VMware Mirage Getting Started Guide

VMware Mirage 5.8

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Getting Started Overview 1

The *VMware Mirage Getting Started Guide* provides an overview of the features of VMware Mirage and details the most common procedures for Mirage.

With the Mirage system, you have centralized control of a full desktop instance in a distributed infrastructure.

You can update a single base layer in the data center, and automatically synchronize the full image with all associated endpoints when they connect to the network.

You can enforce all layers without overwriting user-installed applications, data, or preferences.

With Mirage, you can migrate operating systems while preserving user profile and data.

Intended Audience

This information is intended for IT decision makers, architects, administrators, and others who need to familiarize themselves with the components and capabilities of Mirage.

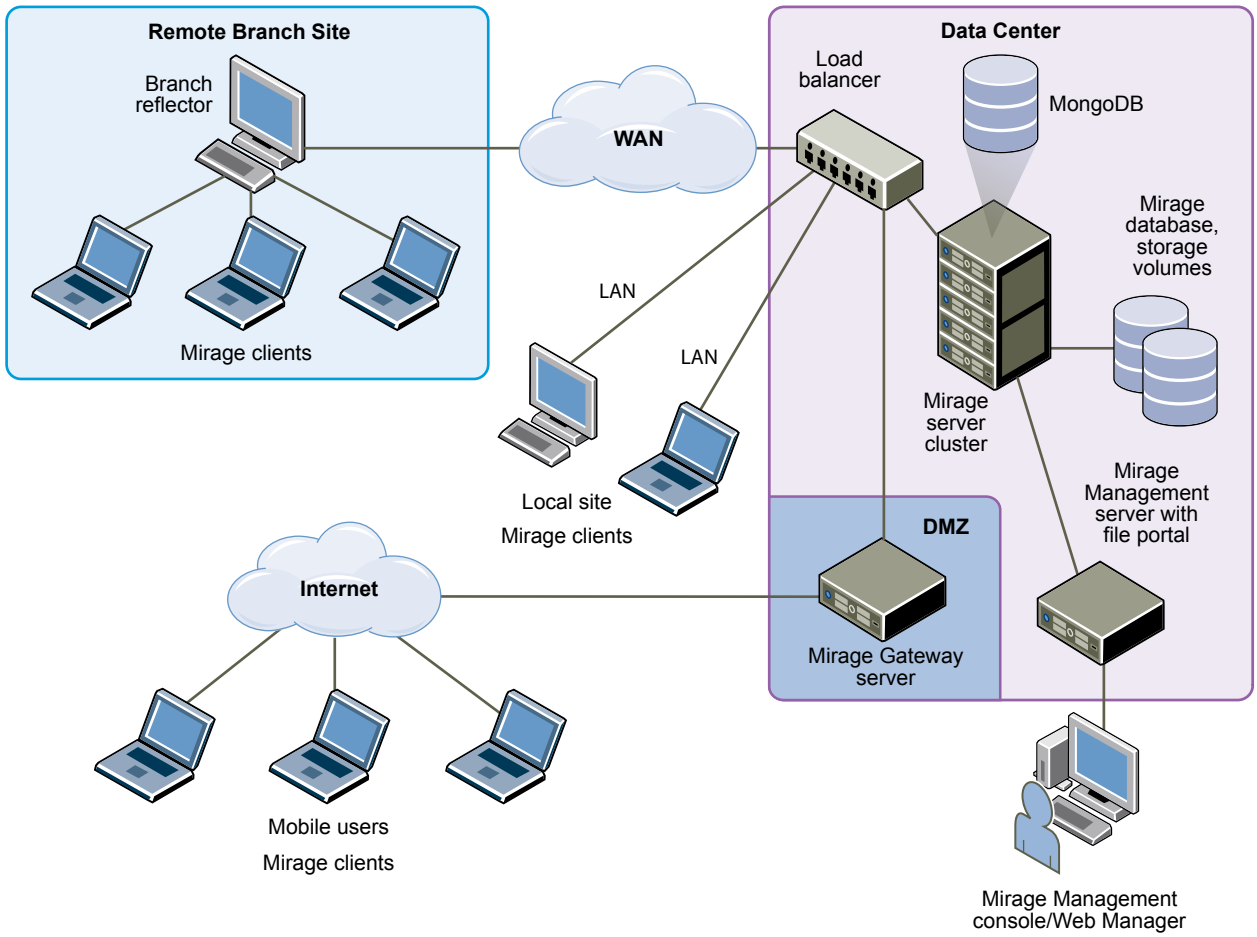
Mirage System Components 2

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

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

Figure 2-1. System Components



Mirage Client

The Mirage client software runs on 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 Mirage client software can run on any Type 1 or Type 2 hypervisor.

Mirage Management Server

The Mirage Management server, located in the data center, is the component that controls and manages the Mirage server cluster. Installing multiple Mirage Management servers increases Mirage availability in the event that a Mirage Management server fails.

Note VMware recommends to set up multiple Management Servers to prevent data loss in case the Management Server fails. A message pops up in the Mirage Management Console whenever you connect to a server inside a cluster with only one enabled Mirage Management server.

Mirage Management Console (Optional)

The Mirage Management console is an optional graphical user interface used for scalable maintenance, management, and monitoring of deployed endpoints. The administrator can use the Mirage Management console to configure and manage Mirage clients, base layers, app layers, and reference machines. The administrator uses the Mirage Management console to update and restore CVDs.

MongoDB File Database

Mirage uses the MongoDB file database to store system data and small files, reducing IOPS and upload time. A MongoDB instance is installed with each Mirage Management server that you install.

Note VMware recommends that you replicate the file database by installing an additional Mirage Management server to achieve a fault tolerance deployment.

If your configuration has only one Mirage Management Server, the Web Management displays a red banner with the following message:

Your system has a single active Management Server. Set up multiple Management Servers to prevent data loss in case the Management Server fails. Important: Do not clone the VM.

If there is more than one management server, but any of the management servers is down or disabled, the following text is displayed:

Some of the Mongo nodes on your system are down, if all nodes are down Mirage **operations will fail. View the Management Servers tab for details. After resolving the issue start the Management Server via Management Servers tab. For more information refer to KB2144975.**

After you install two Mirage Management servers Mirage creates a replica of the MongoDB database.

Verify that you have a dedicated drive with at least 250GB of free disk space for the MongoDB database files. If you cannot designate a local drive or SAN for the MongoDB database files, designate a dedicated NAS volume on higher-end storage with lower latency to minimize disconnects between MongoDB and the MongoDB files.

As an administrator, you can move the MongoDB data of a selected Mirage Management Server to a different location. This feature is enabled only after installing more than one Mirage Management Server. In your Web Management, click **Servers** > **Management Servers** > **Configure**. In the Configure Mirage Management Server dialog, enter the name of the location where you move the MongoDB data and click **OK**.

Mirage Web Management

The Mirage Web Management is the Web-based application that is used for scalable maintenance, management, and monitoring of deployed endpoints. Mirage Web Management has roles such as Helpdesk, Data Protection manager, Image Manager, and Administrator. Data Protection Manager ensures data is properly backed up and protected on user devices. Image manager can capture and deploy layers, provision new devices, and manage branch reflectors. The administrator role has the highest level of permissions and can preform all operations in the system including managing servers. It helps administrator and help desk personnel respond to service queries, and lets the Protection Manager role ensure that user devices are protected. The administrator can use the Mirage Management console to configure and manage Mirage clients, base layers, app layers, and reference machines. The administrator uses the Mirage Management console to update and restore CVDs. For more information, see the *VMware Mirage Web Management Guide*.

Mirage Server

The Mirage servers, located in the data center, synchronize data between the Mirage client and the datacenter. The Mirage servers also 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 run on the same machine as the Mirage Management server.

The server machine must be dedicated for the Mirage server software to use. The server machine must not be used for other purposes.

Centralized Virtual Desktop

CVDs represent the complete contents of each PC. This data is migrated to the Mirage server and becomes the 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 several components.

Table 2-1. CVD Components

Component	Defined By (Role)	Description
Base layer	Administrator	The base layer includes the operating system (OS) image and 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	Administrator	App layers include sets of one or more departmental or line-of-business applications, and any updates or patches for already installed applications. App layers are suitable for deployment to a large number of endpoints.
Driver profile	Administrator	The driver profile 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	End users	User-installed applications and machine state can include a unique identifier, host name, any configuration changes to the machine registry, DLLs, and configuration files.

Mirage Reference Machine

A 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, patches, corporate applications for all target end users to use, corporate configurations, and policies. A reference machine is also used 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 regularly over the LAN or WAN, using a 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.

Mirage Branch Reflector

A 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 Mirage server cluster. A branch reflector can significantly reduce bandwidth use in several situations, such as during mass base or app layer updates. The branch reflector also assists in downloading hardware drivers.

Mirage File Portal

End users can use appropriate Mirage login credentials and the Mirage file portal to access their data from any Web browser. The back-end component runs on the Management server.

Distributed Desktop Optimization

The Distributed Desktop Optimization mechanism optimizes transport of data between the Mirage server and clients, making the ability to support remote endpoints feasible 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.

Mirage Gateway Server

The Mirage Gateway server is the secure gateway server that is deployed outside the Mirage data center environment, but should be within the datacenter. The Mirage Gateway server meets the enterprise security and firewall requirements and provides a better user experience for Mirage clients that access the Mirage servers through the Internet. The Mirage Gateway server seamlessly integrates with the Mirage system with minor modifications to the Mirage system and protocol.

Installation Overview 3

To ensure a successful Mirage deployment, understand the sequence of tasks required.

Before you install the Mirage system, ensure that all of the hardware and software prerequisites are fulfilled, that you have a valid license for the Mirage system, and that you downloaded the latest version of the Mirage software from the support site. For information about licenses for Mirage, see the *VMware Mirage Installation Guide*.

Ensure that the SQL server is installed and reachable before you install the Mirage system. The SQL browser service must be started to allow remote connections. Ensure that the firewall settings allow remote connections on the SQL server host.

You install the Mirage system in this order:

1 Collect the required database information, or install a new database instance to be used with Mirage. You must have database creator privileges to create the Mirage database in the SQL express database.

2 Install the Mirage Management server. See the *VMware Mirage Installation Guide*.

3 Install the Mirage server. See the *VMware Mirage Installation Guide*.

4 Install the Mirage Web Management Console. See the *VMware Mirage Installation Guide*.

5 Install the Mirage File Portal. See the *VMware Mirage Installation Guide*.

6 (Optional) Install the Mirage Management Console. See the *VMware Mirage Installation Guide*.

7 Connect the console to the Mirage System. See the *VMware Mirage Installation Guide*.

8 Install the Mirage Gateway server. See the *VMware Mirage Installation Guide*.

Capturing Base Layers

4

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.

A similar process is employed to capture app layers.

You can use a custom post-base layer script called `post_core_update.bat` to perform certain actions after the base layer update.

Capturing App Layers 5

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 that contains a single application, or a suite of applications from the same vendor. You can 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.

The app layer capture process creates a 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.

Assigning Base Layers

6

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

Processes similar to assigning a base layer are employed to assign applications associated with app layers to endpoints. See Assign an App Layer to CVDs.

For more information about the base layer deployment process, see Layer Management Life Cycle.

For more information, see the *VMware Mirage Administrator's Guide*.

Assigning App Layers

7

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

When you assign app layers to an endpoint, their contents are applied to the endpoint, so that all the changes or modifications to the applications reside on the endpoint devices. See Assign an App Layer to CVDs.

For more information about app layers, see Base Layers and App Layers.

For more information about the layer deployment process, see Layer Management Life Cycle.

For more information, see the *VMware Mirage Administrator's Guide*.

Fixing Broken Layers on Endpoints

8

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

The 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.

Centralizing Endpoints

9

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

When you first introduce Mirage to your organization, you must back up each device, creating a copy of it on the server, in the form of a Centralized Virtual Desktop (CVD) . You can then centrally manage the device.

The endpoint with the client installed appears in the Mirage Management console as Pending Assignment, and is pending activation in the system. You can also reject a device that you do not want to manage in the system.

Provisioning a Layer for an Endpoint 10

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

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

The user can use the desktop as usual, performing offline work and network transitions, after the centralization processing associated with the provisioning operation starts. The 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 provisioning entry. The desktop is protected and you can centrally manage the desktop at the data center.

Creating a Reference Machine from an Endpoint

11

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 you build and configure the reference machine, you can centralize the device as a reference machine for base layer capture.

A pending device that is assigned as a reference machine is moved from the Pending Devices list to the Reference CVDs view.

For more information, see the *VMware Mirage Administrator's Guide*.

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

12 Windows OS Migration

You can migrate existing Windows XP or Windows Vista endpoints to Windows 7, and existing Windows 7 endpoints to Windows 8.1 and Windows 10. The migrations can be either in-place, on the same devices, or to replacement devices.

The migration installs a Windows 7, Windows 8.1, or Windows 10 base layer on each target endpoint while preserving user profile data and settings through the Microsoft User State Migration Tool.

- USMT 4.0 or USMT 5.0 for Windows XP to Windows 7 migration
- USMT 6.3 for Windows 7 to Windows 8.1 migration
- USMT 10.0 for Windows 7 to Windows 10 migration

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 you do not need it.

OS migration with Mirage retains the original computer name but requires rejoining the domain to create a Windows 7, Windows 8.1, or Windows 10 machine account. You can define this account in the Mirage system configuration.

Custom boot loaders on the target machine are removed by the migration. If an endpoint includes multiple operating systems, 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 the new OS.

Note Mirage requires certain Full Disk Encryption applications to be pre-configured before performing an OS migration. For more information about supported Full Disk Encryption software, contact VMware Support.

Prerequisites

- To reduce bandwidth during OS migration in a small or remote office, use the Mirage branch reflector feature. In particular, a Windows 7, Windows 8.1, or Windows 10 test machine configured as a branch reflector can share its OS files with client endpoints to assist in the migration process.
- USMT does not migrate applications installed on Windows XP or Windows Vista to Windows 7, or applications installed on Windows 7 to Windows 8.1, or Windows 10.
- 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 OS Migration End User Experience

After the migration base layer download is completed, the system requests a reboot. A swap is made and Windows 7, Windows 8.1, or Windows 10 boots.

Login is disabled until the system completes the migration process. The new OS is loaded and Plug-and-Play hardware is installed and configured. This process might take a few minutes, during which the computer is busy.

You can monitor the progress in the Windows login screen. When the process is completed, the system restarts the PC and you can then log in.

The post-migration script runs the USMT and then rejoins the domain. The PC must 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 Mirage server and the domain controller. End users can log in using their domain credentials only after the domain join is complete.

Restoring a Device to a CVD Snapshot

13

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

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.

You can use a CVD snapshot to restore a specific file or a complete endpoint on an existing device. Restoring a specific file is the same process as restoring a previous file version. To restore a specific file from a CVD snapshot, see Restore a Previous File Version.

When restoring a complete device from a CVD snapshot you can restore using the same operating system, for example, Windows 7 to Windows 7, or cross-operating systems, for example, Windows 7 to Windows XP or Windows Vista. However, you cannot revert a Windows XP CVD snapshot to a Windows 7 device or a Windows 8 CVD snapshot to a Windows 8.1 device, for example.

For more information, see the *VMware Mirage Administrator's Guide*.

Restoring to a CVD After Hard Drive Replacement or Device Loss

14

If the hard drive on an endpoint is replaced, corrupted, or formatted, or if the user machine is lost and a new machine is 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 Mirage software requirements. See Software Requirements in the *VMware Mirage Installation Guide*.

When replacing the hard drive, 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
- Restore a CVD to a Replacement Device

Endpoint Disaster Recovery 15

You can restore device files to an earlier CVD snapshot, or restore a device from a CVD after hard-drive replacement, file corruption, format operation, or device replacement.

VMware Mirage provides two modes of disaster recovery:

- 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 active upload policies.
- 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 operation.
  - 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.

Index