reassign a CVD to a Different Device

You can reassign a CVD to a different device.

In this procedure, you select one of the following restore options for the selected CVD and device:

**Table 17-1. Restore a CVD to a Replacement Device - Wizard Restore Options**

<table>
<thead>
<tr>
<th>Restore Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full System Restore, including OS, Applications, User Data and Settings</td>
<td>Use this option for systems with Windows volume licenses or Windows OEM SLP licenses. The entire CVD is restored to the replacement device, including OS, applications, and user files. Any existing files on the replacement device are lost or overwritten.</td>
</tr>
<tr>
<td>Restore Applications, User Data and Settings</td>
<td>Use this option when replacing a device that has a different Windows OEM license. The OS of the replacement device must be the same as that of the CVD. Only applications and user data are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.</td>
</tr>
<tr>
<td>Only Restore User Data and Settings</td>
<td>Use this option to migrate users from Windows XP/Vista/Windows 7 machines to new Windows 7 machines. The OS of the replacement device must be the same as or newer than that of the CVD. Only user data and settings are restored to the replacement device. The existing OS and applications installed on the replacement device are retained.</td>
</tr>
</tbody>
</table>

- User data in these options pertain to files and directories listed in the upload policies User area. See “Working with Upload Policies,” on page 18.

- If you migrate a CVD from a Windows XP or Vista device to a replacement device that has Windows 7, you can select only Full System Restore or Only Restore User Data and Settings. This is because Horizon Mirage does not transfer user-installed applications from a Windows XP/Vista to a Windows 7 system. Horizon Mirage cannot guarantee cross-OS compatibility.

When a CVD is migrated from Windows XP or Vista to Windows 7, Horizon Mirage streams down to the endpoint after the CVD has been migrated so that the end user can resume work without waiting for all of their user data to be downloaded first.
If a Windows 7 endpoint is selected to be restored to a Windows XP or Vista CVD, that Windows 7 endpoint becomes a Windows XP/Vista device.

**Prerequisites**

Install the Horizon Mirage client on the client machine as described in “Installing the Horizon Mirage Client,” on page 13.

Verify that the drive letters of the new endpoint and the CVD in the data center are compatible. If the drive letters are different, the system does not allow the restore operation to proceed.

Perform Sync Now on the endpoint before migrating it to a new client machine. This ensures that all data is saved to the data center before the migration takes place. See “Sync Now and Snooze,” on page 29.

The procedure enables you to select a domain for this endpoint to join after the restore operation. If you want to use the same credentials each time, perform the following:

1. In the Horizon Mirage Management console tree, right-click System Configuration and select Settings.
2. Select the General tab and then type the credentials you want to use for domain joining.
   The join domain account must meet the appropriate security privilege requirements. See “General System Settings,” on page 35.

**Procedure**

1. In the Horizon Mirage Management console, select Common Wizards > Hardware Migration.
2. Select the CVD you want to migrate and click Next.
3. Select the device where you want to migrate the CVD and click Next.
   Only devices compatible with the selected CVD are listed.
4. Select a restore option.
   a. Select a restore option for the selected CVD and device.
      You can maintain the current layer, if one applies, select a new base layer from the list, or proceed without a base layer.
   b. If you selected Full System Restore, select the base layer.
   c. Click Next.
5. (Optional) Specify CVD naming and domain options.
   a. Change or define the hostname for a device being restored.
   b. Select a domain for this endpoint to join after the restore operation. The current domain is shown by default.
      Type the OU and Domain or select them from the drop-down menus.
      The drop-down menus are populated with all known domains in the system. Each text box shows the required syntax pattern.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OU</td>
<td>Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com.</td>
</tr>
<tr>
<td>Join Domain account</td>
<td>The join domain account must meet the appropriate security privilege requirements as defined in the system general settings. The account must have access to join the domain. This is not validated.</td>
</tr>
</tbody>
</table>

   c. Click Next.
6 Use the validation summary to compare the target device with the CVD. This summary alerts you to any potential problems that require additional attention.

You cannot proceed until blocking problems are resolved.

7 Click **Next** and click **Finish**.

The migration process proceeds and takes place in two phases. See “End User Experience with Restore Processes,” on page 115.

### Perform a Mass Hardware Migration

You can migrate a mass of old user machines, for example, in the thousands, to new hardware models. The OS version is not changed in this process.

You use a CSV-based input file that defines the set of transitions needed, including source machine, destination machine, and parameters. This is performed using Horizon Mirage command line tools.

<table>
<thead>
<tr>
<th>Table 17-2. CSV File Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
</tr>
<tr>
<td>Source CVD name</td>
</tr>
<tr>
<td>New CVD name</td>
</tr>
<tr>
<td>Target device name</td>
</tr>
<tr>
<td>Optional note per machine</td>
</tr>
<tr>
<td>Identifier</td>
</tr>
<tr>
<td>Credentials for the domain join account</td>
</tr>
<tr>
<td>Server address</td>
</tr>
</tbody>
</table>

**Procedure**

1 Centralize the source machines to the Horizon Mirage server.

2 Assign these CVDs to a specific collection.

3 Connect the new machines to the network with an initial Windows system and deploy the Horizon Mirage client to them. You can use mass deployment tools to deploy the client. There are several ways to do this:

   - Use the Horizon Mirage bootable USB or LAN to deploy the initial image.
   - Deploy an image using third party solutions, for example, PXE or MDT.
   - Ask the hardware vendor to integrate the Horizon Mirage client in the Windows image deployed on the machines.

4 After the Horizon Mirage client is deployed, the new client machines appear in the **Inventory > Pending Devices** queue.

5 Create a CSV file mapping of source machine names to target machine names.

   The target machine names are the desired names of the machines after the migration. Existing names are not used as these are sometimes randomly generated by the hardware vendor.

   Optionally, you can import this mapping from XML.

6 Provide the Management console with a domain join account, with username and password.

   This account is used to rejoin the machines to the domain.
7 Select the pending devices to be used as target machines.
   The number of target and source machines must be the same.

8 Choose from the following base layer options:
   - Maintain the base layer from the source machines, which removes extraneous applications, such as OEM applications, from the target machines.
   - Apply a new base layer to the target machines to apply additional applications to the target devices.

The following migration processes take place:
   - For each source CVD, an available pending device is selected.
   - The source CVD is assigned to the selected pending target device, along with the base layer for the target model, if any.
   - The migration operation starts, including automatic boots whenever necessary.
   - The migration task is marked as done only when an upload was completed.

**What to do next**

After the process is completed, the previous CVDs are migrated to the new machines.
You can perform migrations of existing Windows XP or Vista endpoints to Windows 7. The migrations can be either in-place, on the same devices, or to replacement devices.

The migration procedure involves first setting up the Windows base layer for migration, then performing the migration either in-place to the same devices, or to replacement devices, then applying Windows 7 post-migration scripts.

The migration installs a Windows 7 base layer on each target endpoint, while preserving user profile data and settings through the Microsoft User State Migration Tool (USMT v4.0).

Unlike base layer updates, the migration process installs a complete OS image, including local user profiles as configured on the reference machine when the base layer was captured. You can use this to set up a local administrator and default user account.

The migration moves existing content of a target endpoint to the C:\Windows.Old directory, which is then processed by USMT. Application settings and data that are not handled by USMT are kept in the C:\Windows.Old directory. You can manually restore this data, or delete it when not needed anymore.

Windows 7 migration with Horizon Mirage retains the original computer name but requires rejoining the domain to create a Windows 7 machine account. You define this account in the Horizon Mirage system configuration. See “General System Settings,” on page 35.

Custom boot loaders on the target machine are removed by the migration. If an endpoint includes multiple OSs, the migration overwrites only the one on the active OS Partition and does not provide boot options for the others. You can manually restore other boot options after booting to Windows 7.

**Prerequisites**

- You must be an advanced administrator and familiar with system operations and the functional behavior of Horizon Mirage to proceed with this operation.
- The base layer must include the Boot Configuration Data (BCD) and the required Boot Loader files. These must be on the OS Partition and not on a separate boot partition.
- If you are performing a migration in a small or remote office use the Horizon Mirage branch reflector feature to reduce the bandwidth used during a migration. In particular, a Windows 7 test machine configured as a branch reflector can share its OS files with client endpoints to assist in the migration process. See Chapter 8, “Using Branch Reflectors,” on page 53.
- Applications need to be installed in the base layer in order to be provided upon migration. USMT does not migrate any applications that were installed on XP or Vista to Windows 7.
- Make sure to remove any sensitive data from the reference machine. All user data on the reference machine is applied to the target as part of the migration process.
Windows 7 Migration End User Experience

After the migration base layer download is completed, the system requests a reboot. A swap is made and Windows 7 boots.

Login is disabled until the system completes the migration process. Windows 7 is loaded and Plug-and-Play hardware is installed and configured. This process might take a few minutes, during which the computer is fairly busy.

You can monitor the progress in the Windows login screen. When the process is completed, the system restarts the PC and login is then possible.

The post-migration script runs the USMT and then rejoins the domain. This requires the PC to be connected to the corporate network to be assigned a network address.

**Note** To rejoin the domain, the PC must have network access to the domain controller. End users cannot login using their domain credentials until the domain join is complete.

This chapter includes the following topics:

- “Set up the Windows 7 Base Layer for Migration,” on page 122
- “Performing a Windows 7 In-Place Migration,” on page 123
- “Migrate to Windows 7 Replacement Devices,” on page 126
- “Monitor the Windows 7 Migration,” on page 127
- “Applying Windows 7 Post-Migration Scripts,” on page 127

Set up the Windows 7 Base Layer for Migration

Before you can perform a Windows 7 migration, a setup must be performed to prepare the image so it can be deployed during the migration. Setting up a base layer for migration is similar to setting up a base layer for standard Horizon Mirage operation.

**Prerequisites**

- Verify that all endpoint devices using third-party Full-Disk-Encryption are decrypted before proceeding with an in-place Windows 7 migration. Disk encryption software might interfere with migrations if endpoints are not decrypted first.
- Verify that the USMT 4 package is configured on your Horizon Mirage server. See “Import USMT Settings,” on page 37.

**Procedure**

- Right-click the Horizon Mirage icon in the notification area of the reference machine and select Tools > Windows 7 Image Setup.

The Horizon Mirage client runs a number of actions to prepare the image so it can be deployed during the Windows 7 migration.

**What to do next**

You can now continue to perform the Windows 7 migration. See “Performing a Windows 7 In-Place Migration,” on page 123 or “Migrate to Windows 7 Replacement Devices,” on page 126
Performing a Windows 7 In-Place Migration

You can perform an in-place migration of existing Windows XP or Vista endpoints to Windows 7 on the same equipment.

The migration process first downloads the Windows 7 image to the endpoints and then applies the image. You can perform the Windows 7 in-place migration in two ways:

You can download and apply the Windows base layer in one step. The Windows 7 image is migrated to the endpoints after all the CVDs in the task have finished downloading.

Alternatively, you can download first and apply to selected or all CVDs at a later time. This gives control over when the new Windows 7 is applied to specific endpoints. Since the download time might vary by endpoint, you might find it convenient to migrate certain endpoints that have finished downloading in advance of the others.

In both cases, you start with a basic procedure, where you choose whether to apply CVDs right way, or just download and apply them later. See “Basic Windows 7 In-Place Migration Procedure,” on page 123.

If you choose to only download CVD, after the basic procedure is finished, you complete the migration procedure by performing the steps described in “Download First and Apply in Stages,” on page 125.

To perform a migration to different hardware, see “Migrate to Windows 7 Replacement Devices,” on page 126.

Basic Windows 7 In-Place Migration Procedure

In the basic migration procedure, you can choose to download and apply the Windows base layer in one step, where Windows 7 image is migrated to the endpoints after all the CVDs in the task have finished downloading. Alternatively, for more control, you can choose to download first and apply to selected or all CVDs at a later time.

Prerequisites

A setup must be performed to prepare the base layer so it can be deployed during the migration. See “Set up the Windows 7 Base Layer for Migration,” on page 122.

The procedure enables you to select a domain for this endpoint to join after the restore operation. If you want to use the same credentials each time, perform the following:

1. In the Horizon Mirage Management console tree, right-click System Configuration and select Settings.
2. Select the General tab and then type the credentials you want to use for domain joining.

The join domain account must meet the appropriate security privilege requirements. See “General System Settings,” on page 35.

Procedure

1. In the Horizon Mirage Management console tree, select Common Wizards > Windows 7 Migration.
2. Choose the CVDs you want to update and click Select and click Next.

You can either choose individual or multiple CVDs, or a collection from the Collections tab.
3 Select migration option and Windows 7 base layer image for the migration.

   a  Select **Download and Apply Base Layer** or **Only Download Base layer**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Download and Apply Base Layer</strong></td>
<td>This performs the migration in one step. The Windows 7 image is automatically migrated to the endpoints after all the CVDs in the task have finished downloading.</td>
</tr>
<tr>
<td><strong>Only Download Base Layer</strong></td>
<td>This performs only the Download stage, allowing you to selectively migrate CVDs that have completed downloading as a separate operation. In this case, after the Wizard procedure is finished, you can start to migrate certain endpoints that finished downloading.</td>
</tr>
</tbody>
</table>

b  Select the Windows 7 base layer image for migration.

c  Click **Next**.

4 Select the XP or Vista CVDs or collections of CVDs to migrate to Windows 7 and click **Select** to copy them to the Selected CVDs area, and click **Next**.

   The window shows all the CVDs that are eligible for download or migration.

5 Select one or more available app layers that you want to assign to the endpoint, move them to the Assigned layers list and click **Next**.

   **NOTE**  When performing Windows 7 migration with app layers, Horizon Mirage is only able to deliver driver packages as part of the Mirage driver library mechanism. In this scenario, Horizon Mirage will not deploy driver packages which were recorded as part of the app layers.

6 (Optional) Specify CVD naming and domain options.

   a  Change or define the hostname for a device being restored.

   b  Select a domain for this endpoint to join after the restore operation. The current domain is shown by default.

      Type the OU and Domain or select them from the drop-down menus.

      The drop-down menus are populated with all known domains in the system. Each text box shows the required syntax pattern.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OU</strong></td>
<td>Verify that the OU is in standard open LDAP format. For example, OU=Notebooks, OU=Hardware, DC=VMware, DC=com.</td>
</tr>
<tr>
<td><strong>Join Domain account</strong></td>
<td>The join domain account must meet the appropriate security privilege requirements as defined in the system general settings. The account must have access to join the domain. This is not validated.</td>
</tr>
</tbody>
</table>

   c  Click **Next**.

7 Use the validation page to resolve any compatibility problems between the base layer and selected CVDs.

   You cannot proceed until blocking problems are resolved.

8 Click **Next** and **Finish**.

   After the operation is completed, one task is created which contains all the CVDs that you selected.
What to do next

If you chose **Download and Apply Base Layer**, the migration proceeds and you can now monitor the migration progress. See “Monitor the Windows 7 Migration,” on page 127.

If you chose **Only Download Base Layer**, after the basic procedure is finished, you can start to migrate certain endpoints that finished downloading. See “Download First and Apply in Stages,” on page 125.

**Download First and Apply in Stages**

If you completed the basic Windows 7 in-place migration procedure using the **Only Download Base Layer** option, you can now apply the base layer to CVDs that have downloaded.

The basic migration operation that you ran with the **Only Download Base Layer** option created a Migration Download task containing the CVDs you selected. At the end of that operation, the Windows 7 image download to individual endpoints is either ongoing or completed. See “Basic Windows 7 In-Place Migration Procedure,” on page 123, but applying the CVDs is not started.

You now need to start applying the image to the endpoints.

In that process, you can choose to apply all the CVDs that have finished downloading, or you can select specific CVDs to apply first. You can then apply the remaining CVDs in additional cycles.

If not all the CVDs in the task, or in your selection of CVDs, are finished downloading, you can additionally choose to wait until they have all finished downloading, or apply the ones that have finished so far. You can then apply the remaining CVDs in additional cycles as they finish downloading.

**Procedure**

1. In the Horizon Mirage Management console tree, select **Task Monitoring**.
2. If you want to download all the CVDs in the task:
   a. Right-click the **Migration Download** task and select **Start Migration**.
   b. If downloads were not completed on at least one of the CVDs in the task, select:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Apply migration to the CVDs that have finished downloading so far. The not-yet-downloaded CVDs continue to download and are left in the Migration Download task.</td>
</tr>
<tr>
<td>No</td>
<td>Wait for the downloading to finish on all CVDs in the task and apply migration automatically to all the CVDs at that time.</td>
</tr>
</tbody>
</table>

The migration starts on the eligible CVDs according to the selected option.

   c. Continue to step 4.
3. If you want to make a selection of the CVDs to download within the task:
   a. Right-click the **Migration Download** task and select **View Assignments**.
   b. Select **Image Composer Layer Assignments** to view the CVDs in the task.
c Select the CVDs that you want to migrate, right-click, and select **Start Migration**.

The Status panel shows how many CVDs were downloaded. Multiple statuses are shown while downloading is in progress.

d If downloads were not completed on at least one of the selected CVDs, a warning appears concerning these assignments. Select:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Apply migration to the selected CVDs that have finished downloading so far. The not-yet-downloaded CVDs continue to download and are left in the Migration Download task.</td>
</tr>
<tr>
<td>No</td>
<td>Wait for the downloading to finish on all the selected CVDs and apply migration automatically on all the CVDs at that time.</td>
</tr>
</tbody>
</table>

The migration starts on the eligible CVDs according to the selected option.

4 You can repeat the procedure as more CVDs complete downloading.

The migration operation starts on the eligible CVDs, according to the option you selected.

**What to do next**

You can monitor the progress of the migration. See “Monitor the Windows 7 Migration,” on page 127.

You can repeat the procedure as more CVDs complete downloading.

**Migrate to Windows 7 Replacement Devices**

You can migrate end users from Windows XP, Vista or Windows 7 machines to new Windows 7 machines. This is relevant for smaller customers that use Windows OEM SLP licenses, and supports both disaster recovery and hardware refresh scenarios.

You can use this operation for the following operating systems:

- Windows XP 32-bit to Windows 7 32-bit or 64-bit
- Windows 7 32-bit to Windows 7 32-bit or 64-bit
- Windows 7 64-bit to Windows 7 64-bit
- Windows Vista 32-bit to Windows 7 32-bit or 64-bit
- Windows Vista 64-bit to Windows 7 64-bit

Migration to a different device requires restoring only user data and settings. For this purpose, use the procedure in “Restore a CVD to a Replacement Device,” on page 109. In the **Restore Options**, select **Only Restore User Data and Settings**.

**Note** In-place migration for Windows 7 described in Chapter 18, “Windows 7 Migration,” on page 121 is not suitable for migration to replacement devices.

**Prerequisites**

A setup must be performed to prepare the base layer so it can be deployed during the migration. See “Set up the Windows 7 Base Layer for Migration,” on page 122.
Monitor the Windows 7 Migration

You can monitor the detailed progress of all the CVDs in the migration by viewing the task progress.

**Procedure**

1. In the Horizon Mirage Management console tree, select **Task Monitoring**.
2. Right-click the required task and select **View Assignments**.
3. Select **Image Composer > Layer Assignments** to view the CVDs in the task.

   The Status panel shows how many CVDs were downloaded. Multiple statuses are shown while downloading is in progress.

Applying Windows 7 Post-Migration Scripts

You can create a custom post-migration script to perform certain actions after the migration update, such as install software or add or remove drivers.

A custom post-migration script is required in cases such as:

- Install software requiring execution on the individual endpoint. This can include hardware-specific software that is compatible only with certain endpoints.
- Update or remove hardware drivers that might already exist on the endpoint.

This file and any auxiliary files used or called by the script are captured as part of the base layer and distributed to the various endpoints. It is important to verify that the auxiliary files are placed in the same directory as the script or another directory that is captured in the base layer.

**Procedure**

Create a file called `post_migration.bat` under the `%ProgramData%\Wanova\Mirage Service` directory.

   The file must be edited on the reference machine.

**Note** The Horizon Mirage client installation includes a default sample script that does not perform any post-migration script actions.

The Horizon Mirage client monitors the post-migration script execution and reports events to the Horizon Mirage central management service if the script returns an error value other than zero.
The system dashboard assists you to monitor the system status and operations. The transaction log lets you monitor the progress of updates coming from and to the Horizon Mirage server.

This chapter includes the following topics:
- "Using the System Dashboard," on page 129
- "Using Transaction Logs," on page 131

Using the System Dashboard

The system dashboard provides at-a-glance monitoring of system component status and operations, such as statistics about system activities, alerts, and indications of actions the administrator must carry out, as well as centralization and backup processes. It also assists the Protection Manager role to ensure that user devices are protected.

Most dashboard information is refreshed automatically every three minutes. You can also refresh key information indicators, such as system status, server status, and capacity use, by pressing F5.

System Status

The System Status area shows the number of unacknowledged events by severity (Critical, Warning, or Info) and source (Server or Clients).

System events are propagated from clients, the server, and the management service on the server. Warning and Info events provide advice or instructions that do not require urgent attention. You can click an event button to open the Event log view filtered according to the selected severity and source.

Servers

The Server area shows the Up or Down status of Horizon Mirage servers. The icon also reflects the server status.

Capacity Status

The Capacity Status area shows the number of devices according to the following statuses:
Table 19-1. Device Statuses

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>Number of devices pending restore or activation, irrespective of their connection status.</td>
</tr>
<tr>
<td>Online</td>
<td>Number of activated devices that are online, excluding online devices pending restore.</td>
</tr>
<tr>
<td>Offline</td>
<td>Number of activated devices that are offline, excluding offline devices pending restore.</td>
</tr>
</tbody>
</table>

You can click the Pending label or counter to link to the Pending Devices window where you can view the pending devices and apply relevant actions.

An exclamation mark icon indicates license depletion. This occurs if the total number of pending plus online devices is greater than the licensed capacity.

Update Progress

The Update Progress area histogram shows the number of clients currently downloading updates or involved in restore activities, for example, following base layer assignment, enforcement, or update, and CVD restore. The information is presented in percentage progress ranges, from just started (0-20%) to almost completed (80-100%).

Totals of desktops finished downloading or currently downloading are also provided.

Table 19-2. Totals of Desktops Finished Downloading or Currently Downloading

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Ready</td>
<td>Number of desktops that have finished downloading (reached 100%), or that have no pending download.</td>
</tr>
<tr>
<td>Total in Progress</td>
<td>Total number of desktops that are currently downloading or have an incomplete download pending network reconnection.</td>
</tr>
</tbody>
</table>

Data Protection

The Data Protection meter indicates the total protection level of the desktop deployment.

The gauge shows the ratio of total desktop content stored and protected at the server versus total desktop data at the endpoint in the process of synchronization. The gauge reflects information provided by online devices. Offline devices report the next time they connect.

Core Image Compliance

The Core Image Compliance meter indicates the total compliance level of your endpoints.

The gauge represents the percentage compliance of managed endpoints with their IT-approved base layer. Based on this information, you can enforce the base layer for one or many endpoints to bring them back into compliance and decrease the likelihood of end user problems.

Efficiency Benchmarks

The Efficiency Benchmarks area shows the actual traffic between the desktops and the server over the last 24 hours as a histogram.

Table 19-3. Efficiency Benchmark Histograms

<table>
<thead>
<tr>
<th>Histogram</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Usage (In)</td>
<td>Shows upload traffic from desktops to server.</td>
</tr>
<tr>
<td>Network Usage (Out)</td>
<td>Shows the download traffic from server to desktops.</td>
</tr>
</tbody>
</table>
Each bar shows the total data for one hour. The bar representing the current hour shows total traffic from the start of the hour to the last dashboard refresh time.

### Table 19-4. Information Provided in Each Histogram

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y axis</td>
<td>Data size in bytes, KB, MB, or GB, according to the maximum data transferred in the 24-hour span.</td>
</tr>
<tr>
<td>X axis</td>
<td>Time in hours, where each bar represents one hour.</td>
</tr>
<tr>
<td>Total</td>
<td>Total traffic in the last 24 hours.</td>
</tr>
<tr>
<td>Average</td>
<td>Hourly traffic average in the last 24 hours.</td>
</tr>
<tr>
<td>Peak</td>
<td>Hourly traffic peak in the last 24 hours.</td>
</tr>
</tbody>
</table>

### Using Transaction Logs

A transaction is a logical operation between the Horizon Mirage server and the client. You can use the transaction log to monitor the progress of updates coming from and to the server.

Each transaction is built from a collection of sub-transactions, each representing a network session between the client and server. Sub-transactions are reported only when a session is either complete (succeeded) or terminated (failed due to a network disconnect or other specified reason).

### Table 19-5. Transaction Types in the Transaction Log

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralize Endpoint</td>
<td>First time upload of the end user machine to the server.</td>
</tr>
<tr>
<td>Upload Incremental Changes</td>
<td>Synchronizing ongoing changes from the end user machine to the server.</td>
</tr>
<tr>
<td>Update Base Layer</td>
<td>End user machine is updated with the assigned base layer.</td>
</tr>
<tr>
<td>Update App Layer</td>
<td>End user machine is updated with the assigned app layer.</td>
</tr>
<tr>
<td>Base Layer Caching</td>
<td>The branch reflector downloads a base layer.</td>
</tr>
<tr>
<td>Base Layer Verification</td>
<td>Base layer download is verified prior to being applied.</td>
</tr>
<tr>
<td>Restore Prefetch</td>
<td>Client downloads the minimum file set required from the CVD to allow the endpoint to boot the restored CVD and allow network access to complete restore through background streaming.</td>
</tr>
<tr>
<td>Restore Streaming</td>
<td>Client streams the remainder of the restored CVD to the endpoint while the user works normally online.</td>
</tr>
</tbody>
</table>

**Note** More than one sub-transaction appears when one or more attempts to complete the parent transaction failed. The sub-transaction status reported is final and does not change.

### Transaction Entry Properties

### Table 19-6. Transaction Log Information for Each Entry

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVD</td>
<td>Number of the CVD</td>
</tr>
<tr>
<td>CVD Name</td>
<td>Name of the CVD</td>
</tr>
<tr>
<td>Type</td>
<td>Type of operation being performed, such as Centralize Endpoint or Upload Incremental Changes</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the transaction, for example Success.</td>
</tr>
<tr>
<td>Layer</td>
<td>Base Layer ID and version, if applicable</td>
</tr>
</tbody>
</table>
Table 19-6. Transaction Log Information for Each Entry (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changed Files</td>
<td>Total number of changed files</td>
</tr>
<tr>
<td>Unique Files</td>
<td>Total number of files to be transferred, after duplicate files are eliminated</td>
</tr>
<tr>
<td>Size (MB)</td>
<td>Total Data size of the files to be transferred, after duplicate files are</td>
</tr>
<tr>
<td></td>
<td>eliminated</td>
</tr>
<tr>
<td>Size After File Dedup (MB)</td>
<td>Data Size After Dedup, meaning the total size of file and metadata to be</td>
</tr>
<tr>
<td></td>
<td>transferred after it is reduced by intra-file and inter-file block level</td>
</tr>
<tr>
<td></td>
<td>deduplication, but before LZ compression</td>
</tr>
<tr>
<td>Size After Block Dedup (MB)</td>
<td>Before Compression size, which is the total network transfer as seen over</td>
</tr>
<tr>
<td></td>
<td>WAN, before applying LZ compression</td>
</tr>
<tr>
<td>Data Transferred (MB)</td>
<td>The total network transfer that took place.</td>
</tr>
<tr>
<td>Branch Reflector Transfer (MB)</td>
<td>The amount of data that was sent from the branch reflector to the endpoint</td>
</tr>
<tr>
<td></td>
<td>(instead of from the Horizon Mirage server directly to clients).</td>
</tr>
<tr>
<td>Savings</td>
<td>Transfer Savings, meaning the ratio of the total size of the changed files</td>
</tr>
<tr>
<td></td>
<td>and actual transfer size</td>
</tr>
<tr>
<td>Start Time</td>
<td>Start time of the transaction</td>
</tr>
<tr>
<td>End Time</td>
<td>End time of the transaction</td>
</tr>
<tr>
<td>Duration</td>
<td>Duration of the transaction</td>
</tr>
</tbody>
</table>

Search and Filter Results Specification

Whenever a search or filter query is initiated in any list window, the first page of results appears in the view area. The number of pages of qualifying records appears under the Search text box and you can scroll to the next or previous page by clicking arrow icons. For improved query response time, when the number of records retrieved is very large, the associated page count is not calculated and is replaced by three dots (...).

Total Transaction Record Limits

The system implements transaction record limits to prevent log files from becoming too large:

Table 19-7. Transaction Record Limit by Record type

<table>
<thead>
<tr>
<th>Transaction Record Type</th>
<th>Cleaned up after:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steady State (SS) transactions</td>
<td>30 days</td>
</tr>
<tr>
<td>Layer transactions</td>
<td>180 days</td>
</tr>
<tr>
<td>All other transactions</td>
<td>365 days</td>
</tr>
</tbody>
</table>
You can generate and view a variety of reports on-demand.

You can request the following reports:

**Table 20-1. Reports that can be Requested**

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage Usage Report</td>
<td>Describes storage use on the selected volume or volumes.</td>
</tr>
<tr>
<td></td>
<td>To run the report, select the report in the Reports node, click Generate Report, select volumes, and click OK.</td>
</tr>
<tr>
<td></td>
<td>To view the report, select the report line and click the View Report icon on the report list toolbar.</td>
</tr>
<tr>
<td>Base Layer Dry-Run Reports</td>
<td>Compare the content of the base layer and the CVD.</td>
</tr>
<tr>
<td></td>
<td>■ Application-level report: Describes projected applications that are added to, updated in, or deleted from an endpoint device when the selected base layer is downloaded.</td>
</tr>
<tr>
<td></td>
<td>■ Program Executable (PE) level report: Analyzes the outcome of removing or updating a PE file.</td>
</tr>
<tr>
<td></td>
<td>For more information about these reports, see “Layer Dry Run Reports,” on page 134.</td>
</tr>
<tr>
<td>Device Hardware Report</td>
<td>Provides a CSV file inventory of all devices, showing information such as chassis type, CPU, printing system, hardware components and associated vendor details.</td>
</tr>
<tr>
<td></td>
<td>To run the report, select the report in the Reports node, click Generate Report, select devices, and click OK.</td>
</tr>
<tr>
<td></td>
<td>To view the report, select the report line and click the View Report icon on the report list toolbar.</td>
</tr>
<tr>
<td>CVD Integrity Report</td>
<td>Verifies that a CVD is consistent and free of corruption and can continue to reside in the system and be used for restore and other purposes.</td>
</tr>
<tr>
<td></td>
<td>For more information about this report, see “CVD Integrity Report,” on page 135.</td>
</tr>
</tbody>
</table>

This chapter includes the following topics:

- “Layer Dry Run Reports,” on page 134
- “CVD Integrity Report,” on page 135
Layer Dry Run Reports

You can run a Layer Dry Run report to compare the content of the layers and the CVD before applying a layer update to a CVD or collection of CVDs. This report provides a method to detect unforeseen effects, and resolves conflicts that might result from any mismatch between the CVD and the layers content.

Table 20-2. Types of Conflict Described in the Report

<table>
<thead>
<tr>
<th>Conflict Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Layer Application Downgrades a user installed application</td>
<td>An application installed in the base layer uses an older version of shared components than another user installed application uses.</td>
</tr>
<tr>
<td>Base Layer Application Downgrades OS component</td>
<td>An application installed in the base layer downgrades OS components.</td>
</tr>
<tr>
<td>Base Layer OS Components downgrades user installed application</td>
<td>OS components in the base layer downgrades shared components that are used by a user installed application.</td>
</tr>
</tbody>
</table>

You can generate this report in two ways:

Table 20-3. Types of Layer Dry Run Report

<table>
<thead>
<tr>
<th>Report Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-level report</td>
<td>Describes projected applications that are added to, updated in, or deleted from to an endpoint device when the selected layer changes are applied. It compares the applications installed on the layers and the CVD and provides a general view of the result for the change in layers. For more information, see 16.2 Comparison Report between Base Layer and CVD.</td>
</tr>
<tr>
<td>Program Executable (PE) level report</td>
<td>Analyzes the outcome of removing or updating a PE file. It projects affected software modules, such as .DLL files, when a base layer is downloaded to an endpoint device client, and details whether each affected module is downgraded.</td>
</tr>
</tbody>
</table>

**Note** Depending on the number of CVDs selected, running the report might take some time.

**Procedure**

1. In the Horizon Mirage Management console tree, under the Reports tree, click the report type that you want to generate or view.

2. To generate a dry run report:
   a. Click the Generate Report icon on the report toolbar.
   b. Type a report name in the Report Name text box.
   c. Select a CVD and click Select, and click Next.
      To deselect a CVD, click Remove. To deselect all CVDs, click Clear.
   d. Select a base layer option.
      Select No change to target base layer, or Select Base layer from list and select a base layer, and click Next.
   e. Select app layers to be included in the report.
   f. Click Finish.

The report is generated. You can view the report when the status is Done.
3 To view a report that was generated:

   - Click the View Report icon on the report list toolbar.
   
   The report appears as an HTML page.

4 To delete a report:

   a On the report list, select the report you want to delete.
   
   b Click the Delete icon on the report console toolbar.

CVD Integrity Report

You generate the CVD Integrity report if a system event warns that a CVD might have inconsistencies.

The CVD Integrity report verifies that a CVD is consistent and free of corruption, and can continue to reside in the system and be used for restore and other purposes.

**IMPORTANT** Consider your privacy and regulatory requirements before sending support data to VMware. Log files, system reports and support data generated in order to obtain support from VMware may contain sensitive, confidential or personal information, including file and folder names and information about installed programs and user settings.

**Procedure**

1 In the Horizon Mirage Management console tree, expand the Reports node and select the CVD Integrity report.

2 To generate a report:

   a Click the Generate Report icon on the report toolbar.
   
   b Type a report name in the Report Name text box. If none is given, the default name format is applied (CVD_Integrity_{User's environment name}_{Short date}).
   
   c Select a CVD in the CVD List area, and click Next.
   
   d Select a report option:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Only</td>
<td>Generates only the CVD Integrity report, which checks for errors on the selected CVD. No repair actions are performed.</td>
</tr>
<tr>
<td>Fix For Upload</td>
<td>Use this report option if you were performing a non-restore process (for example, periodic upload) when you encountered a problem with the CVD. Corrupted files are re-uploaded so that the interrupted process can resume.</td>
</tr>
<tr>
<td>Fix For Restore</td>
<td>Use this report option if you were performing a restore process when you encountered a problem with the CVD. Corrupted files are repaired so that the interrupted process can resume.</td>
</tr>
</tbody>
</table>

   e Click Next and click Finish.

3 To view a report that was generated:

   - Click the View Report icon on the report list toolbar.
   
   The report appears as an HTML page.

4 To delete a report:

   a On the report list, select the report you want to delete.
   
   b Click the Delete icon on the report console toolbar.
You can perform maintenance operations on Horizon Mirage servers and the Management server, including backup, restore, and upgrade from previous Horizon Mirage versions.

This chapter includes the following topics:

- “Server and Management Server Operations,” on page 137
- “Upgrading from Previous Horizon Mirage Versions,” on page 139

### Server and Management Server Operations

You can perform maintenance operations on Horizon Mirage servers and the Management server, including backup and restore.

#### Back up a Server or the Management Server

You can back up a Horizon Mirage server or the Management server. Server state backup involves the backup of all storage volumes and the database.

**IMPORTANT** Configure your server backup software to stop the Horizon Mirage server cluster and the Management server during the snapshot and database backup time. Back up the SIS and the database using a point-in-time representation so that the backup is consistent across all the volumes and the database.

Contact VMware Support for assistance with this procedure.

**Prerequisites**

Copy the Horizon Mirage storage volumes to the backup location, preferably through a snapshot mechanism, and also back up the database.

If storage snapshots are not used, verify that the Horizon Mirage servers and the Management server are stopped for the full duration of the backup.

#### Restore the Horizon Mirage Management Server

You can restore the Horizon Mirage Management server, without reference to Horizon Mirage servers.

When the Management server needs to be restored, you need to reinstall only the Management server. For detailed instructions on installing a Management server, see Install the Horizon Mirage Management Server in the Horizon Mirage Installation Guide.
Use the same fully-qualified name of the original Management server so that existing Horizon Mirage servers can locate the Management server and connect to it.

**IMPORTANT** Restore all Horizon Mirage storage volumes and the database at the same time, even if only a single volume or only the Horizon Mirage database needs to be restored.

**Procedure**

1. Restore the complete server system from a full disk image.
2. Start the server in Windows Safe Mode.
3. Set the VMware Server Service and VMware Management Service start type to Disabled.
4. Start the server normally.
5. Run the following commands: `Wanova.Server.Tools.exe ResetPendingBI`
6. Set the VMware Server Service and VMware Management Service start type to **Automatic**.
7. Start the VMware server service and VMware management service.

**Restore a Horizon Mirage Server**

You can restore a Horizon Mirage server, without reference to the Horizon Mirage Management server.

- When only a single server needs to be restored and no Horizon Mirage storage or database is installed on this machine, you need to reinstall only the server and point it to the Management server.
- If the Management server was installed on the same machine, you need to reinstall the Management server before reinstalling the server.

For more information about installing the Horizon Mirage server and Management server, see [Install the Server](#) and Install the Horizon Mirage Management Server in the [Horizon Mirage Installation Guide](#).

**Restore Horizon Mirage Storage Volumes and Database**

You can restore the Horizon Mirage storage volumes and database in a standalone or clustered environment, where the volumes and database are not co-hosted on the same server as the Horizon Mirage Management server.

**Prerequisites**

- You must obtain the `Server.Tools.zip` package prior to installing the Horizon Mirage server. For information about obtaining the package, contact VMware Support.

**Procedure**

1. Verify that all servers and the Management server are stopped.
2. Restore all the storage volumes and the database from backup.
   - Make sure to restore to original UNC paths.
4. Start the Management server and all servers.

**What to do next**

If the UNC path was changed on any of the volumes, you must change the UNC path in the Edit Volume dialog box and mount the volume. See “Edit Storage Volume Information,” on page 49.
Restore a Standalone Server

Restoring a standalone Horizon Mirage server is suitable for small-scale, standalone server setups where the database, storage and Horizon Mirage services are all co-hosted on the same server.

The procedure restores the complete Horizon Mirage server system from backup, including OS image, server software, storage and database.

Procedure

1. Restore the complete server system from a full disk image.
2. Start the server in Windows Safe Mode.
3. Set the VMware Server Service and VMware Management Service start type to Disabled.
4. Start the server normally.
5. Run the following commands: `Wanova.Server.Tools.exe ResetPendingBI`
6. Set the VMware Server Service and VMware Management Service start type to **Automatic**.
7. Start the VMware server service and VMware management service.

Upgrading from Previous Horizon Mirage Versions

You can upgrade the Horizon Mirage system from earlier Horizon Mirage versions.

Uninstalling the Horizon Mirage servers does not remove data from storage volumes that were connected to the Horizon Mirage system.

Before You Start to Upgrade Horizon Mirage

Before you begin the upgrade process, you must perform certain pre-upgrade steps.

For more information about backing up the MS SQL database, see Using SQL Server Management Studio in the MSDN article Create a Full Database Backup (SQL Server), at http://msdn.microsoft.com/en-us/library/ms187510.aspx#SSMSProcedure

Select the database called `MirageDB`, and use the Full backup type. Note the location of the backup file.

Prerequisites

Verify that you have the following information available from the server `config` file.

- Database server name
- Credentials for the database server
- Horizon Mirage server cache directory location
- Cache size

Procedure

1. Stop Horizon Mirage services.
2. Back up the Horizon Mirage database.
   - Double-click the `C:\Program Files\Wanova\Mirage Management Server\sysreport_full.cmd` file to run a full sysreport in Horizon Mirage
   - Use SQL Server Management Studio.
3 Take snapshots of all Horizon Mirage storage volumes.
   Use image-based block backup, not file-based backup.
4 If you cannot make a snapshot, create and run a backup job for each volume's directory using any
   available backup program.
   This process can take a significant amount of time to complete. The backup software must support
   Alternate Data Streams (ADS). For best results, use block-based backup programs rather than file-level
   backup using ADS.

Upgrade Horizon Mirage

When you upgrade Horizon Mirage, uninstall the system components before installing the new version. It is
important to upgrade Horizon Mirage in a certain order.

Procedure
1 Select Control Panel > Add or Remove Programs to uninstall the system components.
   a Uninstall all Horizon Mirage servers.
   b Uninstall the Horizon Mirage Management console.
   c Uninstall the Horizon Mirage Management server.
   d Uninstall Horizon Mirage WebAccess.
2 Use the new mis files to install the latest version of Horizon Mirage.
   a Install the Horizon Mirage Management server.
   b Install the Horizon Mirage Management console.
   c Install the Horizon Mirage servers.
   d Install Horizon Mirage WebAccess.
Various troubleshooting mechanisms are available, including the CVD History view, Event and other system logs and reports.

This chapter includes the following topics:

- “CVD Events History Timeline,” on page 141
- “Using Event and Other System Logs,” on page 141
- “Customize the Minimal Restore set,” on page 142
- “Generate System Reports,” on page 143
- “Generate System Reports Remotely,” on page 144

CVD Events History Timeline

To help you troubleshoot problems in a CVD, the Management console consolidates all the events during a CVD’s life in a common timeline.

The following events are displayed in the CVD history view:

- Transaction log events
- Audit events
- Client system events

Procedure

1. Expand the Inventory node and select All CVDs.
2. Right-click the CVD name and select History.
3. Click Timeline.
4. You can copy and paste information from the CVD History view for use elsewhere by using the standard Windows key combinations Ctrl + C to copy, and Ctrl + V to paste.

Using Event and Other System Logs

The Horizon Mirage Management console provides a range of system logs, including the Event log, Transaction log, and the Manager Journal which records audit events.

The Horizon Mirage Management console includes the following logs:
### Table 22-1. Management Console Logs

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Log</td>
<td>Lists important system events as propagated from the server and clients.</td>
</tr>
<tr>
<td>Transaction Log</td>
<td>Records logical operations between the Horizon Mirage server and client. You can use the transaction log to monitor the progress of updates coming from and to the server. See “Using Transaction Logs,” on page 131.</td>
</tr>
<tr>
<td>Manager Journal</td>
<td>Collects and tracks audit event history. An audit event is created for any administrator action that results in a system setting or configuration change. This includes actions performed using the Management console or through a CLI. Read-only actions do not create audit events. Audit events provide the operation time, name, and details, and the user name.</td>
</tr>
</tbody>
</table>

---

### Customize the Minimal Restore set

You can customize the minimal set of files that must be restored to an endpoint so that it can reboot to the CVD and work online. The Minimal Restore set generally includes the organization VPN, antivirus, firewall applications, and driver store.

Minimal restore sets can be static or dynamic.

#### Table 22-2. Minimal Restore Set Types

<table>
<thead>
<tr>
<th>Minimal Restore Set Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Minimal Restore Set</td>
<td>A static list of files created by the administrator and placed in an XML file that is fetched during the restore operation. The files restored provide the endpoint with the minimum environment required to boot to a CVD. The static list is used for all endpoint devices in the system.</td>
</tr>
<tr>
<td>Dynamic Minimal Restore Set</td>
<td>This is a CVD-specific list of files that is acquired during normal CVD use. The list is built on each boot and captures the system, applications, and user files over a short time period after booting. A separate dynamic restore set is created for each CVD in the system and is used in conjunction with the static minimal restore set when a restore is performed.</td>
</tr>
</tbody>
</table>

The procedure describes how to customize the minimal set.

You can remove the minimal set using this procedure with the command `removeMinimalSet`. When this command is run, the entire CVD content is downloaded prior to the restore and online streaming is not used.

You can revert to the original (default) VMware minimal set. The file is located at: C:\Program Files\Wanova\Mirage Server\MinimalSet.xml.

You can used the same file as basis for further customization, such as adding the corporate antivirus and VPN files.

**IMPORTANT** The procedure describes how to modify critical Horizon Mirage configurations using the CLI. Follow these steps carefully, as serious problems can occur if the CLI is used incorrectly.

### Prerequisites

You must be authenticated as a member of a group with access to the VMware Management console. See “Managing Role-Based Access Control and Active Directory Groups,” on page 148.

### Procedure

1. On the Start menu, click Run, type `cmd`, and click OK.
2 In the Command window, type: `cd Mirage Server program files path\`
   For example, `C:\Program Files\Wanova\Mirage Server` and then press Enter.
   The VMware server management console starts running.
4 To export the minimal restore set, type: `getminimalset path to output file`.
5 Edit the file using an XML editor.
6 Add the modified file to the minimal set, using the following command: `addMinimalSet path to XML file`
7 Press Enter.

   **NOTE** Executing this command overrides any existing static minimal set.

   A message appears confirming that the Static Minimal Set was added successfully.
8 To view the minimal set type `printMinimalSet` and press Enter.
9 Type `Exit` and press Enter to exit the Command window.

### Generate System Reports

You can use the System Report Utility to collect internal system log files, relevant registry entries, event logs, and system information and configuration, to help VMware Support and IT with troubleshooting.

**NOTE** This command can be CPU-intensive, especially on the server, so an intermediate impact is generally expected.

You can generate the following system report types:

**Table 22-3. Available Report Types**

<table>
<thead>
<tr>
<th>Report</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full report</td>
<td>Collects the most comprehensive set of system logs, registry and system information. While helpful in troubleshooting confirmed problems, this report can be very large (containing several hundreds of MB of data), and is used only by special request from VMware Support.</td>
</tr>
<tr>
<td>Medium report</td>
<td>Used most frequently, this report type collects a limited set of system logs and system information. It is faster to generate and more resource efficient than the full report.</td>
</tr>
<tr>
<td>Logs only report</td>
<td>Returns a minimal set of log entries. Usually used in early troubleshooting stages to determine next steps.</td>
</tr>
</tbody>
</table>

**Prerequisites**

You must run the reports as an administrator.
Procedure

◆ Run the report.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From a server</td>
<td>Run the sysreport batch file from the Horizon Mirage install directory, for example: C:\Program Files\Wanova\Mirage Server, and use the required command line:</td>
</tr>
<tr>
<td></td>
<td>￭ Full Report: sysreport_full.cmd</td>
</tr>
<tr>
<td></td>
<td>￭ Medium report: sysreport_medium.cmd</td>
</tr>
<tr>
<td></td>
<td>￭ Logs Only report: sysreport_logs_only.cmd</td>
</tr>
<tr>
<td>From a client</td>
<td>Right-click the Horizon Mirage icon in the notifications area, and select Tools and select the report you want.</td>
</tr>
</tbody>
</table>

A CAB file containing all the logs is created. You can find it at: c:\sysreport-MMDDYYYY-HHMM-ComputerName.cab

Generate System Reports Remotely

You can save system reports from any device attached to the Horizon Mirage server.

The reports can be saved to a UNC path or sent to an FTP site.

**IMPORTANT** Consider your privacy and regulatory requirements before sending support data to VMware. Log files, system reports and support data generated in order to obtain support from VMware may contain sensitive, confidential or personal information, including file and folder names and information about installed programs and user settings.

Procedure

1. In the Horizon Mirage Management console tree, expand the Inventory node and select All CVDs.
2. Right-click the CVD for which you want to generate a report and select Device > Generate System Report.
3. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Includes all logs and collectable information from this endpoint.</td>
</tr>
<tr>
<td>Medium</td>
<td>Includes the logs and some additional information.</td>
</tr>
<tr>
<td>Logs</td>
<td>Generates a report of only the basic logs for this client.</td>
</tr>
</tbody>
</table>

4. Indicate either the UNC path or FTP Server details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNC</td>
<td>Select the Remote Share radio button and type the UNC path.</td>
</tr>
<tr>
<td>FTP</td>
<td>Select FTP server and type the server name, user name, and password.</td>
</tr>
</tbody>
</table>

5. Click OK.
Advanced topics serve to supplement information provided by main Horizon Mirage Administrator's Guide topics.

This chapter includes the following topics:

- “Horizon Mirage and SCCM,” on page 145
- “Setting Up the SSL Certificate in Windows Server,” on page 146
- “Using Microsoft Office 2010 in a Layer,” on page 148
- “Managing Role-Based Access Control and Active Directory Groups,” on page 148
- “Macros in Upload Policy Rules,” on page 150

Horizon Mirage and SCCM

When you capture a base layer for Windows 7 migration using Microsoft System Center Configuration Manager (SCCM), certain preparatory steps must be performed.

The reference machine must not be rebooted, and the ccmexec service must not be restarted during the time between performing the procedure and capturing the base layer.

Regular base layer updates do not require these steps, as this is already handled by Horizon Mirage.

Procedure

1. If SCCM client is not yet installed, manually install the client following the instructions at http://technet.microsoft.com/en-us/library/bb693546.aspx.
   
   Do not specify a SCCM site code for the client in the COSetup.exe command-line properties (SMSSITECODE parameter).

2. Stop the SMS Agent Host service (net stop ccmexec).

3. Use ccmdelcert.exe to delete the SMS certificates. ccmdelcert.exe is available as part of the Systems Management Server 2003 Toolkit, and is also attached to the wiki page.

4. Delete c:\windows\smscfg.ini if it exists.

5. Capture a base layer.

   Do not reboot or start the ccmexec service. Otherwise you must repeat this procedure.
Setting Up the SSL Certificate in Windows Server

For environments with multiple Horizon Mirage servers where SSL is required, you must enable SSL and install the SSL certificate for each server.

Enabling SSL involves setting up the SSL certificate in Windows Server on Horizon Mirage servers, which includes generating the certificate signing request (CSR), requesting the CSR, and installing the signed certificate.

In a multiserver setup, the SSL certificate setup for Windows Server must be repeated for each installed Horizon Mirage server.

Generate the Certificate Signing Request

When you set up an SSL certificate, you must first generate the certificate signing request.

Procedure

1. On the server, open the Horizon Mirage Management console.
2. Add and configure the Certificates snap-in:
   a. Open the Horizon Mirage Management console.
   b. Select File > Add/Remove Snap-in.
   c. Add Certificates.
   d. Specify that the snap-in will manage certificates for the Computer account and click Next.
   e. Verify that This snap-in will always manage Local computer is selected and click Finish.
   f. Click OK.
3. Select the Certificates node in the console root, right-click Personal store and select All Tasks > Advanced Operations > Create Custom Request.
4. In the Custom Request area, select Proceed without enrollment policy.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Request</td>
<td>Select Proceed without enrollment policy.</td>
</tr>
<tr>
<td>Template and Request Format</td>
<td>Accept the default settings for the CNG Key and PKCS #10 text boxes.</td>
</tr>
<tr>
<td>Certificate Information</td>
<td>Click Details for the Custom Request and click Properties.</td>
</tr>
</tbody>
</table>

5. Click the General tab and type a certificate-friendly name.
   You can use the same name as the subject name.
6. Click the Subject tab, and in the Subject Name area, provide the relevant certificate information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common name, value</td>
<td>Server FQDN. This is the certificate subject name that is used in the Horizon Mirage configuration to find the certificate. The FQDN must point to that server and is validated by the client upon connection.</td>
</tr>
<tr>
<td>Organization, value</td>
<td>Company name, usually required by the CA.</td>
</tr>
<tr>
<td>Country, value</td>
<td>Two-letter standard country name, for example, US or UK. Usually required by the CA.</td>
</tr>
<tr>
<td>State, value</td>
<td>(Optional) State name.</td>
</tr>
<tr>
<td>Locality, value</td>
<td>(Optional) City name.</td>
</tr>
</tbody>
</table>
7 Click the **Extensions** tab and select the key use information from the pull-down menus.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Usage</strong></td>
<td>Select Data Encipherment.</td>
</tr>
<tr>
<td><strong>Extended Key Usage</strong></td>
<td>Select Server Authentication.</td>
</tr>
</tbody>
</table>

8 Click the **Private Key** tab and select key size and export options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Options</strong></td>
<td>Select the required key size (usually 1024 or 2048).</td>
</tr>
<tr>
<td><strong>Make Private Key Exportable</strong></td>
<td>Select to export the CSR, and later the certificate, with the private key for backup or server movement purposes.</td>
</tr>
</tbody>
</table>

9 Click **OK** to close the Certificate Properties window, and click **Next** in the Certificate Enrollment wizard.

10 Leave the default file format (Base 64), and click **Browse** to select a filename and location of where to save the CSR.

The certificate request is completed.

11 Click the **Certificate Enrollment Requests & Certificates** tab, and click **Refresh**.

You can export the CSR with the private key for backup purposes.

**What to do next**

After you generate the certificate signing request, you submit the certificate request. See “Submit the Certificate Request,” on page 147

### Submit the Certificate Request

After you generate the certificate signing request, you submit the request.

**Procedure**

1. Open the `csr.req` file with notepad.
2. Copy the text.
3. Go to the external CA Web site, paste the CSR text in the provided form, and submit the form.

**What to do next**

When the CA sends you the signed certificate file (`.cer` or `.crt`), you can install the signed certificate.

### Install the Signed Certificate

When the CA sends you the signed certificate file (`.cer` or `.crt`), go back to the certificates snap-in and install the signed certificate.

**Procedure**

1. On the server, open the Horizon Mirage Management console.
2. Select the **Certificates** node in the console root, right-click **Personal store** and select **All Tasks > Import**.
3. Browse to the signed certificate file and select it.
4. Select **System Auto Selection** or **Personal Store** for the certificate.
5. Follow the prompts to complete the import.
6 Click the **Personal Certificates** tab and click **Refresh** to load current details.

7 Open the certificate and verify that it states that you have the private key.

8 Click the **Certification Path** tab and check that you have all of the certificates in the chain and that no validity warnings or missing certificates are present.

### Using Microsoft Office 2010 in a Layer

You can build Microsoft Office licenses into your layers to prevent interfering with existing licenses on user endpoints.

During the layer capture process, Horizon Mirage prompts you for the Microsoft Office 2010 license key, as well as licenses for every other activated Office component on the reference machine, such as Office, Visio, and OneNote. When you deploy the layer to an endpoint, these Office keys are used when installing Office. This is done to preserve the licensing for an existing version of Office and helps prevent problems with Office and Visio licensing.

**Note**: If you are upgrading from Office 2007 to Office 2010 and end users have specific components, such as Visio, installed on their endpoints, make sure that those components are also installed in the new base layers so that those applications will remain on the endpoints.

### Managing Role-Based Access Control and Active Directory Groups

An administrator can use dynamic role-based access control (RBAC) to define which users can perform which operations in the system. You can grant a role to one or more Active Directory (AD) groups. The Horizon Mirage server identifies users by AD group membership and automatically assigns their matching user roles in the system.

A user can have only one active role at a time. If the user’s group is assigned to more than one role, the user inherits the superset privileges of all assigned roles.

Each role is mapped to a set of actions the user can perform in the system, such as managing CVDs, base layers, users, groups, and events, as well as viewing the dashboard and other system information.

You can define additional custom roles to suit various company processes.

### Role Definitions

The following is a list of actions in the system for which role-based access can be defined for specific users:

**Table 23-1. System Actions for which Role Based Access can be Defined for a User**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View dashboard</td>
<td>View the dashboard.</td>
</tr>
<tr>
<td>View server status</td>
<td>View the server status node. If not applicable, it appears as an empty list.</td>
</tr>
<tr>
<td>View tasks</td>
<td>View the tasks list in the Task Monitoring node.</td>
</tr>
<tr>
<td>Manage tasks</td>
<td>Delete running tasks.</td>
</tr>
<tr>
<td>View CVDs</td>
<td>View the CVD inventory.</td>
</tr>
<tr>
<td>Manage CVDs</td>
<td>Delete a CVD, assign a base layer to a CVD, enforce a base layer, assign a policy to a CVD, and revert to snapshot.</td>
</tr>
<tr>
<td>Manage collections</td>
<td>Create and remove collections.</td>
</tr>
<tr>
<td>Manage collections CVDs</td>
<td>Add and remove CVDs from a collection.</td>
</tr>
<tr>
<td>View upload policies</td>
<td>View policies.</td>
</tr>
<tr>
<td>Manage upload policies</td>
<td>Edit, create, and delete policies.</td>
</tr>
</tbody>
</table>
### Table 23-1. System Actions for which Role Based Access can be Defined for a User (Continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View devices</td>
<td>View the devices in the device inventory and the pending list.</td>
</tr>
<tr>
<td>Manage devices</td>
<td>Assign a device to a CVD, reject a device, restore a device, remove a device, suspend a device, and synchronize the device with the CVD.</td>
</tr>
<tr>
<td>View layers</td>
<td>View the layers that are assigned to different devices.</td>
</tr>
<tr>
<td>Manage layers</td>
<td>Create layers, delete layers, cancel layer assignment (this is a bug), and update layer data (name, details).</td>
</tr>
<tr>
<td>View ref CVDs</td>
<td>View the Reference CVD inventory.</td>
</tr>
<tr>
<td>Manage ref CVDs</td>
<td>Assign a reference device to a reference CVD, assign a base layer to a reference CVD, assign a policy to a reference CVD, and delete a reference CVD.</td>
</tr>
<tr>
<td>View base layer rules</td>
<td>View the image rules.</td>
</tr>
<tr>
<td>Manage base layer rules</td>
<td>Add new rules, remove rules, test base layer draft rules, and set new default base layer rules.</td>
</tr>
<tr>
<td>View driver library</td>
<td>See the driver profiles and driver folders and their details in the driver library</td>
</tr>
<tr>
<td>Manage driver library</td>
<td>Add drivers to the driver folders and create new driver profiles, and modify existing driver folders and libraries.</td>
</tr>
<tr>
<td>View reports</td>
<td>View the generated reports.</td>
</tr>
<tr>
<td>Manage reports</td>
<td>Create reports and delete reports.</td>
</tr>
<tr>
<td>View events</td>
<td>View the events under the Event log and Manager Journal.</td>
</tr>
</tbody>
</table>

### Predefined User Roles

Horizon Mirage includes predefined Administrator, Desktop Engineer, and Helpdesk user roles:

### Table 23-2. Predefined User Roles

<table>
<thead>
<tr>
<th>User role</th>
<th>Access Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator role</td>
<td>Access to all Horizon Mirage functions, including base layer management functions and the management of users and roles. The Administrator role cannot be edited or deleted.</td>
</tr>
<tr>
<td>Desktop Engineer role</td>
<td>By default, authorized to perform all system operations except base layer management, user management, and role management. You can customize the default privilege set.</td>
</tr>
<tr>
<td>Helpdesk role</td>
<td>By default, authorized to perform only view operations on the system to troubleshoot a CVD problem. You can customize the default privilege set.</td>
</tr>
</tbody>
</table>

### Add a New User Role

You can add a new user role.

#### Procedure

1. In the Horizon Mirage Management console tree, right-click Users and Roles and select Add a Role.
2. Type the role name and description, and click OK.

   By default, the new role does not have any privileges until they are assigned by the administrator.
Edit an Existing User Role

You can edit an existing user role.

Procedure

1. In the Horizon Mirage Management console tree, click **Users and Roles**.
2. Edit the role check boxes in the right pane as required and click **Save**.

Assign an Active Directory Group to a User Role

You can assign an Active Directory (AD) Group to a role.

A group cannot be added to two different roles.

The role view is not auto-refreshed.

Procedure

1. Expand the **Users and Roles** node, right-click the required user role, and select **Add a Group**.
2. Type the group name in the **Group Name** text box, using the following syntax: `domain\group`.

Macros in Upload Policy Rules

Macros assist specification of various Horizon Mirage directory paths addressed by policy rules. For example, macros allow Horizon Mirage and the administrator to handle cases when some endpoints have Windows in `c:\windows` and some in `d:\windows`. Using macros and environment variables makes sure Horizon Mirage backups important files regardless of their specific location.

For information about upload policy rule specification, see “Add or Edit Upload Policy Rules,” on page 20.

System Directories

The following macros are supported for System directory paths:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%systemvolume%</td>
<td>The system drive letter followed by a “:”</td>
</tr>
<tr>
<td></td>
<td>For example, <code>c:</code>.</td>
</tr>
<tr>
<td>%systemtemp%</td>
<td>The Windows system temp directory.</td>
</tr>
<tr>
<td></td>
<td>Usually <code>c:\windows\temp</code>.</td>
</tr>
<tr>
<td>%windows%</td>
<td>The Windows directory. Usually <code>c:\windows</code>.</td>
</tr>
<tr>
<td>%Anyvolume%</td>
<td>Expands to multiple rules, one per drive letter.</td>
</tr>
<tr>
<td></td>
<td>For example: <code>c:, d:, e:</code>.</td>
</tr>
<tr>
<td>%documentsandsettings%</td>
<td>Expands to one rule of the path that contains the user profiles.</td>
</tr>
<tr>
<td></td>
<td>Usually <code>c:\documents and settings</code>).</td>
</tr>
<tr>
<td>%programfiles%</td>
<td>The program files directory, including support for localized Windows versions,</td>
</tr>
<tr>
<td></td>
<td>and the Program Files (x86) in 64-bit.</td>
</tr>
<tr>
<td>%systemdir%</td>
<td>The Windows system directory.</td>
</tr>
</tbody>
</table>

Profile Directories

The following macros are supported for Profile directory paths:
### Table 23-4. Profile Directory Macros

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%anyuserprofile%</td>
<td>Expands to multiple rules, one per any user profile, including both local user profiles and domain user profiles (for example, C:\Documents and settings\myuser, and so on). This macro does not include the %defaultuserprofile % content.</td>
</tr>
<tr>
<td>%domainuserprofile%</td>
<td>Expands to multiple rules, one per any domain user profile.</td>
</tr>
<tr>
<td>%localuserprofile%</td>
<td>Expands to multiple rules, one per any local user profile.</td>
</tr>
<tr>
<td>%anyuserlocalappdata%</td>
<td>All the users local app data directories.</td>
</tr>
<tr>
<td>%anyusertemp%</td>
<td>All the user’s TEMP directories.</td>
</tr>
</tbody>
</table>

### Special Profile Directories

The following macros are supported for special profile directory paths, not included in the profile directories:

### Table 23-5. Special Profile Directory Macros

<table>
<thead>
<tr>
<th>Macro</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ProgramData%</td>
<td>The special Application data directory under the All Users directory.</td>
</tr>
<tr>
<td></td>
<td>For example, C:\Documents and Settings\All Users\Application data.</td>
</tr>
<tr>
<td>%defaultuserprofile%</td>
<td>The special Default User directory.</td>
</tr>
<tr>
<td>%builtinuserprofile%</td>
<td>Expands to multiple rules, one for each built-in user profile (not including local or domain users). For example, “NetworkService?” and “LocalService?” In Windows XP, this also includes “All Users”.</td>
</tr>
<tr>
<td>%localserviceprofile%</td>
<td>The special “local service” directory.</td>
</tr>
<tr>
<td>%Anyuserroamingappdata%</td>
<td>The roaming application data directory is calculated by appending the roaming application data suffix to the user profile directory. This suffix is AppData\Roaming in Windows 7 and Application Data in Windows XP.</td>
</tr>
<tr>
<td>%Anyusertempinternetfiles%</td>
<td>All the user’s temp internet directories on the machine.</td>
</tr>
<tr>
<td>%any% desktop%shellpaths%</td>
<td>All the directories below.</td>
</tr>
<tr>
<td>%desktop%</td>
<td>All the user’s desktop directories in the machine.</td>
</tr>
<tr>
<td>%favorites%</td>
<td>All the user’s favorites directories in the machine.</td>
</tr>
<tr>
<td>%videos%</td>
<td>All the user’s Video directories in the machine.</td>
</tr>
<tr>
<td>%pictures%</td>
<td>All the user’s pictures directories in the machine.</td>
</tr>
<tr>
<td>%documents%</td>
<td>All the user’s documents directories in the machine.</td>
</tr>
<tr>
<td>%music%</td>
<td>All the user’s music directories in the machine.</td>
</tr>
</tbody>
</table>
Horizon Mirage allows administrators to use Horizon Mirage base and app layering capabilities to manage Horizon View desktop machines of type, persistent memory and fully cloned.

With Horizon Mirage, an administrator of a large scale environment can automatically update operating system and infrastructure software, add and remove application layers, and fix software problems. The user can keep applications, data, and settings intact for software that they have installed.

A Horizon View desktop pool might share storage and resources with other Horizon View pools. Desktop machines undergoing a Horizon Mirage layer update require more resources than usual. Mass image management operations can affect user experience for users in an updated pool and in neighboring pools with which it shares resources. To diminish this effect, Horizon Mirage must limit the level of concurrency when you perform image management operations in the Horizon View pool. An administrator can control the concurrent level via the concurrency value, which controls the effect Horizon Mirage has on the ESX resources.

**Supported Configurations**

Horizon Mirage supports the following Horizon View configurations.

- VMware Horizon View 5.3
- Persistent fully cloned desktop pools

**Supported Horizon Mirage Operations**

The following Horizon Mirage operations are supported with Horizon View:

<table>
<thead>
<tr>
<th>Mirage Operation</th>
<th>Supported with Horizon View</th>
</tr>
</thead>
<tbody>
<tr>
<td>App layer assignment</td>
<td>Yes</td>
</tr>
<tr>
<td>Base layer assignment</td>
<td>Yes</td>
</tr>
<tr>
<td>Enforce layers</td>
<td>Yes</td>
</tr>
<tr>
<td>Apply driver library</td>
<td>Yes</td>
</tr>
<tr>
<td>Centralization</td>
<td>No</td>
</tr>
<tr>
<td>File Portal</td>
<td>No</td>
</tr>
<tr>
<td>HW migration</td>
<td>No</td>
</tr>
<tr>
<td>Provisioning base layer</td>
<td>No</td>
</tr>
<tr>
<td>Restore</td>
<td>No</td>
</tr>
</tbody>
</table>
Table 24-1. Supported Horizon Mirage Operations in Horizon View (Continued)

<table>
<thead>
<tr>
<th>Mirage Operation</th>
<th>Supported with Horizon View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revert to snapshot</td>
<td>No</td>
</tr>
<tr>
<td>Steady state uploads</td>
<td>No</td>
</tr>
<tr>
<td>Windows 7 migration</td>
<td>No</td>
</tr>
</tbody>
</table>

Behavior of Horizon Mirage CVDs with the Horizon View Policy

CVDs that use the Horizon View-optimized policy have special characteristics.

- **No data protection**: The corresponding devices do not upload files to the data center. You cannot revert the devices to a Horizon Mirage snapshot or restore user files to previous versions. Horizon Mirage only periodically uploads metadata about these devices, for example the list of installed applications.

- **No WAN optimizations**: To improve performance for managing Horizon View pools, Horizon Mirage disables most WAN optimizations for these CVDs because they are assumed to be hosted in the same data center as the Horizon Mirage server.

Workflow for Managing Horizon View Desktops

The general workflow for managing Horizon View desktops with Horizon Mirage is that you create a pool that Horizon Mirage manages. This workflow comprises the following procedures:

1. Capturing initial base and app layers.
2. Create a parent virtual machine.
3. Assign the base layer and any app layers to the parent virtual machine.
4. Creating a Horizon View desktop pool from the parent machine.
5. Creating CVDs for all desktops in the newly created pool.

When a base or app layer update is needed, you perform an image update on the relevant CVDs. This process comprises the following procedures:

1. Capturing new or updated base or app layers.
2. Assigning the new layers to the pool.

The desktops are updated gradually, until all desktops have the new layers.

For more information, see the *Managing Horizon View Desktops with Horizon Mirage* documentation.
Index

A
about this guide 7
activating endpoints 13
Active Directory groups and role-based access control 148–150
advanced administration topics 145
app layer assignment
cancel assignment in progress 105
detect potential effects 103
monitor assignment progress 105
procedure 104
testing before distribution 103
app layer capture
capture overview 85
capture procedure 87
multiple layer capture 91
OEM software in app layer 91
post-app layer deployment script 92
procedure 87–89
reference machine 86
what you can capture 90
app layer definition 67
archive CVDs
assign to a device 23
manage CVDs in the archive 22, 23
move to another volume 23
audit events in Manager journal 141
B
back up servers and Management server 137
base layer provisioning 101
base layer
and BitLocker support 69
and system-level software 69
and user-specific software 69
and endpoint security software 69
and OEM software 69
and software licensing 69
hardware considerations 69
recreate reference machine from 75
base layer assignment
assign to a previous layer version 99
detect potential effects of layer change 93–95
enforce layers on endpoints 100
monitor assignments 99
software conflict correction 100
testing before distribution 96
base layer capture
capture procedure 81
override rule examples 80
override registry values and keys 81
post-base layer deployment script 82
rules 77
base layer definition 67
base layer assignment procedure
cancel assignment in progress 98
monitor progress 98
base layer capture rules
set default rule set 79
test 78, 79
view and create rules 77, 78
base layer capture override rules, add override rule set 79
base layer override rule examples
avoid losing local customization 81
avoid shared component incompatibility 80
BitLocker support in base layers 69
bootable USB keys
create 112
customize 114
how to use 113
branch reflectors
configurable values 55
default values 55
disable peering service 56
enable branch reflector 54
IP detection and proximity algorithm 53
matching process 53
pause 56
peer clients, accept or reject 56
select clients to be branch reflectors 54
server network operations 57
settings in system configuration 37
branch reflector download monitoring
connected peer clients 58
CVD associations 57
peer client transactions 58
show potential branch reflectors 59
C
capturing app layers, See app layer capture
capturing base layers, See base layer capture
centralize endpoints
  by administrator 16
  by end-user 16
client status, access 27
comparison report
  base layer assignment 94, 95
  potential effects of app layer 103
  potential effects of base layer 93
configure the system, See system settings
CVD
  archive, See archive CVDs
  autocreation 36
  events history timeline view 141
  file portal end-user mapping 32
  settings 35
  snapshot generation and retention 38
  view files in CVD with file portal 31
CVD collection
  add dynamic collection 21
  add dynamic using Active Directory 22
  static collection management 21
CVD Integrity report 133, 135

D
  dashboard statistics 129
  database and volumes restore 138
  desktop deployment monitoring 129
detect potential effects of layer change 93–95
device hardware report 133
directory-level restore 29
disaster recovery, See endpoint disaster recovery
drivers
  and base layers 69
  and folder management 42–44
driver library 41
driver library architecture 41
driver profile management 44
  import drivers to folders 43
E
  end-user operations
    directory-level restore 29
    file-level restore 28
    Snooze to suspend synchronization 29
    Sync Now to resume synchronization 29
  view client status 27
  view files in CVD with file portal 31
  endpoint disaster recovery
    bootable USB keys 111
    reconnect a device to a CVD 115
    restore process experience 115
  endpoint disaster recovery, restore to a CVD
  after device loss 108, 109
  after hard drive replacement or format 108
  specific files from a CVD snapshot 107
  endpoints
    activate 13
    base layer provisioning 101
    centralize by administrator 16
    centralize by end-user 16
    enforce layers on endpoints 100
  Event log 141
  events history timeline for a CVD 141
F
  file portal
    allow access to 31
    configuration in system settings 36
    end-user CVD mapping 32
    view files 32
  file-level restore
    deleted file from Recycle Bin 28
    previous file version 28
H
  hardware drivers, See drivers
  Horizon View desktops, managing with Horizon Mirage 153
I
  image management overview 67
  install the client
    silent with command-line arguments 14
    through the user interface 13
  IP detection and proximity algorithm 53
J
  Join Domain Account settings 35
L
  layer dry run report 133, 134
  layer management life cycle 67
  licenses for Horizon Mirage 37
  licenses for Office 2010 upgrade in layer 148
  load balancing framework 64
  logs, See system logs
M
  macros in upload policy rules 150
  maintain the system
    servers, Management server, and volumes 137
    upgrade Horizon Mirage version 139
  Management server restore 137
  Manager journal 141
managing Horizon View desktops, supported configurations 153
Microsoft Office 2010 licenses in layer 148
Microsoft System Center Configuration Manager, See SCCM
migrate to Windows 7, See Windows 7 migration
migrate users to different hardware
    a user CVD to another device 117
    many user CVDs 119
minimal restore set, customize 142
monitor system status
    dashboard statistics 129
Transaction log 131
mount volumes 50
multiple servers, See servers
multiple volume deployment, See volume deployment

N
network client throttle mechanism 29

O
OEM software
    in app layer 91
    in base layers 69

P
pending assignment devices
    reinstate using Remove 17
    reject 17
potential branch reflectors 59
provisioning, See base layer provisioning
reassign users to different hardware, See
    migrate users to different hardware
reference machine for app layer capture 86
reference machine for base layer capture
data selection 74
recreate from a base layer 75
setup 73
software considerations and settings 74
registry value override in base layer capture 81
reports
    CVD integrity 133, 135
device hardware 133
layer dry run 133, 134
storage usage 133
system reports 143, 144
restore
customize minimal restore set 142
Management server 137
restore process experience 115
servers 138
specific files from a CVD snapshot 107
standalone server 139
storage volumes and database 138
restore device to a CVD
    after device loss 108, 109
    after hard drive replacement or format 108
specific files from a CVD snapshot 107
restore files
deleted file from Recycle Bin 28
directories from a CVD 29
files from a CVD 28
previous file version 28
retention policy
    CVD snapshots 38
transaction records 131
role-based access control (RBAC) 148
rules for base layer capture 77

S
SCCM client migration preparation 145
scripts for
    post-app layer deployment operations 92
    post-base layer deployment operations 82
    post-Windows 7 migration operations 127
secure socket layer communication, See SSL
servers
    add another server 63
    load balancing integration 64
    multiple server scenario 61
    network operations with branch reflectors and
        clients 57
parameters 62
    remove from system 64
restore 138
    restore standalone server 139
    stop or start server service 63
VMware Watchdog service 64
servers and Management server
    back up 137
    maintenance 137
show potential branch reflectors 59
single-instance storage integrity, See SIS
SIS volume integrity procedure 51
snapshot generation and retention
    snapshots kept 35
Snooze to suspend synchronization 29
software in base layers
    conflict correction 100
    endpoint security 69
    licensing 69
    OEM 69
    system-level 69
    user-specific 69
SSL
  install the SSL certificate 40
  server SSL configuration 40
SSL certificate setup 146, 147
storage usage report 133
storage volumes, See volume deployment
Sync Now to resume synchronization 29
system dashboard 129
system monitoring, See monitor system status
system reports, See reports
system settings
  access 35
  branch reflector settings 37
  CVD auto creation 36
  file portal 36
  general system settings 35
  licenses for Horizon Mirage 37
  SSL configuration 39
  USMT setting import 37
system components 9
system logs
  audit events in Manager journal 141
  events 141
  Transaction log 141
system maintenance, See maintain the system

T
  testing
    app layers before distribution 103
    base layers before distribution 96
    layer capture rules 78
  Transaction log, record retention policy log 131
  troubleshooting 141

U
  unblock volumes 50
  unmount volumes 49
  update app layer, See app layer assignment
  update base layer, See base layer assignment
  upgrade Horizon Mirage version
    before you start 139
    upgrade procedure 140
  upload policies
    upload policy management 19, 20
    upload policy rule macros 150
    upload policy rule management 20
  USMT setting import 37

V
  virtual machine
    and base layer 69
    multiple app layer capture on 91
  VMware Watchdog service, configuration 64
  volume deployment
    add volumes 48
    block volumes 50
    edit volume information 49
    maintain volumes 51
    mount volumes 50
    remove volumes 49
    restore volumes and database 138
    SIS volume integrity procedure 51
    unblock volumes 50
    unmount volumes 49
    volume information 47
  volume settings 35
  volume reactivation, See mount volumes

W
  Watchdog, See VMware Watchdog service
  Windows 7 migration
    in-place migration to same machine 123, 125
    migration to replacement devices 126
    monitor the migration process 127
    post-migration operations using a script 127
    set up the Windows 7 base layer 122