VMware Mirage Installation Guide

Mirage 5.2

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-001655-00

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Mirage Installation

The *VMware Mirage Installation Guide* provides information about how to install and deploy the Mirage components and prepare the system to centralize endpoint devices.

Installing the system involves installing the Mirage Management server, console, and server components, and associated applications that facilitate, for example, file portal access.

Intended Audience

This information is intended for anyone who wants to install Mirage. 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.

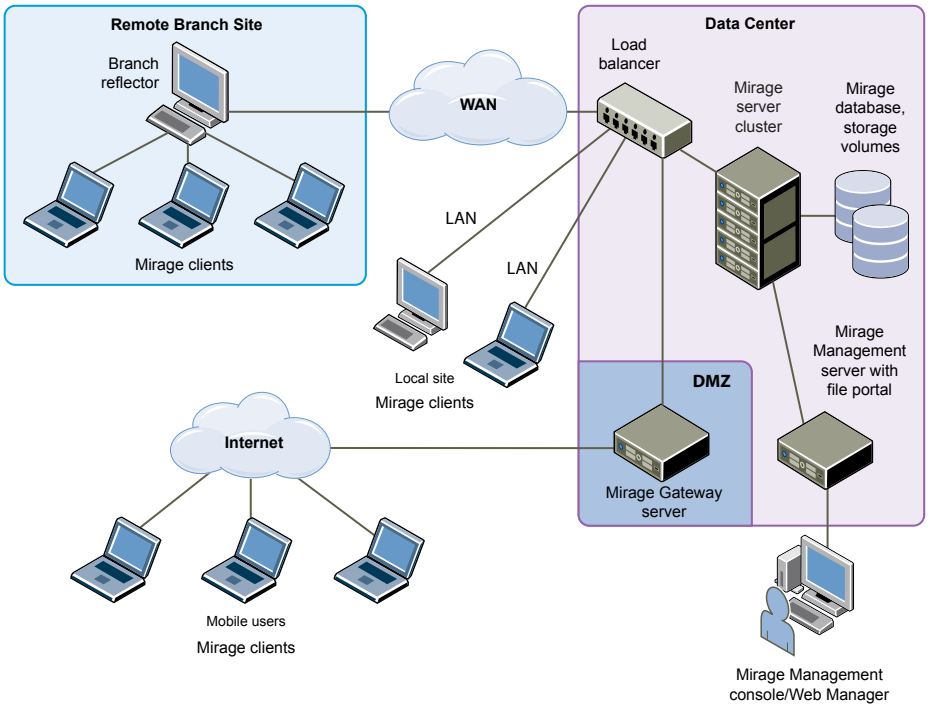
1 Mirage System Components

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 1-1. 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.

Mirage Management Console

The Mirage Management console is the 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.

Mirage Web Manager

The MirageWeb Manager lets help desk personnel respond to service queries, and lets the Protection Manager role ensure that user devices are protected. The Web Manager mirrors Mirage Management console functionality. For more information, see the *VMware Mirage Web Manager 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 1-1. 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 front-end component for the file portal runs on any server machines that have IIS 7.0 or later installed. 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.

Planning the Mirage Deployment 2

Deploying the Mirage system involves ensuring that various requirements of its hardware components, the Mirage Management server, Mirage Management console, Mirage server components, and associated software applications, are satisfied.

The Mirage components support a range of operating systems. Software, hardware, and database requirements apply to each component. The Mirage system and clients use default communication ports and protocols.

This chapter includes the following topics:

Operating System Requirements

Before you deploy Mirage, verify that the operating system requirements for each Mirage component that you install are satisfied.

Table 2-1. Operating System Requirements for Mirage Components

Component	Requirements
Mirage client	■ Windows XP Professional with SP3, 32-bit ■ Windows Vista Business or Enterprise, 32-bit and 64-bit ■ Windows 7 Professional or Enterprise, 32-bit and 64-bit ■ Windows 8.0 and 8.1 Professional or Enterprise, 32-bit and 64-bit ■ Windows Embedded Point of Service (WEPOS) IMPORTANT Mirage only supports updating WEPOS to POSReady 2009 as part of a base layer update procedure.
Mirage server	■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit ■ Windows Server 2012 Standard Edition, 64-bit ■ Windows Server 2012 R2 Standard or Datacenter Edition ■ Domain membership required.
Mirage Management server	■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit ■ Windows Server 2012 Standard Edition, 64-bit ■ Windows Server 2012 R2 Standard or Datacenter Edition ■ Domain membership required

Table 2-1. Operating System Requirements for Mirage Components (Continued)

Component	Requirements
Mirage file portal	■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit ■ Windows Server 2012 Standard Edition, 64-bit ■ Windows Server 2012 R2 Standard or Datacenter Edition ■ Domain membership required
Mirage Web Manager	■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit ■ Windows Server 2012 Standard Edition, 64-bit ■ Windows Server 2012 R2 Standard or Datacenter Edition ■ Domain membership required
Mirage Management console	■ Windows XP Professional with SP3, 32-bit ■ Windows Vista Business or Enterprise, 32-bit and 64-bit ■ Windows 7 Professional or Enterprise, 32-bit and 64-bit ■ Windows 8.0 and 8.1 Professional or Enterprise, 32-bit and 64-bit ■ Windows Server 2008 R2 Standard or Enterprise Edition, 64-bit ■ Windows Server 2012 Standard Edition, 64-bit ■ Windows Server 2012 R2 Standard or Datacenter Edition
Mirage reference machine	■ Windows XP Professional with SP3, 32-bit ■ Windows 7 Professional or Enterprise, 32-bit and 64-bit ■ Windows 8.1 Professional or Enterprise, 32-bit and 64-bit
Mirage Gateway server	The Mirage Gateway server runs on the SUSE11 SP3 operating system. The OS is deployed during the Mirage Gateway installation.

NOTE Windows XP Fast User Switching mode must be disabled if the computer is not an AD domain member.

Hardware Requirements

Before you deploy Mirage, verify that the hardware requirements for each Mirage component that you install are satisfied.

Table 2-2. Hardware Requirements for Mirage Components

Component	Requirements
Mirage client	■ Client systems: ■ Enterprise-class laptops and desktops Virtual machines compatible with Windows XP SP2 or later, Windows Vista or Windows 7 ■ Minimum RAM: 512 MB for Windows XP, 1 GB for Windows Vista, Windows 7, Windows 8, and Windows 8.1 ■ Client installation and normal operation: At least 5 GB of free space
Mirage server node (up to 1000 clients)	■ Minimum RAM: 8 GB ■ Minimum CPU: 4 vCPU ■ Minimum System Drive capacity: 146 GB, including 100 GB for the Mirage network cache Mirage SIS storage is not included. ■ 2 x Gigabit Ethernet Port **NOTE** It is good practice to separate client network and storage network access to dedicated ports.

Table 2-2. Hardware Requirements for Mirage Components (Continued)

Component	Requirements
Mirage server node (up to 1500 clients)	■ Minimum RAM: 16 GB ■ Minimum CPU: 8 vCPU or dual Quad-Core Processor, 2.26 GHz Intel core speed ■ Minimum System Drive capacity: 146 GB, including 100 GB for the Mirage network cache Mirage SIS storage is not included. ■ 2 x Gigabit ethernet port **NOTE** It is good practice to separate client network and storage network access to dedicated ports.
Mirage storage	■ Standalone Mirage server: ■ Direct Attached Storage (DAS) ■ Storage Area Network (SAN) connected through iSCSI or Fiber Channel (FC) ■ Network Attached Storage (NAS) connected through iSCSI, Fiber Channel (FC), or CIFS network share ■ Mirage server cluster: Network Attached Storage (NAS) connected using a CIFS network share. A Windows-based NAS (CIFS share or a file server) can be used for up to 3000 endpoints. An enterprise-grade NAS devices is required for more that 3000 endpoints. ■ Alternate Data Streams: NAS through CIFS share must support Alternate Data Streams. To verify that the NAS device conforms with the Mirage requirements, use the `Wanova.Server.Tools.exe NasCompatibilityTest`. See the VMware knowledge base article at http://kb.vmware.com/kb/2070000 ■ Storage Capacity: Consumed capacity varies, depending on file duplication level across CVDs, base layers, and the number of snapshots stored, but on average, each user requires 15 GB of data center storage. ■ Storage Performance: A minimum of 1.5 IOPS per CVD is required for Mirage steady-state (incremental) uploads. For the centralization phase, higher performance might be needed. Consult with VMware or its partners for the appropriate requirements. ■ Enabling Compression: For DAS, SAN (FC, iSCSI), and Windows-based NAS (CIFS shares), you can realize up to 40% in storage savings by enabling the built-in Windows NTFS compression on your `MirageStorage` folder. For NAS systems that are not NTFS, you need to leverage the systems' compression options. **NOTE** Apply this change only when Mirage services are stopped. Also consider making this change before the directory is heavily populated .
Mirage Management Server	■ Minimum RAM: 8 GB. ■ Minimum CPU: 1 Quad-Core Processor or 4 vCPUs in virtual configuration, 2.26GHz Intel core speed or equivalent
Mirage Management console	■ Minimum RAM: 512 MB. ■ Network connectivity to the Mirage Management server ■ Minimum screen resolution: 1280 x 1024
Mirage File Portal	■ Minimum RAM: 512 MB. ■ Network connectivity to the Mirage Management server ■ Minimum screen resolution: 1280 x 1024
Mirage Web Management Console	■ Minimum RAM: 512 MB. ■ Network connectivity to the Mirage Management server ■ Minimum screen resolution: 1280 x 1024
Mirage Gateway server	■ 4 core CPU, 2.26 GHz Intel core speed or equivalent ■ 4 GB RAM ■ 40 GB available disk space ■ 1 x Gigabit Ethernet port

Table 2-2. Hardware Requirements for Mirage Components (Continued)

Component	Requirements
Microsoft SQL Server 2012	Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2012.
Microsoft SQL Server 2008 R2	Use the recommended Microsoft Hardware and Software Requirements for Installing SQL Server 2008 R2.

Software Requirements

Before you deploy Mirage, verify that the software requirements for each Mirage component that you install are satisfied.

Table 2-3. Software Requirements for Mirage Components

Component	Requirements
Mirage client	Microsoft .NET Framework version 3.5 SP1
Mirage server	■ Microsoft .NET Framework version 3.5 SP1 64-bit ■ For the file portal, an IIS 7.0 or later installation, the IIS 6 Management Compatibility Role, and the ASP.NET feature. Both options are within the IIS installation and are not selected by default.
Mirage Management server	Microsoft .NET Framework version 3.5 SP1 64-bit.
Mirage Management console	■ Microsoft .NET Framework version 3.5 SP1 ■ Microsoft Management Console version 3.0 or later

Mirage reference machine	■ Mirage client.
	■ The OS and applications installed on the reference machine must use volume licenses and be designed for multiuser and multimachine deployment.
	■ Verify that the reference machine does not include the following items:
	  ■ Applications that install and use hardware-specific licenses.
	  ■ Applications that install and use local user accounts, local groups, or both.
	  ■ Software that uses a proprietary update service. Such software must be installed directly on endpoints.

Mirage file portal	■ Microsoft IIS 7 or later ■ Microsoft .NET Framework version 3.5 SP1
Mirage Web Manager	■ Microsoft IIS 7.0 or later ■ Microsoft .NET Framework 4.0

Database Requirements

Before you deploy Mirage, verify that all database software requirements are satisfied.

Table 2-4. Database Software Requirements for Mirage Components

Component	Requirements
Database software	■ Windows Installer 4.5 (MS KB942288) or later ■ Microsoft SQL Server 2012 64-bit SP1 Express, Standard, and Enterprise editions ■ Microsoft SQL Server 2008 64-bit R2 Express, Standard, and Enterprise editions NOTE If you install SQL Server 2008 R2 on Windows Server 2012, you must install Service Pack 1 or later. MS SQL Server must be set up with Windows Authentication. The Windows account used for installing Mirage must have **dbcreator** privileges, and the user account running the Mirage server services must be configured with access privileges to the Mirage database.

Database Sizing Requirements

Table 2-5. Mirage Database Sizing Guidelines

Mirage Cluster Size	Minimum System Requirements
Mirage cluster with fewer than 5000 endpoints	Microsoft SQL Server 2008 Express R2 or Microsoft SQL Server 2012 Express
	At least one CPU, 2.0 GHz or faster
	At least 1 GB RAM
Mirage cluster with more than 5000 endpoints	Microsoft SQL Server 2008 Standard R2 or Microsoft SQL Server 2012 Standard
	At least two CPUs, 2.0 GHz or faster
	At least 4 GB RAM

The database sizing requirements for Mirage are based on the Microsoft hardware and software requirements for installing SQL Server 2008 R2.

Ports and Protocols Used by Mirage

The Mirage system and clients use default communication ports. Make sure that the correct ports and protocols are selected for the system.

The Mirage Management server and Mirage servers use external communications to communicate with the Mirage clients or the Mirage Management console, and internal communications to communicate with each other.

Table 2-6. Ports and Protocols for Mirage Components

Component	Communications	Port	Protocol	Notes
Mirage service	External	8000	TCP/IP or SSL/TLS	The only port required for communications between Mirage clients and servers. NOTE SSL/TLS is optional and can be enabled. See "Install the Server SSL Certificate," on page 21.
Mirage Branch Reflector	External	8001	TCP/IP	Used for communication between the branch reflector and the local peers at the remote site.

Table 2-6. Ports and Protocols for Mirage Components (Continued)

Component	Communications	Port	Protocol	Notes
Mirage Management service	External	8443 , 1443	TCP/IP	Used for communication between the Mirage Management console and the Mirage Management service. SOAP Message-level Security is applied.
Mirage Server service	Internal	135, 445	TCP/IP	Used for control communication between the Mirage Management service and the Mirage server. **NOTE** You can limit access to this port to incoming connections from the Mirage Management service host.
File portal	Internal	6080, 6443	TCP/IP	Used to access the file portal.
Mirage Web Manager	Internal	7080, 7443	TCP/IP	Used to access the Web Manager.
Mirage Gateway server	Internal	8000	TCP/IP	Used for communication between the Mirage Gateway server and the Mirage server. **NOTE** The port must have DNS update access.
	Internal	389, 636	TCP/IP LDAP or LDAPS	Used for communications between the Mirage Gateway server and the LDAP servers.
	Internal	8080	TCP/IP	Used for communications between the Mirage Gateway server and the Mirage Management server.
	External	8000	TLS/SSL	Used for communication between the Mirage client and the Mirage Gateway server.
	Internal	8093	TCP/IP	Used for communication between the Mirage server and the Mirage Gateway server.
Mirage API	Internal	7443	HTTPS	

Installing the Mirage System

3

The Mirage deployment involves a number of components, which you must install in a specific order.

Prerequisites

- Verify that all hardware and software prerequisites are fulfilled.
- Verify that you have a valid license for the system.
- Verify that the latest version of the Mirage software is downloaded from the support site.
- Verify that the SQL server is installed and reachable. The SQL browser service must be started to allow remote connections. Verify that firewall settings allow remote connections on the SQL server host.
- Prepare the required database information, or install a new database instance to use with Mirage.
- Verify that antivirus software running on the server machine excludes Mirage server folders and processes from scanning.
  - Server folders, including the Mirage storage directory folder and the local cache directory, for example, `C:\ProgramData\Wanova Mirage\LocalCache`.
  - Server processes, for example, `Wanova.Server.Service.exe`.
- You must have **dbcreator** privileges to create the Mirage database in the SQL express database. If you do not have these privileges, ask the database administrator to create the database and then designate you as the database creator.

Procedure

1 Worksheet for Installing the Mirage Management Server on page 19

When you install the Mirage Management server, the installation wizard prompts you to configure certain options. You must prepare your configuration options before you install the Management server.

2 Install the Mirage Management Server on page 19

The Mirage Management server is the component that controls and manages the Mirage server cluster.

3 Install a Mirage Server on page 20

The Mirage server manages the storage and delivery of base and app layers and CVDs to clients, and consolidates monitoring and management communications. After you install and license the Mirage Management server, you can install Mirage servers.

4 Install IIS on page 23

You must install Windows Internet Information Services (IIS) 7.0 before installing the Mirage file portal or the Mirage Web Manager.

5 Install the Web Manager on page 25

You install the Mirage Web Manager using the Web Manager `.msi` file provided in the installation package.

6 Install the Mirage File Portal on page 25

Install the Mirage file portal so that end users can view files in their CVD snapshots from a Web browser. End users can access the file portal with the appropriate login credentials.

7 Install the Mirage Management Console on page 27

The Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints. The Management console is built as a Microsoft Management Console version 3.0 snap-in.

8 Connect the Console to the Mirage System on page 27

After you install the Mirage Management console, you can connect the console to the Mirage system.

9 Installing the Mirage Gateway Server on page 27

The Mirage Gateway server is a secured gateway server that is deployed outside the Mirage data center environment.

10 Installing the Mirage Client on page 36

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

11 Install the Mirage PowerCLI on page 38

VMware Mirage PowerCLI provides an easy-to-use Windows PowerShell interface for command-line access to administration tasks.

12 Managing Mirage Software Licenses on page 39

The Mirage Management server requires a license. The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement.

13 Configure the Environment for Endpoints on page 39

Before you can attach endpoints to your system, you need to perform a minimum configuration, which includes configuring the Web URL for the file portal, importing USMT settings, and performing domain joining operations.

Worksheet for Installing the Mirage Management Server

When you install the Mirage Management server, the installation wizard prompts you to configure certain options. You must prepare your configuration options before you install the Management server.

Table 3-1. Configuration Options for Installing the Mirage Management Server

Option	Description	Your Value
SQL server name and instance	Select the SQL server name and instance. ■ SQLEXPRESS is defined as the default SQL instance for the SQL Server Express edition. ■ You can type the server name without an SQL instance when using a default unnamed instance such as SQL Standard. Alternatively, you can type the SQL instance name that is configured in your environment. ■ MSSQL is defined as the default SQL instance for the SQL Server Enterprise edition. ■ Use the default SQL instance name if your Microsoft SQL Server edition was installed with default options, or the custom instance name if you defined a custom name.	
Storage areas	Use the **Create new storage areas** option if this is a new installation of the system or if you do not want to keep the current data. Do not select the **Create new storage areas** check box when upgrading the Mirage Management server. If you select this option and enter the path to the original storage area, your entire Mirage installation, including base layer, app layer, CVD data, and so on, are deleted and become irretrievable if a backup is unavailable.	
Services account configuration	You can use a local system account or a specific user account. Use of a specific user account requires use of login credentials.	

Install the Mirage Management Server

The Mirage Management server is the component that controls and manages the Mirage server cluster.

In the installation process you are prompted to join the VMware Customer Experience Improvement Program (CEIP). If you join CEIP, the CEIP tool collects technical data from the Mirage database and log files, and sends the data to VMware on a daily basis. Before the data is sent to VMware, it is deidentified and encrypted in your systems or servers. If you do not join CEIP during the Mirage Management server installation, you can join CEIP by updating the CEIP settings in the Web Manager. See the *VMware Mirage Web Manager Guide*.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

Verify that the following conditions are in place.

- You have **db_creator** privileges on the SQL Server.
- You have **dbo** permissions on the MirageDB databasee.
- The relevant software requirements are met. See "Software Requirements," on page 14

Procedure

1 Double-click the `mirage.management.server.64x.msi` file to start the installation wizard.

2 Follow the prompts to install the Mirage Management server.

Use the configuration information that you gathered in the worksheet.

The Mirage Management server is installed.

What to do next

- Set the SQL server recovery model to simple.
- You can install a Mirage server. See "Install a Mirage Server," on page 20.
- If you plan to use Mirage PowerCLI, you must enable the WCF HTTP Activation Feature in Windows Server 2008 R2 and Windows Server 2012. See the *VMware Mirage API Programming Guide*.

Install a Mirage Server

The Mirage server manages the storage and delivery of base and app layers and CVDs to clients, and consolidates monitoring and management communications. After you install and license the Mirage Management server, you can install Mirage servers.

You can deploy multiple servers as a server cluster to manage endpoint devices for large organizations. With multiple servers and storage volumes, enterprise organizations can store, manage, and protect end-user device data for large numbers of managed endpoint devices. For more information, see Deploying Additional Mirage Servers in the *VMware Mirage Administrator's Guide*.

The Mirage server uses local cache, a storage of popular data blocks, to perform data deduplication over the WAN. When large files are transferred, their blocks are kept in the cache, and the next time similar files need to be transferred, the server obtains the blocks from the cache instead of over the network. It is good practice to keep the cache on fast storage, for example, on a local drive or even on an SSD drive.

The server installation process includes the default option to set up SSL, which requires an SSL Certificate to be installed on the server. See "Install the Server SSL Certificate," on page 21.

If SSL is not implemented during server installation, you can implement it after the server is installed. See Configuring Secure Socket Layer Communication in the *VMware Mirage Administrator's Guide*.

IMPORTANT Disabling SSL encryption is not recommended as this mode of connection is not secure.

Procedure

1 Install the Server SSL Certificate on page 21

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

2 Worksheet for Installing the Mirage Server on page 22

When you install the Mirage server, the installation wizard prompts you to configure certain options. Prepare your configuration options before you install the Mirage server.

3 Install the Mirage Server on page 23

The Mirage servers manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate communications for monitoring and management. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations.

Install the Server SSL Certificate

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

The Mirage server uses the local computer store.

Prerequisites

Ensure that the certificates are installed in the local Computer Trust Store . If you do not have a certificate, you can create one with tools such as the Microsoft MakeCert. You must then import the result into the Certificate Manager.

Procedure

1 Open the Windows Management Console, add the Certificates snap-in, and select the local computer account.

2 To navigate to your certificate, select **Certificates > Personal > Certificates**.

3 Note the Certificate Subject and Certificate Issuer values.

What to do next

For the Mirage server, continue to the server installation procedure to enter the SSL certificate values. See Install the Mirage Server.

Worksheet for Installing the Mirage Server

When you install the Mirage server, the installation wizard prompts you to configure certain options. Prepare your configuration options before you install the Mirage server.

Table 3-2. Configuration Options for Installing the Mirage Server

Option	Description	Your Value
SQL server name and instance	Select the SQL server name and instance. ■ SQLEXPRESS is defined as the default SQL instance for the SQL Server Express edition. ■ You can type the server name without an SQL instance when using a default unnamed instance such as SQL Standard. Alternatively, you can type the SQL instance name that is configured in your environment. ■ MSSQL is defined as the default SQL instance for the SQL Server Enterprise edition. ■ Use the default SQL instance name if your Microsoft SQL Server edition was installed with default options, or the custom instance name if you defined a custom name.	
Local cache areas	Select the **Create new local cache area** check box to allocate a new local cache area. If not selected, the installer attempts to use existing cache data. Do not select the **Create new storage areas** check box when upgrading the Mirage server. If you select this option and the path of the original storage area is entered, the local cache of the server itself is deleted. This might result in short-time performance penalties as the cache has to be refilled.	
Name of the Mirage server local cache folder	The path to where the local cache is stored if different from the default. A default path is provided.	
Size of local cache in MB	A cache size of 100GB (102400MB) is recommended.	
Port	The default port for client-server communication is 8000. If you change the port, additional firewall rules might be required to open the port.	

Table 3-2. Configuration Options for Installing the Mirage Server (Continued)

Option	Description	Your Value
Encryption type	You can select to have an SSL certificate to have clients communicate with the server using SSL encryption. SSL encryption requires the Certificate Subject and Certificate Issuer values. Typically, the Certificate Subject is the FQDN of the Mirage server, and the Certificate Issuer is a known entity like VeriSign. You can leave the **Certificate Issuer** text box blank if only one certificate is installed on this server.	
Services account configuration	You can use a local system account , or you can use a specific user account for your services account. Select the specific user account if you access CIFS share servers in a Mirage cluster environment. This option requires Windows login credentials.	

Install the Mirage Server

The Mirage servers manage the storage and delivery of base layers, app layers, and CVDs to clients, and consolidate communications for monitoring and management. You can deploy multiple servers as a server cluster to manage endpoint devices for large enterprise organizations.

You can allocate a larger number of concurrent CVDs for high-end servers, or a smaller number for low-end servers.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

- Install an SSL Certificate on the server. See "Install the Server SSL Certificate," on page 21.
- Verify that the SQL server is reachable from the server node, and that the firewall settings on the SQL server allow for remote connections.

Procedure

1 Double-click the `mirage.server.64x.msi` file to start the installation wizard.

2 Follow the prompts in the wizard to install the Mirage server.

Use the configuration information that you gathered in the worksheet.

3 Restart the server when the installation is completed.

What to do next

You can now install IIS and the Mirage Web Manager.

Install IIS

You must install Windows Internet Information Services (IIS) 7.0 before installing the Mirage file portal or the Mirage Web Manager.

The `.msi` installation file is located in the Mirage installation package.

Procedure

1 Install the IIS server role on the Windows Server 2008 R2 or later machine where the Mirage server software is installed.

   a In the Server Manager, right-click the **Roles** node and select **Add Roles**.

   b On the left-panel menu, select **Server Roles**.

   c Select the **Web Server (IIS)** check box.

2 After the IIS server role is installed, install Web Service (IIS) services.

   a Expand the **Roles** node and select **Web Server (IIS)**.

   b On the right panel, click **Add Role Services**.

   c Expand the **Web Server** node and add these services.

Role Service	Required Items
Common HTTP Features	■ Static Content ■ Default Document ■ Directory Browsing ■ HTTP Errors ■ HTTP Redirection
Application Development	■ ASP.NET ■ .NET Extensibility ■ ISAPI Extensions ■ ISAPI Filters
Health And Diagnostics	There are no required items for this role service.
Security	Request Filtering
Performance	There are no required items for this role service.

3 Install Management Tools services.

   a Expand the **Roles** node and select **Web Server (IIS)**.

   b On the right panel, click **Add Role Services**.

   c Expand the **Management Tools** node and add these services.

Role Service	Required Items
IIS Management Console	All subitems are required
IIS Management Scripts and Tools	All subitems are required
Management Service	All subitems are required
IIS 6 Management Compatibility	All subitems are required

What to do next

Verify that the appropriate ports are enabled between IIS and the Mirage Management server. See "Ports and Protocols Used by Mirage," on page 15.

Cipher Suites

You can configure cipher suites in IIS.

VMware recommends that you configure IIS with TLS cipher-suites during the Mirage deployment.

TLS Cipher-Suites

- `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA`

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_RSA_WITH_AES_256_CBC_SHA
- TLS_DH_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DH_RSA_WITH_AES_128_CBC_SHA
- TLS_DH_DSS_WITH_AES_128_CBC_SHA

Install the Web Manager

You install the Mirage Web Manager using the Web Manager `.msi` file provided in the installation package.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

- You must enable Cookies and JavaScript.
- The Mirage Web Manager must be installed on a Windows server with IIS 7 or later and .NET Framework 4.
- You can view the Web Manager using Microsoft Internet Explorer 9 and later, Chrome, and Firefox.
- Make sure that your Microsoft Internet Explorer browser supports JavaScript and Cookies on an intranet environment.

Procedure

1 Double-click the `.msi` file for your environment and click **Run** to start the installation wizard.

Option	Description
64-bit	`mirage.WebManagement.x64.`*`buildnumber`*`.msi`
32-bit	`mirage.WebManagement.x86.`*`buildnumber`*`.msi`

2 When prompted, provide the path to the Mirage Management server location.

3 Verify the HTTP port and the HTTPS port.

The default HTTP port is 7080, and the default HTTPS port is 7443.

4 Follow the prompts to complete the installation.

Install the Mirage File Portal

Install the Mirage file portal so that end users can view files in their CVD snapshots from a Web browser. End users can access the file portal with the appropriate login credentials.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

You must install Microsoft IIS 7.0 or later for the file portal. For more information about installing IIS, see "Install IIS," on page 23.

Procedure

1 Double-click the `.msi` file for your environment and click **Run** to start the installation wizard.

Option	Description
64-bit	`mirage.WebAccess.x64.`*`buildnumber`*`.msi`
32-bit	`mirage.WebAccess.x86.`*`buildnumber`*`.msi`

2 Follow the prompts until you come to Web Access Configuration page and provide the Web access configuration information.

Option	Description
Web Access	Select **Web Access** to provide access to only an end-user's user files, as defined by the administrator, across all CVD snapshots. The Mirage client user can access the Web Access feature to only download their files at http://server:6080/Explorer.
Admin Web Access	Select **Admin Web Access** to give the administrator full access to all user CVDs across all CVD snapshots. The administrator can access the Admin Web Access feature to download all files of any user at http://server:6080/AdminExplorer.

By default, both the **Web Access** and **Admin Web Access** web applications are configured for the file portal. You can choose not to configure either of these options by clicking the drop-down menu and selecting **Entire feature will be unavailable**.

3 When prompted, provide the path to the Mirage Management server location.

4 Verify the HTTP port and the HTTPS port.

The default HTTP port is 6080, and the default HTTPS port is 6443.

5 Complete the installation.

What to do next

You can now install the Mirage Management console.

Troubleshooting the File Portal Installation

You might be unable to access the Mirage file portal because of local or domain security policies.

Problem

After the installation is finished, you might experience difficulty accessing the file portal.

Cause

You might be unable to access the file portal because of a local or domain security policy on IIS servers.

Solution

1 On the IIS server machine where the file portal is installed, select **Local Security Policy > Local Policies > User Rights Assignments**.

2 Add all users who need file portal access to the `Allow logon locally` policy.

Install the Mirage Management Console

The Mirage Management console is the graphical user interface used to perform scalable maintenance, management, and monitoring of deployed endpoints. The Management console is built as a Microsoft Management Console version 3.0 snap-in.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

Install the Mirage Management server.

Procedure

1 Double-click the `.msi` file for your environment to start the installation wizard.

Option	Description
64-bit	`mirage.management.console.x64.`*`buildnumber`*`.msi`
32-bit	`mirage.management.console.x86.`*`buildnumber`*`.msi`

2 Follow the prompts to complete the installation wizard.

After you install the Management console, a shortcut to the Management console is added to your desktop.

What to do next

You can connect the console to the Mirage Management system. See "Connect the Console to the Mirage System," on page 27.

Connect the Console to the Mirage System

After you install the Mirage Management console, you can connect the console to the Mirage system.

Procedure

1 In the Mirage Management console tree, click **VMware Mirage** in the root directory, and select **Add System**.

2 Type the IP address or host name of the Mirage Management server in the **Management Server Address** text box, and click **OK**.

The Management console is connected to the system. A Mirage server node now appears in the console window.

After the console is connected, it shows Server Down status for the system because a Mirage server is not yet installed. The server status changes to Up when a server is installed.

What to do next

You can install the Mirage Gateway server. See "Installing the Mirage Gateway Server," on page 27.

Installing the Mirage Gateway Server

The Mirage Gateway server is a secured gateway server that is deployed outside the Mirage data center environment.

The Mirage Gateway server lets end users who have installed the Mirage client to communicate securely with the Mirage servers over the Internet without using VPN configurations.

After installing the Mirage Gateway server, you can configure a Gateway server to your Mirage system by accessing the configuration web portal or by using the Mirage Management console.

1 Generate the Certificate Signing Request for the Mirage Gateway Server on page 28

When you set up the SSL certificate for the Mirage Gateway server, you must first generate the Certificate Signing Request (CSR).

2 Submit the Certificate Request on page 30

After you generate the certificate signing request, you submit the request.

3 Convert the Certificate File Extension on page 30

After you generate the certificate, you convert the certificate file extension from `.p7b` to `.pfx`. The certificate file extension must be `.pfx` for the Mirage Gateway server installation.

4 Configure the Mirage System to Work with SSL on page 31

After you convert the certificate file type, you configure the Mirage system to work with SSL.

5 Deploy the OVA Template in ESX on page 31

You must deploy the OVA template before installing the Mirage Gateway server.

6 Worksheet for Installing the Mirage Gateway Server on page 33

When you install the Mirage Gateway server, you are prompted to configure certain options. You must prepare your configuration options before you install the Mirage Gateway server.

7 Install the Mirage Gateway by Using the Configuration Web Portal on page 34

Install the Mirage Gateway server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

8 Install the Mirage Gateway Server by Using a Command Line on page 34

Install the Mirage Gateway server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

9 Install the Mirage Gateway Server Using an Input File on page 35

You can install the Mirage Gateway server with an input file that you edit before the installation procedure.

10 Upgrade the Mirage Gateway Server on page 35

You can upgrade the Mirage Gateway server from 5.0 to 5.1 by exporting your configuration settings from the 5.0 environment and importing them to the 5.1 environment.

Generate the Certificate Signing Request for the Mirage Gateway Server

When you set up the SSL certificate for the Mirage Gateway server, you must first generate the Certificate Signing Request (CSR).

You can use the OpenSSL tool or the MakeCert tool to generate the CSR.

Procedure

1 On the Mirage Management console, select **File > Add/Remove Snap-in**.

2 On the Add or Remove Snap-ins window, select **Certificates** and click **Add**.

3 On the Certificates snap-in window, select **Computer account** and click **Next**.

4 Select **Local computer** and click **Finish**.

5 Click **OK** in the Add or Remove Snap-ins window to close the window.

6 Expand the **Certificates (Local Computer)** node.

7 Expand the **Personal** node and right-click **Certificates**.

8 Select **All Tasks > Advanced Operations > Create Custom Request**.

9 Follow the prompts, and on the Select Certificate Enrollment Policy page, select **Proceed without enrollment policy** and click **Next**.

10 Verify the relevant information on the Custom Request page and click **Next** .

a Select **Legacy key** for the template type.

b Select **PKCS #10** for the request format.

11 Expand the **Details** drop-down menu and click **Properties**.

12 On the **General** tab of the Certificate Information page, type a certificate-friendly name.

You must use this name in the DNS record.

13 On the **Subject** tab, verify the relevant information.

Option	Description
Common name, value	The server FQDN. This is the certificate subject name that is used in the Mirage configuration to locate the certificate. The FQDN must point to that server and is validated by the client upon connection.
Organization, value	The company name. Usually required by the CA.
Country, value	A two-letter standard country name, for example, US or UK. Usually required by the CA.
State, value	The state name.
Locality, value	The city name.

14 On the **Extensions** tab, select the key-use information from the drop-down menus.

a Expand the **Key usage** drop-down menu, select **Data encipherment** and click **Add**.

b Expand the **Extended Key usage** drop-down menu, select **Server Authentication** and click **Add**.

15 On the **Private Key** tab, select the key size and export options.

Option	Description
Key Options	This is the required key size (usually 1024 MB or 2048 MB).
Make private key exportable	This option exports the CSR, and later the certificate, with the private key for backup or server movement purposes.
Key Type	Select **Exchange** (the default value is **Signature**).

16 Click **Apply** and then click **OK** to close the Certificate Properties window, and click **Next** in the Certificate Enrollment wizard.

17 On the Certificate Enrollment page, leave the default file format (Base 64), and click **Browse** to enter a file name and location for the CSR, and click **Finish**.

The certificate request is complete.

18 On the **Certificates Enrollments & Certificates** tab, click **Refresh**.

You can export the CSR with the private key for backup purposes.

What to do next

After generating the Certificate Signing Request, submit the CSR. See "Submit the Certificate Request," on page 30.

Submit the Certificate Request

After you generate the certificate signing request, you submit the request.

Procedure

1 Go to the external CA Web site and click **Request a certificate**.

2 On the Request a Certificate page, select **advanced certificate request**.

3 On the Advanced Certificate Request page, select **Submit a certificate request using a base-64-encoded CMC or PKCS #10 file or submit a renewal request by using a base-64-encoded PKCS #7 file**.

4 Open the `csr.req` file with a text editor and copy the text.

5 Paste the CSR text in the **Base-64-encoded certificate request** text box.

6 Select **Web Server** from the **Certificate Template** drop-down menu and click **Submit**.

7 On the Certificate Issued page, select **Base 64 encoded**, and then click **Download certificate**.

8 When prompted, select **Save As**, type the file name, and save the certificate as a `.p7b` file.

Convert the Certificate File Extension

After you generate the certificate, you convert the certificate file extension from `.p7b` to `.pfx`. The certificate file extension must be `.pfx` for the Mirage Gateway server installation.

Prerequisites

- Verify that you installed the Mirage server.
- Verify that you generated a certificate.

Procedure

1 Double-click the certificate and right-click **Install Certificate** to start the Certificate Install wizard.

2 Select **Place all certificates in the following store** and click **Browse**.

3 Select the **Personal** folder in the Select Certificate Store window, click **OK** to close the window, and click **Next**.

4 Verify the information for installing the certificate, and click **Finish**.

5 In the Windows MMC, expand the **Certificates** node followed by the **Personal** node, and then select **Certificates**.

6 Right-click the certificate and select **All Tasks > Export** .

7 Follow the prompts, select **Yes, export the private key**, and click **Next**.

8 Select the export file format.

   a Select the **Personal Information Exchange - PKCS #12 (.PFX)** check box.

   b Select the **Include all certificates in the certification path if possible** check box.

   c Click **Next**.

9 On the Security page, select the **Password** check box and enter a new password, confirm the password, and click **Next**.

10 Save the certificate.

   a On the File to Export page, click **Browse**

   b Locate and select the certificate, and save it as a `.pfx` file.

   c Click **Save**.

11 Follow the prompts to complete the export procedure.

The certificate is now installed on the Mirage server and configured for SSL.

Configure the Mirage System to Work with SSL

After you convert the certificate file type, you configure the Mirage system to work with SSL.

Prerequisites

Verify that you converted the certificate to the `.pfx` extension.

Procedure

1 In the MMC, expand the **Certificates** node, then expand the **Personal** node, and then select **Certificates**.

2 Double-click the **certificate** and on the **Details** tab, select **Subject.**.

   a Note the common name (CN) of the certificate.

3 On the **Details** tab, select **Issuer**.

   a Note the CN of the issuer.

4 In the Mirage Management console, expand the **System and Configuration** node and select **Servers**.

5 Right-click the **server** and select **Configure**.

6 Configure the server and click **OK**.

   a Select the **SSL** option.

   b Enter the CN of the certificate in the **Certificate Subject** text box.

   c Enter the CN of the certificate issuer in the **Certificate Issuer** text box.

Deploy the OVA Template in ESX

You must deploy the OVA template before installing the Mirage Gateway server.

The `.ova` file is located in the Mirage installation package.

Prerequisites

Verify that VMware ESX® is installed to deploy the OVA template.

Procedure

1 Double-click the `.ova` file and click **Run** to start the deployment wizard.

2 Provide login credentials for the ESX, and click **Login**.

3 In the ESX console, select **File > Deploy OVF Template** to start the deployment wizard.

4 Deploy the OVA template and click **Next**.

Option	Description
File	You can specify a location that is accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive. To select a file location, click **Browse**.
URL	You can type a URL to download and install the OVA package from the Internet.

After the OVA template is verified, a green check mark appears next to the publisher name.

5 Verify the OVA template details and click **Next**.

6 Accept the end user license agreement and click **Next**.

7 Enter a name, select a location for the deployed template, and click **Next**.

8 Select the host and cluster and click **Next**.

9 Select the resource pool and click **Next**.

10 Select a storage destination for the virtual machine files and click **Next**.

11 Select the disk format and click **Next**.

Option	Description
Thick Provision Lazy Zeroed	Create a virtual disk in a default thick format. Space required for the virtual disk is allocated when the disk is created. Data remaining on the physical device is not erased during creation, but is zeroed out on demand at a later time on first write from the virtual machine. Virtual machines do not read stale data from the physical device.
Thick Provision Eager Zeroed	Create a type of thick virtual disk that supports clustering features such as Fault Tolerance. Space required for the virtual disk is allocated at creation time. In contrast to the thick provision lazy zeroed format, the data remaining on the physical device is zeroed out when the virtual disk is created. It might take longer to create virtual disks in this format than to create other types of disks.
Thin Provision	Use this format to save storage space. For the thin disk, you provision as much datastore space as you expect the disk to require based on the value that you enter for the virtual disk size. However, the thin disk starts small and at first, uses only as much datastore space as the disk needs for its initial operations. If the thin disk needs more space later, it can grow to its maximum capacity and occupy the entire datastore space provisioned to it. Thin provisioning is the fastest method to create a virtual disk because it creates a disk with just the header information. It does not allocate or zero out storage blocks. Storage blocks are allocated and zeroed out when they are first accessed.

12 Complete the deployment wizard.

The OVA template is deployed.

Worksheet for Installing the Mirage Gateway Server

When you install the Mirage Gateway server, you are prompted to configure certain options. You must prepare your configuration options before you install the Mirage Gateway server.

Table 3-3. Configuration Options for Installing the Mirage Gateway Server

Option	Action	Your Value
LDAP type	You can select either **LDAP** or **LDAPS**. The default value is LDAP.	
LDAP server address	You can type either the LDAP server or the IP address, for example, ldap.yourcompany.com, or, ldapIPaddress.	
LDAP server port	The default port is 389. Verify that your firewall settings allow the selected port.	
LDAP user DN to bind Mirage Gateway with the LDAP server	This follows the format: cn=username, cn=users, dc=domain, dc=com For example: `CN=Administator, CN=USERS, DC=MIRAGEDOMAIN, DC=COM`	
LDAP bind user password	This is your password.	
Token expiration time (in hours)	The default is 168 hours.	
Mirage server address	You can type either the hostname or the IP address, for example, *mirageserver*.*yourcompany*.com The default is *mirageserver*.*yourcompany*.com.	
Mirage server port	The default is 8000. Verify that your firewall settings allow the selected port.	
Mirage Gateway activation code	You create the activation code during the installation. The activation code must contain at least 8 characters, including a number, an upper-case character, a lower-case character, and a special character.	
Certificate file	This follows the format: `/opt/MirageGateway/certificatename.pfx` or `/opt/MirageGateway/certificatename.pem`	
Certificate private key password	The password you created as part of the certificate export procedure.	

Install the Mirage Gateway by Using the Configuration Web Portal

Install the Mirage Gateway server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

Linux is case sensitive.

Prerequisites

- Verify that you installed the following Mirage components:
  - Mirage server
  - Mirage Management server
  - Mirage Management console
- Create a bind user to authenticate the communication request between the client and the Mirage servers.
- Deploy the OVA for Mirage 5.1 Gateway server.

Procedure

1 In the ESX console, power on the VM.

2 Navigate to https://*MirageGWIPaddress*:8443/WebConsole, where *MirageGWIPaddress* is the IP address of the Mirage Gateway server.

3 When prompted, provide the login credentials.

The default username is **`mirage`**, and the default password is **`vmware`**.

4 Follow the prompts to install the Mirage Gateway server.

Use the configuration information that you gathered in the worksheet.

The Mirage Gateway server is installed and available in the Mirage Management console.

Install the Mirage Gateway Server by Using a Command Line

Install the Mirage Gateway server to secure your data center environment for users that communicate with the corporate enterprise data center via Internet.

Linux is case sensitive.

Prerequisites

- Ensure that you installed the following Mirage components:
  - Mirage server
  - Mirage Management server
  - Mirage Management console
- Create a bind user to authenticate the communication request between the client and the Mirage servers.
- Add your company's DNS server IP address to the top of the `/etc/resolv.conf` file. In the `/etc/resolv.conf` file, type **`nameserver`** ***`IP address`***, where *IP address* is the IP address for the DNS server. You can use the Linux *vim* text editor, or WinSCP to use a Windows text editor. If you use WinSCP to edit the file, use the username *root* and the password *vmware*. If you cannot use your company's DNS server, then you must add a DNS record to the `/etc/hosts` file.

Procedure

1 In the ESX console, power on the VM.

2 On the **Console** tab, press **Enter**.

3 When prompted, provide the login credentials.

The default username is **mirage**, and the default password is **vmware**.

4 To start the installation, run the `sudo /opt/MirageGateway/bin/install.sh` command.

5 Follow the prompts to install the Mirage Gateway server.

Use the configuration information that you gathered in the worksheet.

The Mirage Gateway server is installed and available in the Mirage Management console.

Install the Mirage Gateway Server Using an Input File

You can install the Mirage Gateway server with an input file that you edit before the installation procedure.

Prerequisites

Use the configuration information that you gathered in the worksheet to install the Mirage Gateway server to edit the configuration text file. See "Worksheet for Installing the Mirage Gateway Server," on page 33.

Procedure

1 Edit the configuration text file with a text editor.

Option	Description
vim	Use this option to edit the text file with the Linux text editor.
WinSCP	Use this option to edit the configuration text file with a Windows text editor, such as notepad. The configuration file is located on the Linux server panel. The file path for the configuration file is `/opt/MirageGateway/etc/config.txt`.

2 To install the Mirage Gateway server with the input file, run the install command.

`sudo /opt/MirageGateway/bin/install.sh –f /opt/MirageGateway/etc/updatedconfigfile.txt` where *updatedconfigfile.txt* is the name of the configuration text file you created.

For example, `sudo /opt/MirageGateway/bin/install.sh –f /opt/MirageGateway/etc/config.txt`

The Mirage Gateway server is installed and available in the Mirage Management console.

The password is removed from the input file.

Upgrade the Mirage Gateway Server

You can upgrade the Mirage Gateway server from 5.0 to 5.1 by exporting your configuration settings from the 5.0 environment and importing them to the 5.1 environment.

You can use the WinSCP tool to copy files from one environment to another environment.

When you copy or save files, scripts, and so on between environments, for example, from Mirage 5.0 to Mirage 5.1, you must save them to the same folder in both environments.

Prerequisites

- Verify that you installed the following Mirage components:
  - Mirage server

- Mirage Management server
- Mirage Management console

- Create a bind user to authenticate the communication request between the client and the Mirage servers.
- Add your company DNS server IP address to the top of the `/etc/resolv.conf` file. In the `/etc/resolv.conf` file, type **`nameserver`** ***`IP address`***, where *IP address* is the IP address for the DNS server. If you cannot use your company DNS server, then you must add a DNS record to the `/etc/hosts` file.
- Deploy the OVA for Mirage 5.1 Gateway server.

Procedure

1 In the ESX console, power on the VM.

2 On the **Console** tab, press **Enter**.

3 When prompted, provide the login credentials.

The default username is **`mirage`**, and the default password is **`vmware`**.

4 Navigate to the `/opt/MirageGateway/bin` folder and copy the `export.sh` script from the Mirage 5.1 environment to the Mirage 5.0 environment.

5 Run the `sudo /opt/MirageGateway/bin/export.sh` script in the Mirage 5.0 environment, and when prompted enter a password.

The `config.tar.gz.enc` file is generated.

6 Copy the `config.tar.gz.enc` file from the VM to your desktop.

7 Navigate to https://*MirageGWIPaddress*:8443/WebConsole/configuration.html, where *MirageGWIPaddress* is the IP address of the Mirage Gateway server in the Mirage 5.1 environment, and when prompted, provide the login credentials.

The default username is **`mirage`**, and the default password is **`vmware`**.

8 Click the **Import Settings** tab on the left and follow the prompts to import the `config.tar.gz.enc` file.

The Mirage 5.1 Gateway server is now available in the Mirage Management console.

Installing the Mirage Client

You can install the Mirage client installer using the Mirage 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 re-installation of the client.

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

Install the Mirage Client Using the Active Installer

You can install the client using the Mirage Management console.

The `.msi` installation file is located in the 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 Mirage servers in your DMZ premises, you must use a VPN to connect clients that are used outside the network.

4 You must configure SSL on both the Mirage client and the Mirage server for the clients to connect using SSL.

Procedure

1 Double-click the `.msi` file for your environment to start the installation wizard.

Option	Description
64-bit	`MirageClient.x64.`*`buildnumber`*`.msi`
32-bit	`MirageClient.x86.`*`buildnumber`*`.msi`

2 Follow the prompts until you come to the server settings page, type the server settings, and then click **Next**.

Option	Action
IP or FQDN of server	Type the IP address or FQDN of the Mirage server or the shared IP of the load balancer in a cluster that 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 port (the default port is 8000).
Use SSL to connect to the server option	Select this option to enable SSL if your server is configured for SSL use, and type the required SSL port.

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

4 (Optional) Restart your computer.

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

After the 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 Mirage Client Silently

The administrator can deploy the 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 Mirage servers in your DMZ premises, you must use a VPN to connect clients that are used outside the network.

4 You must configure SSL on both the Mirage client and the Mirage server for the clients to connect using SSL.

Procedure

1 Select **Start > Run**, type **`cmd`**, and click **OK**.

2 Type the required expression for your environment and press **Enter**.

Option	Description
32-bit clients	`<Mirage MSI path>\MirageClient.x86.buildnumber.msi SERVERIP=MirageServer /quiet` *SERVERIP* is the FQDN, hostname, or IP of the Mirage server or shared IP of the load balancer.
64-bit clients	`<Mirage MSI path>\MirageClient.x64.buildnumber.msi SERVERIP=MirageServer /quiet` *SERVERIP* is the FQDN, hostname, or IP of the Mirage server or shared IP of the load balancer.

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

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

What to do next

Verify that SSL is enabled on the Mirage server.

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

Install the Mirage PowerCLI

VMware Mirage PowerCLI provides an easy-to-use Windows PowerShell interface for command-line access to administration tasks.

The `.msi` installation file is located in the Mirage installation package.

Prerequisites

- Verify that you installed Microsoft PowerShell 1.0.
- Verify that you installed .NET 3.5 or later.
- If you already installed an earlier version of the Mirage PowerCLI, uninstall the earlier version.

Procedure

1 Double-click the `.msi` file for your environment to start the installation wizard.

Option	Description
64-bit	`VMwarePowerCLIForMirage.x64.msi`
32-bit	`VMwarePowerCLIForMirage.x86.msi`

2 When prompted with the Execution Policy window, access Windows PowerShell as an administrator, and run the `Set-ExecutionPolicy RemoteSigned` command.

3 Type **`Y`** and press **Enter** to accept the execution policy change, and close the Window PowerShell window.

4 Follow the prompts to complete the installation wizard.

Managing Mirage Software Licenses

The Mirage Management server requires a license. The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement.

Individual Mirage servers do not need licenses.

Software licenses are separate from the server installation package.

You can view the license details at any time. See "Add and View Licenses," on page 39.

When a license expires, all management actions are disabled. However, the administrator can still view the system status and track operation status. Mirage endpoint-related functions, including backup, restore, and image management operations continue, so that clients can still upload changes to the CVD on the server.

When a license expires, or when you install the Mirage system, a dialog box appears when you open the Mirage Management console, where you can type the license key. An audit event is created.

When you need a new license, contact VMware.

Add and View Licenses

The license file enforces the number of CVDs that you can run on your system and the duration of the license agreement. You can view the current license details at any time.

You can add a license or view the number of CVDs currently licensed and the license expiry date through system configuration settings.

If your license expires, or when the system is installed, when you open the Management console a dialog box appears where you can type the license key.

You do not need to restart the Mirage Management server to update the license.

Procedure

1 In the Management console tree, right-click **System Configuration**, select **Settings**, and click the **License** tab.

2 Type or copy and paste the serial key in the **Use license key** text box.

3 Click **OK**.

Configure the Environment for Endpoints

Before you can attach endpoints to your system, you need to perform a minimum configuration, which includes configuring the Web URL for the file portal, importing USMT settings, and performing domain joining operations.

For information about importing USMT files, see Import USMT Settings.

For join domain account information, see General System Settings.

Prerequisites

Verify that a Mirage server is installed.

Procedure

1 (Optional) Configure the file portal Web URL.

2 (Optional) To perform migration operations, import the USMT folder.

3 (Optional) To perform domain joining operations, provide join domain account details.

What to do next

You can now configure and use your Mirage system.

Index

U

W