Deployment and Design Considerations for VMware Mirage

VMware Mirage 5.7

WHITE PAPER

vmware®

Table of Contents

Introduction

This paper describes best practices for planning a VMware Mirage™ deployment, especially the primary phases, which include sizing and design considerations and gathering of environmental data.

Every Mirage deployment is unique, so unless your environment contains fewer than 1,000 endpoints, it is useful to consult the VMware Professional Services Organization (PSO) or partners for assistance. You can find an extensive list of resources in the References section of this paper. The following items have also proved to be useful:

- For a thorough overview of Mirage functionality, see the VMware Mirage 5.0 Reviewer's Guide.
- For more information on installing Mirage, see the VMware Mirage Getting Started Guide and the VMware Mirage Installation Guide.
- For more information on configuring Mirage, see the VMware Mirage Administrator's Guide and the VMware Mirage Web Management Guide.
- See also the VMware Mirage Large-Scale Reference Architecture.

Audience

This information is meant to help anybody considering or in the early stages of a Mirage deployment, such as IT administrators and design architects. The reader should be familiar with Windows data center technologies such as Active Directory, SQL, and Microsoft Management Console (MMC).

System Architecture

Mirage provides centralized image management for physical desktops and for View virtual desktops in VMware Horizon® 6.

Mirage provides enhanced backup, recovery, updates for endpoints, and migration functionality for hardware and operating systems. These functions centralize endpoint content in the data center for better protection and easier management, download images to endpoints, and optimize the data transfer. Network compression of up to 30 percent and data deduplication also reduce the network traffic load.

Mirage supports the following Interactions between the data center and managed endpoints on the LAN, especially in distributed environments:

- A Mirage client installed on each endpoint communicates with a Mirage server or a cluster of Mirage servers.
- Base and app layer updates are downloaded to endpoints as scheduled by IT.
- Changes to endpoints are uploaded to the data center to keep centralized desktop images synchronized with endpoints. Either the user or IT can initiate these changes.

Mirage components integrate well with typical distributed infrastructures:

- Mirage clients connect to a Mirage server, either directly or through a load balancer or Mirage Gateway. The Mirage servers and the Mirage Management servers share access to the Mirage database and storage volumes.
- The administrator connects to the Mirage Management server.

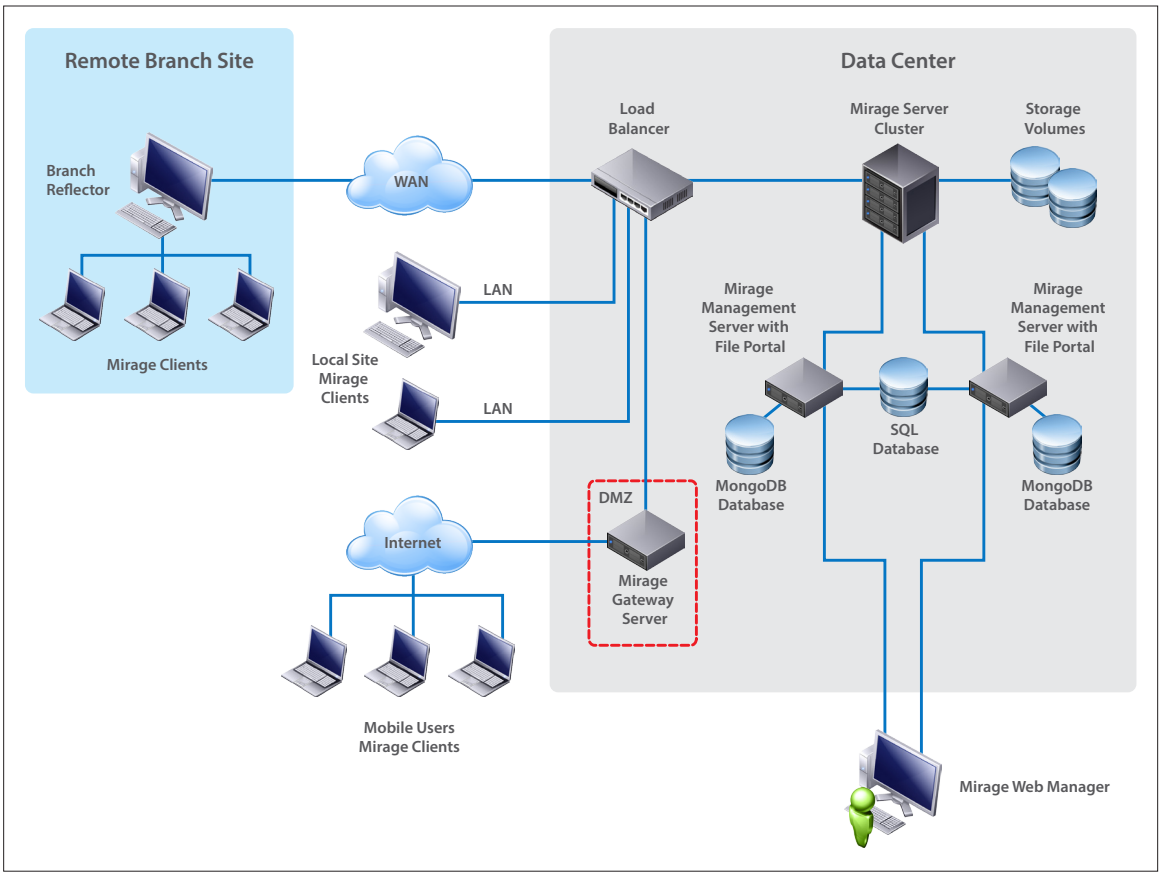

Figure 1: Mirage System Components in a Distributed Infrastructure

For a closer look at the Mirage system architecture, see the VMware Mirage Administrator's Guide and the VMware Mirage Installation Guide. For a description of remote branch functionality, see Branch Reflectors.

System Components

Mirage components in the data center connect to endpoints over a WAN, LAN, or Internet connection. Each endpoint corresponds to a centralized virtual desktop (CVD), a desktop image stored in the data center.

Mirage components are described in Table 1.

COMPONENT	DESCRIPTION
Mirage client	Enables an endpoint to be managed by Mirage. The Mirage client manages uploads and downloads between the centralized virtual desktop (CVD) and the endpoint. The Mirage client supports both physical and virtual desktops.
Mirage Management server	Controls and manages the Mirage server cluster. Use at least two Mirage Management servers to increase Mirage cluster availability in case the primary Mirage Management server fails.
Mirage server	Synchronizes data between Mirage clients and the data center. Manages the storage and delivery of base layers, app layers, and CVDs to clients. Consolidates monitoring and management communications. **Note:** Although a Mirage server can run on the same machine as the Mirage Management server, it is good practice to keep the Mirage server on a dedicated physical or virtual machine.
Mirage Console	Provides the user interface (UI) for the Mirage Management server, and allows administrators to manage Mirage server deployment functions. The Mirage Console is installed as an MMC snap-in or a Web application. Wizards enable the administration of common Mirage functions.
Mirage database	Contains information about the base and app layers, the driver library, CVDs in storage, endpoint configurations, and communication between the Mirage Management server and Mirage servers.
Mirage storage	Includes files uploaded from the endpoints. Files are deduplicated in single-instance storage (SIS). The Mirage storage array is accessible from any Mirage server.
Mirage branch reflector (optional)	Serves as a local Mirage update service for peer PCs in branch-office environments, reducing the time and network bandwidth requirements for base-layer deployment and endpoint migration. Any endpoint can be configured as a branch reflector.
Mirage Gateway (optional)	Provides users with secure communication to Mirage servers without using a VPN. It is deployed in the DMZ outside the data center environment.
Mirage file portal (optional)	Archives historical snapshots of user files and folders. Users can access this read-only data from any device with a Web browser.
Mirage Web Manager	Provides some of the administrative functions in the Mirage Console. Administrators in a help-desk role can use this Web-based tool to resolve endpoint issues.
MongoDB Database	Used to store small files, to reduce IOPS and upload time. A MongoDB instance is installed with each Mirage Management server. Install additional Mirage Management servers for a fault-tolerant deployment. Mirage replicates the MongoDB database on other Mirage Management server instances.

Table 1: Mirage System Components

For more information about individual Mirage components, see the *Mirage System Components* section of the VMware Mirage Getting Started Guide.

Mirage Concepts

The Mirage-related terms used in this paper are listed in Table 2.

TERM	DESCRIPTION
App layer	A template for deploying one or more applications to specific endpoints. An app layer requires a base layer on the endpoint. You can update an app layer and base layer independently.
Base layer	A template for deploying common desktop contents to specific endpoints. A base layer can include the operating system, service packs and patches, and core enterprise applications and their settings.
Centralization	Backing up of endpoint contents and all protected files to the data center, where they can be managed centrally.
Centralized virtual desktop	The image backup of an endpoint. The end user performs functions on an endpoint locally, and all changes to the endpoint are backed up to the CVD.
Endpoint	A physical or virtual machine on which the Mirage client is installed. Endpoints communicate with a Mirage server.
Mirage cluster	A collection of Mirage servers managed by a single Mirage Management server.
Mirage driver library	A set of Windows device drivers that are downloaded to each endpoint based on the endpoint's hardware requirements and assigned driver profiles. A driver library eliminates the need to create a base layer for each hardware type. You can create a single hardware-independent base layer for all endpoints. Note: You cannot share driver libraries between Mirage clusters. If you deploy multiple Mirage clusters, you must manually synchronize the Mirage driver libraries. For more information, see Managing Multiple Mirage Clusters.
Mirage reference machine	An endpoint managed by an administrator that is used to capture base layers. Before capturing a base layer, you must create a reference CVD for the Mirage reference machine.
Mirage reports	The reports provide health and progress status of the Mirage environment. For example, the Data Protection Status report shows the percentage of users' systems that are backed up. The OS Migration Progress displays the number of CVDs that have started, are still pending, or have completed an OS migration during a specified time frame. For a list of Mirage reports and their definitions, see the *Working with Reports for Mirage Operations* section of the VMware Mirage Web Management Guide. All Mirage reports can be accessed through the Mirage Web Manager (see Figure 2).
Mirage transaction logs	A history of Mirage functions that includes the actions performed and whether they completed successfully.
Steady state	The status of an endpoint and its CVD after centralization.

Table 2: Mirage Concepts and Terminology

Mirage reports are illustrated in Figure 2.

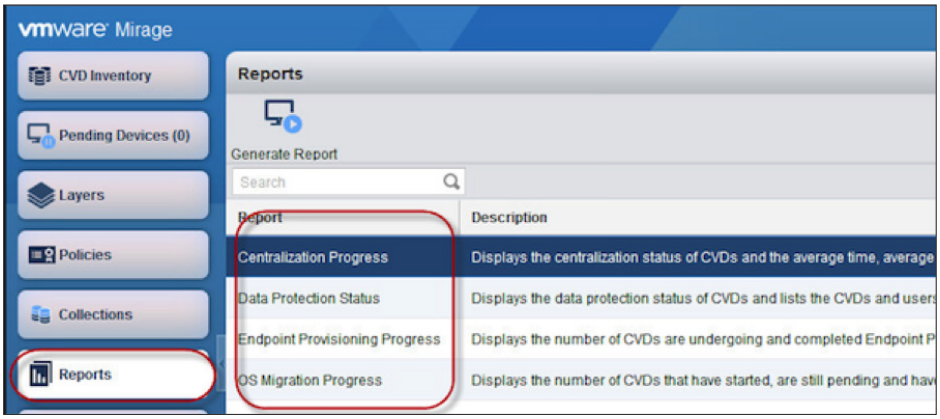

Figure 2: Mirage Reports on the Mirage Web Manager

Use Cases

Mirage provides centralized image management for physical and virtual desktops, including endpoint backup, recovery, and updating, as well as hardware and operating system migration. Mirage supports image management of virtual endpoints exclusively in a View in Horizon 6 environment. For more information, see the *Supported Mirage Operations* section of Image Management for View Desktops using VMware Mirage.

Mirage addresses the following use case scenarios:

- **Desktop recovery and repair** – Mirage stores full desktop images in the data center and keeps them synchronized with user changes. The default snapshot interval is once per hour. Periodic endpoint snapshots allow IT to recover partial or full desktops and to access previous versions of a file or folder. This feature enables
  - Quick delivery of a desktop to a user, including applications and data, to replace a lost or broken endpoint
  - Retention of all changes made to an endpoint that gets disconnected from the corporate network
  - Restoration of a previous version of a file, directory, application, or operating system in the event of accidental deletion or software malfunction
  - Access to files from anywhere through the Mirage file portal
- **Simplified Windows OS migrations** – Mirage enables in-place migration of endpoints from one OS to another, such as to a later version of Windows, as well as migration of endpoints between hardware platforms, without impacting users. For more information, see the *Migrating to Windows OS Replacement Devices* section of the VMware Mirage Administrator's Guide.
- **Endpoint management and app layering** – Mirage enables remote management of physical or virtual desktops as a set of logical application and base layers. You can update layers while maintaining user files and personalization. You can also deploy or remove applications from one or more endpoints. This feature enables you to
  - Assign a single base layer and optional multiple app layers to endpoints and automatically synchronize the full image with all associated endpoints
  - Update or delete layers from endpoints
  - Enforce all layers without overwriting user-installed applications, data, or preferences
- **Branch-office optimization** – Updates can be downloaded once from the Mirage server to the branch reflector instead of individually to each endpoint. Peer-to-peer updates from the branch reflector to other Mirage clients in the branch office conserve data center and network resources.

For a more detailed description of Mirage functionality, see the Mirage Overview video.

Because Mirage is a multidimensional product with many capabilities, not all of which are used in every scenario, each deployment is unique. Mirage can address multiple use cases at the same time, and use cases can be modified to fit specific requirements.

The first step of a Mirage deployment is to determine which use cases, and associated requirements, need to be addressed. For example, for a large hardware migration, consider the network traffic and storage IOPS caused by this activity. For occasional restore operations, however, network traffic and storage IOPS are less important considerations because they do not affect system sizing. After you determine the use cases and associated requirements, survey the environment and collect data to size and design your Mirage deployment accordingly.

Surveying the Environment and Accumulating Data

It is important to gather the appropriate environmental data to size and design a Mirage deployment accurately. VMware recommends Liquidware Labs Stratusphere FIT or Lakeside Software SysTrack as appropriate tools to collect much of this data.

Endpoint Properties

First, you need to know the number of endpoints and each endpoint's specifications.

Number of Endpoints
When you calculate the total number of endpoints to be included in your Mirage-managed environment, include all endpoints, not just those you expect be connected concurrently.

To calculate the number of endpoints quickly, view the entries in your DHCP server. In most cases, DHCP data provides an accurate endpoint count. Alternatively, you can use an IP scanner tool, although most security solutions block IP scanners.

When you know the number of endpoints in your environment, you can estimate the number of Mirage servers to allocate—along with network bandwidth, storage performance and capacity—and whether to use more than one Mirage cluster.

Centralization Schedule
Knowing the number of endpoints in your environment, and when they are online and connected to the network, helps to approximate the amount of time needed to complete centralization. This information helps you schedule a convenient window of time for centralization.

You can optimize endpoint connectivity by enlisting group policies that prevent machines from automatically disconnecting from the network. You can also deploy a Mirage Gateway to maximize connectivity.

Another factor to consider when determining a centralization schedule is the ratio of laptops to desktops. If your environment contains more laptops than desktops, you might need to extend the centralization schedule, because laptops are online less frequently and not necessarily during typical business hours.

Endpoint Information
Gather all information regarding the individual endpoints, including make, model, CPU, RAM, OS, and hard disk. You need this information to build driver libraries that reside in the data center.

A driver library is essential to restoring a CVD to a new machine or performing an OS migration. You must use an image that includes the appropriate drivers for each endpoint.

Endpoint information is also used to determine how many of them require hardware migration. Many endpoints that can run Windows XP cannot run Windows 7 or later. Additionally, many endpoints in your environment might be incompatible with newer versions of the applications included in either your base layer or app layers. Therefore, you might need to provision users with new endpoints.

By consulting the specifications of each endpoint, you can determine how many of them need to be replaced. You can then use Mirage to migrate data from an old physical endpoint to a new one. The data migration includes applications, files, folders, and settings.

Endpoint Applications

Compiling an application inventory for your environment, including each endpoint, is essential to ensure application compatibility during OS migration. It is also useful in provisioning new endpoints or replacing lost or stolen ones.

A comprehensive application inventory is also useful in determining which applications to assign to base layers and which to app layers. Infrastructure applications, such as Microsoft Office and antivirus software, are assigned to the base layer and deployed to all or most endpoints. Less common applications are assigned to app layers and deployed to individual endpoints or to groups of endpoints with similar needs and users.

User Data on Endpoints

Determine how much data is stored across all endpoints. The amount of data uploaded to the Mirage server determines how much server storage is required and the length of time needed for a centralization schedule.

Data uploaded to the Mirage server from each endpoint is stored in an associated CVD. CVD sizes vary from one organization to another, depending on work culture, infrastructure resources, and other factors. The best way to size your environment is to perform a centralization pilot with a representative sample of your organization's endpoints.

When the centralization process is complete, check the used space in Mirage storage, then extrapolate the total amount of server storage required. Typically, you can use a relatively small sample to determine the average CVD size. The average pre- and post-deduplication CVD size for a representative sample of 150 endpoints is almost the same as the average size for a full deployment of 10,000 or more endpoints. For more information on how to calculate storage requirements, see Storage Capacity.

Endpoint Security Measures

Determine which security products are in use in your environment and how many endpoints use each product. Security products that provide disk encryption, antivirus solutions, and personal firewalls can affect centralization and OS migration. Mirage is compatible with many, but not all, popular security products. For more information on which security products are compatible with Mirage, see the latest Mirage release notes.

If your environment includes security products incompatible with Mirage, you might be required to create exclusions for some or all of them.

For more information on the impact of some security products on Mirage and how to resolve associated issues, see the following VMware knowledge base articles:

- Configuring antivirus and computer protection software exclusions for VMware Horizon Mirage
- Limitations of using VMware Mirage to manage endpoints protected by Kaspersky Endpoint Security
- Limitations of using VMware Mirage to manage endpoints protected with Sophos SafeGuard full disk encryption

For further information, consult VMware PSO, partners, or VMware Global Support Services (GSS).

Personal Firewalls

If users have personal firewalls installed on their endpoints, connections between Mirage clients and the Mirage server can be disrupted. Endpoints with active firewalls cannot upload data or be migrated, so they cannot be managed by Mirage.

Workarounds include setting Mirage as an authorized service in the firewall settings, opening a port between the client and the server, and temporarily disabling a user's personal firewall.

Antivirus Software
Some antivirus applications label Mirage as a threat and prevent the execution of Mirage operations. For example, writing system files during a restore or migration operation can be blocked by an antivirus application that is trying to protect critical files.

Work with your security team to establish Mirage as an approved antivirus exception.

Disk Encryption
Mirage has been tested to work with Check Point, Symantec, McAfee, Sophos, Becrypt, and BitLocker disk encryption software.

When performing the OS migration of an endpoint that has disk encryption, decrypt the endpoint, perform the migration, and then re-encrypt it after the migration has been completed.

Note: This procedure is not required with Sophos disk encryption.

Network Topology

Determine the location of all endpoints, how they are connected to the network, and the amount of bandwidth available to each. This information helps you to estimate the length of time required for a centralization schedule and to determine whether you need to provision multiple clusters of Mirage servers. For example, centralization over a WAN takes much longer than centralization over a LAN, and some sites might need additional bandwidth or a Mirage Gateway.

Consult your networking team to see if they have already mapped the network topology. For more information, see Managing Multiple Mirage Clusters.

Architecture Planning

This section discusses best practices for planning your Mirage deployment according to the specifications collected in Surveying the Environment and Accumulating Data.

Mirage Cluster

A Mirage cluster is a collection of Mirage servers managed by a single Mirage Management server. The following components are included in a Mirage cluster:

- Two Mirage Management servers, each with a local MongoDB database
- One Mirage database based on Microsoft SQL
- One or more Mirage servers
- Single Mirage storage array, organized into one or more storage volumes
- One or more file portal servers (optional)
- One or more Mirage Web Manager servers
- Load balancer (optional)
- One or more Mirage Gateways (optional)

For more information, see System Components.

Note: All Mirage cluster components must be installed within the same LAN. For example, it is not possible to install Mirage storage and servers in a branch office and the Mirage Management server in the data center. Endpoints, including branch reflectors, can be installed remotely, but servers cannot.

Multiple Mirage Clusters

Mirage does not provide centralized management for multiple Mirage clusters. Each cluster must be deployed and managed separately.

A single cluster is recommended in most environments; however, multiple Mirage clusters are recommended in the following cases:

- **Low data-center upload bandwidth** – Deploy multiple Mirage clusters if there is not enough upload bandwidth in a single cluster within a data center to support centralization and steady-state operations. (Bandwidth requirements are discussed in detail in the Network section.)
- **More than 20,000 CVDs** – A single Mirage cluster supports up to 20,000 CVDs. Deploy multiple Mirage clusters if the number of CVDs is larger than 20,000.
- **Multiple geographical regions** – Deploy multiple Mirage clusters if data transfer between geographical regions is restricted for legal or security reasons.

Managing Multiple Mirage Clusters

Each Mirage component must belong to a single Mirage cluster. Components cannot be shared between clusters, and data cannot be automatically shared between clusters. Therefore, if you deploy multiple Mirage clusters, you must synchronize the following data manually:

- Base layers and app layers, using `Wanova.Server.Tools.exe ExportLayers` and `Wanova.Server.Tools.exe ImportLayers`
- Master policy, using `Wanova.Server.Cli.exe` and `getFactoryPolicy`
- CVD policies, using the Mirage Web Manager to import and export
- Driver libraries and profiles, using `Wanova.Server.Tools.exe DriverLibraryCloner`
- Dynamic collections
- Cluster settings (such as snapshots and User State Migration Tool)
- Scripts and customizations

Mirage Servers

A Mirage server manages the upload of data from endpoints to their respective CVDs, which are stored in Mirage storage, and the download of layers and drivers to endpoints.

Note: You can deploy a Mirage server to either a physical or virtual machine. There is no performance difference between physical and virtual Mirage servers.

Host Hardware and Software Requirements

The server where a Mirage server is installed must meet certain requirements. Table 3 lists two tested options.

OPTION	CPUS FOR PHYSICAL MACHINES	VCPUS FOR VIRTUAL MACHINES	RAM	SUPPORTED ENDPOINTS IN STEADY STATE
Option 1: 8/16	4 cores	8 vCPUs	16 GB	1,500
Option 2: 4/8	8 cores	4 vCPUs	8 GB	1,000

Table 3: Two Tested Options for Mirage Server Hosts

The following requirements apply to both options listed in Table 3:

- Hard disk – 200 GB local disk (RAID 0 or 1) for OS, plus local cache. You can reduce the size if a network cache is not needed in the following cases:
  - Layer management only (no centralization)
  - LAN deployment only
- Network – Two Gigabit Ethernet ports.
- Ports – It is recommended that you separate the endpoint and storage networks and use a different dedicated port for each network.
- Operating system – Windows Server 2008 R2 Standard, Windows Server 2008 Enterprise Edition 64-bit, and Windows Server 2012 Standard Edition 64-bit are supported.
- Microsoft .NET Framework 4.5.1 or later.
- The server must be in a domain.

Number of Mirage Servers
When calculating how many Mirage servers you need, consider the following:

- One Mirage server can support
  - Up to 1,000 CVDs in a 4 vCPU configuration with 8 GB of RAM
  - Up to 1,500 CVDs in an 8 vCPU configuration with 16 GB of RAM
- For deployments with more than 1,000 endpoints, an extra Mirage server is needed.
- An extra Mirage server is required for resiliency in a production environment.

The calculation for the recommended number of Mirage servers is

$$Ne / Se + 1$$

where **Ne** is the total number of endpoints, and Se is the supported number of endpoints in a steady state per Mirage server, as determined by the Mirage server installation option selected.

Note: Regarding steady-state operations, a Mirage server *can* support up to 1,500 endpoints. However, if multiple endpoints are being centralized concurrently, the number might fall to fewer than 400 concurrent active endpoint centralizations per Mirage server. Therefore, depending on the operation, the number of endpoints supported by a single Mirage server can vary widely.

Mirage Management Server

Two Mirage Management servers control and manage the Mirage server cluster. Each Mirage Management server includes a MongoDB database instance, where it stores all small files from endpoints to reduce storage IOPS and upload time.

Note: You can deploy a Mirage Management server to either a physical or virtual machine. There is no performance difference between physical and virtual Mirage Management servers.

When provisioning a Mirage Management server, consider the requirements in the following subsections.

Hardware Requirements
- Processor:
  - 1 Quad-core processor 2.26 GHz in a physical configuration or
  - 4 vCPUs in a virtual configuration
- 8 GB RAM
- Two Gigabit Ethernet ports
- Local dedicated disk drive or SAN LUN for MongoDB
  - At least 250 GB of free space
  - 600–1000 IOPS

Note: A new Mirage installation may require you to increase the amount of disk space, so this disk should be expandable. For more information on disk size calculations, see Mirage MongoDB location and sizing best practices.

Software Requirements

• The following operating systems are supported:

- Windows Server 2008 R2 with SP1 Standard or Enterprise Edition, 64-bit
- Windows Server 2012 Standard Edition, 64-bit
- Windows Server 2012 R2 Standard or Datacenter Edition, 64-bit

• Microsoft .NET Framework 4.5.1 or later.

• The server must be part of the Active Directory domain.

MongoDB File Location

Place MongoDB files on a dedicated local drive or SAN LUN to avoid the possibility of data corruption or loss. If you cannot designate a local drive or SAN LUN for MongoDB database files, then designate a dedicated NAS volume on higher-end storage with lower latency to minimize disconnects between MongoDB and the MongoDB files. Do not allocate CVDs on the same volume as the MongoDB.

Although it is possible to use a Mirage shared volume, this option is not recommended for MongoDB.

Important: In Mirage 5.4, the MongoDB database was stored in shared volumes. Beginning with Mirage 5.5, however, local storage is recommended for the MongoDB database, so the MongoDB database is not moved automatically during an upgrade from Mirage 5.4 to Mirage 5.5. If you have Mirage 5.4, move the MongoDB database to a more stable location before performing an upgrade.

For additional information, contact VMware PSO, partners, or VMware Global Support Services (GSS), or see the following VMware knowledge base articles:

• Changing the location of MongoDB when in use by Mirage

• Mirage MongoDB location and sizing best practices

Free Space

For a new Mirage installation, allocate at least 250 GB of free space on a local dedicated drive. For existing installations, dedicate an amount of local disk space equivalent to five percent of the space used by Mirage volumes.

Number of Management Servers

In most cases, two Mirage Management servers provide sufficient availability and resiliency for a successful deployment.

Mirage Storage

Mirage uses storage for CVDs, layers, driver libraries, and related data.

Storage Architecture

In a test environment or an environment with fewer than 1,000 CVDs, you can use a single Mirage server and deploy the following storage types:

- Direct-attached storage
- SAN connected through iSCSI or Fibre Channel
- Network-attached storage (NAS) connected through iSCSI, Fibre Channel, or CIFS network share

In a large production environment, however, you are likely to need multiple Mirage servers, each of which requires access to the entire storage array. In a large environment, use storage that meets the following requirements:

- NAS is connected through SMB, SMB2, or SMB protocols.
- NAS devices must support Alternate Data Streams.

  To verify, you can use the `Wanova.Server.Tools.exe NasCompatibilityTest` command.

  Note: NFS is not supported.

For example, the following devices, which meet these requirements, are currently being used by organizations with multiple Mirage servers:

- EMC VNX and Isilon OneFS
- NetApp with Data ONTAP
- Hitachi HNAS with BlueArc

For deployments up to 3,000 endpoints, you can use any of these devices or separate Windows servers configured in a file-server role (Windows NAS). Windows 2012 Server, which supports SMB 3.0, is highly recommended for this purpose. A single Windows file server can support up to 2,000 endpoints, but consider lowering the number of endpoints when there is a large amount of data per CVD.

Storage Capacity

The storage needed by a CVD varies greatly. The average post-deduplication size of a CVD can range from 9 GB to 48 GB per endpoint.

To determine the required storage capacity:

1. Run a pilot project with 150 endpoints, representing the different types of users in your environment, such as task workers, heavy users, roaming users, and office workers; and departments, such as Sales, Legal, and IT.
2. After centralization, run the StorageReports tool.

```
Wanova.Server.Tools.exe StorageReports StoragePath C:
\MirageStorage –OutputDir C:\Reports
```

3. Identify the file types and directories that use large amounts of storage, such as media files, mobile phone backups, and archived files, so that you do not have to migrate them.
4. Update the upload policy and sync all endpoints.
5. Make sure no snapshots are left.
6. Calculate the average CVD size by dividing the occupied space by the number of CVDs.

7. Add 30 percent for snapshots (for the default snapshot policy).
8. Add 20 to 30 percent for natural growth in areas such as the number of employees and the typical size of hard drives, assuming that the organization is growing and that storage becomes less expensive.

Note: For a quick estimate, begin with 20 GB per endpoint.

Storage Performance

The main consideration for storage performance in a Mirage deployment is data upload speed. Consider the following aspects of data upload:

- Steady-state upload – Regular incremental upload requires a minimum of 1.2 IOPS per CVD.
- Centralization – The number of IOPS needed during centralization is affected by the number of endpoints, endpoint connectivity, and network bandwidth.

Note: Consult your storage vendor to determine how to reach the required IOPS, which might require more than one NAS gateway. It is a best practice to provision multiple storage IP addresses so that you can use multiple CIFS channels from each Mirage server.

Other Storage Considerations

Additional recommendations and design considerations for Mirage storage include the following:

- Use RAID 5 or RAID 6. For NetApp, RAID DP is recommended.
- If you are using NetApp, you can raise the number of inodes.
- For more information, see the NetApp Communities article, How to increase the maximum number of volume inodes or files.
- If you are using NAS, disable compression, deduplication, and NAS snapshots. Mirage creates and deletes many files during its operation. If NAS snapshots are enabled, deleted-files storage is not reclaimed, and storage-capacity usage is higher than expected.
- If you are using a Windows file server, enable NTFS compression.
- Assign 1,000 CVDs per storage volume. This number takes high deduplication into account and limits IOPS contention.
- Make sure that Mirage storage is the only folder on the storage volume or file share. Do not place more than one Mirage storage directory on a volume.
- Make sure that no antivirus tool is scanning the Mirage storage. For more information, see the VMware knowledge base article, Configuring antivirus and computer protection software exclusions for VMware Horizon Mirage.
- Create appropriate security measures for Mirage storage. For more information, see Configuring Mirage Storage security.

Network

Various aspects of network configuration are considered in the following sections. Mirage can manage endpoints in both LAN and WAN environments.

Bandwidth Configuration

Typically, centralization and steady-state uploads are the major bandwidth considerations for Mirage, and they both need to take the following into account:

- Endpoint uplink – The bandwidth needed by each endpoint as it sends data to the data center.
- Data center uplink – The bandwidth needed by the data center to receive data sent by all endpoints combined.

Download bandwidth (downlink) is not typically a consideration because of the branch reflector architecture. However, some projects, such as hardware migrations, should consider downlink requirements.

Bandwidth Estimation

Centralization and steady-state uploads are the major consumers of bandwidth, and both should be considered.

For centralization, a typical uplink requirement is 100 to 200 Mbps for the data center and 20 to 100 Kbps per endpoint.

Note: Network requirements are affected by many parameters. When estimating your data center and endpoint uplink requirements, take into account the number of endpoints in your environment, your laptop-to-desktop ratio (desktops are connected all the time, while laptops are connected erratically), number of users connected over the WAN, number of users connected over the LAN, CVD size, deduplication ratio, and the amount of user-initiated changes made daily.

Steady-state upload is based on the required upload amount per hour. A typical high-workload endpoint uploads 150 MB of changes daily. If the endpoints are connected all day, you can estimate that every endpoint needs an uplink of 15 Kbps.

The data center uplink required by steady-state upload is related to the endpoint uplink and the number of endpoints deployed outside of the data center, as expressed in the following formula:

data center uplink
= (endpoint uplink) x (number of endpoints outside the data center)

For the download link estimate, Mirage typically transfers data from Mirage servers to endpoints when performing layer updates and migrations. Consider the number of endpoints, the image size for the layer update and the Windows OS migration, and the required distribution time.

You can estimate the download link with the following formula:

download link
= (image size) x (number of endpoints) ÷ (required distribution time)

Note: If branch reflectors are deployed, include the number of branch reflectors plus the number of endpoints in the data center. If no branch reflectors are deployed, use the total number of endpoints.

Full-image download is used infrequently, typically for disaster recovery situations. It is therefore not a factor for network and storage sizing. However, for projects with massive hardware refresh (migration) or site disaster recovery events that require restoring hundreds of endpoints, you might need to perform a similar calculation, based on the average unique file size (the post-deduplication CVD size calculated previously), minus the 30 percent typical compression rate. Branch reflectors are not used for the non-layer part of the restore operation (the user files).

Network Limiting

In a production environment, Mirage servers coexist with other software. To ensure that Mirage does not interfere with other software, you can use traffic shaping, quality of service (QoS), or class of service (CoS) to manage network activity. Figure 3 shows an example of traffic shaping.

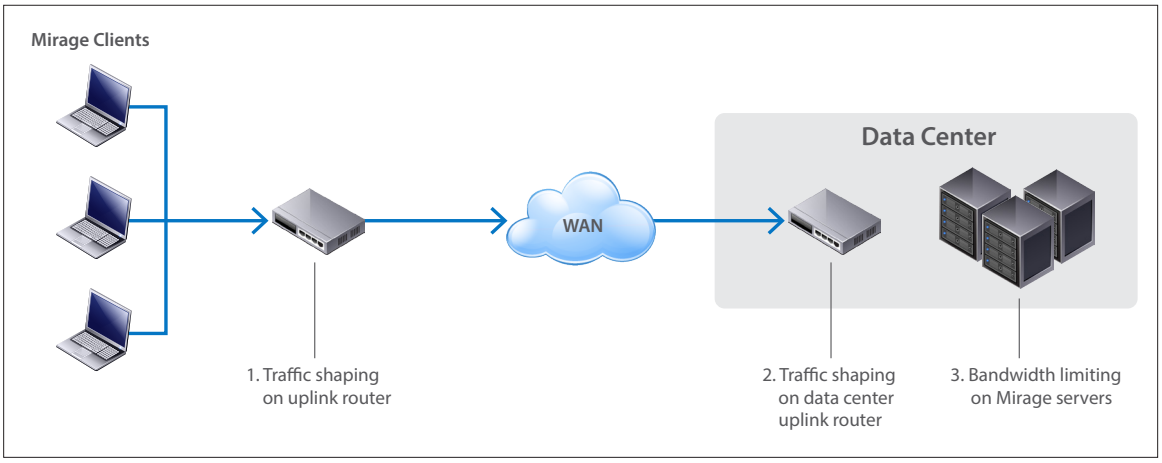

Figure 3: Traffic Shaping in a Mirage Environment

Note: You can use third-party software such as SoftPerfect Bandwidth Manager or F5 Local Traffic Manager for non-Mirage data.

Mirage bandwidth limitation rules cover all Mirage scenarios in your environment, including centralization, base layer provisioning, restores, base and app layer updates, OS migrations, and steady-state uploads. Mirage bandwidth limiting can also update the bandwidth limits on the clients without performing a reboot or other client-side action.

The best option is to implement network limiting on branch routers, because the routers can give more bandwidth to Mirage when other endpoints are not active with line-of-business data transfers.

The second-best recommendation is to use QoS on data center routers.

If there is a problem with QoS, use Mirage bandwidth limitation rules with any third-party software for traffic shaping of non-Mirage data.

Mirage bandwidth limitation rules let you define

- Global bandwidth usage limits on all Mirage clients
- Bandwidth limitation rules according to time and day, for instance for low bandwidth utilization during peak hours and higher bandwidth during nights or weekends
- Bandwidth usage limits per branch, as determined by subnet
- Bandwidth usage limits based on Active Directory sites
- Separate bandwidth usage limits on download or upload operations

For more information, see *Managing Bandwidth Limitation Rules* in the VMware Mirage Administrator's Guide.

Ports and Protocols

Make sure that your firewall allows the ports and protocols used by Mirage.

- By default, the Mirage servers and the Mirage Gateway use port 8000, with SSL encryption.
- The Mirage Gateway uses port 389 to access the Active Directory server.
- All ports use TCP.

Additional lockdown configurations on the firewall can provide additional security hardening. For example, IPsec integrated with the firewall can secure the packets transferred between the Mirage Gateway and the Active Directory server.

Figure 4 depicts all the connections between these components.

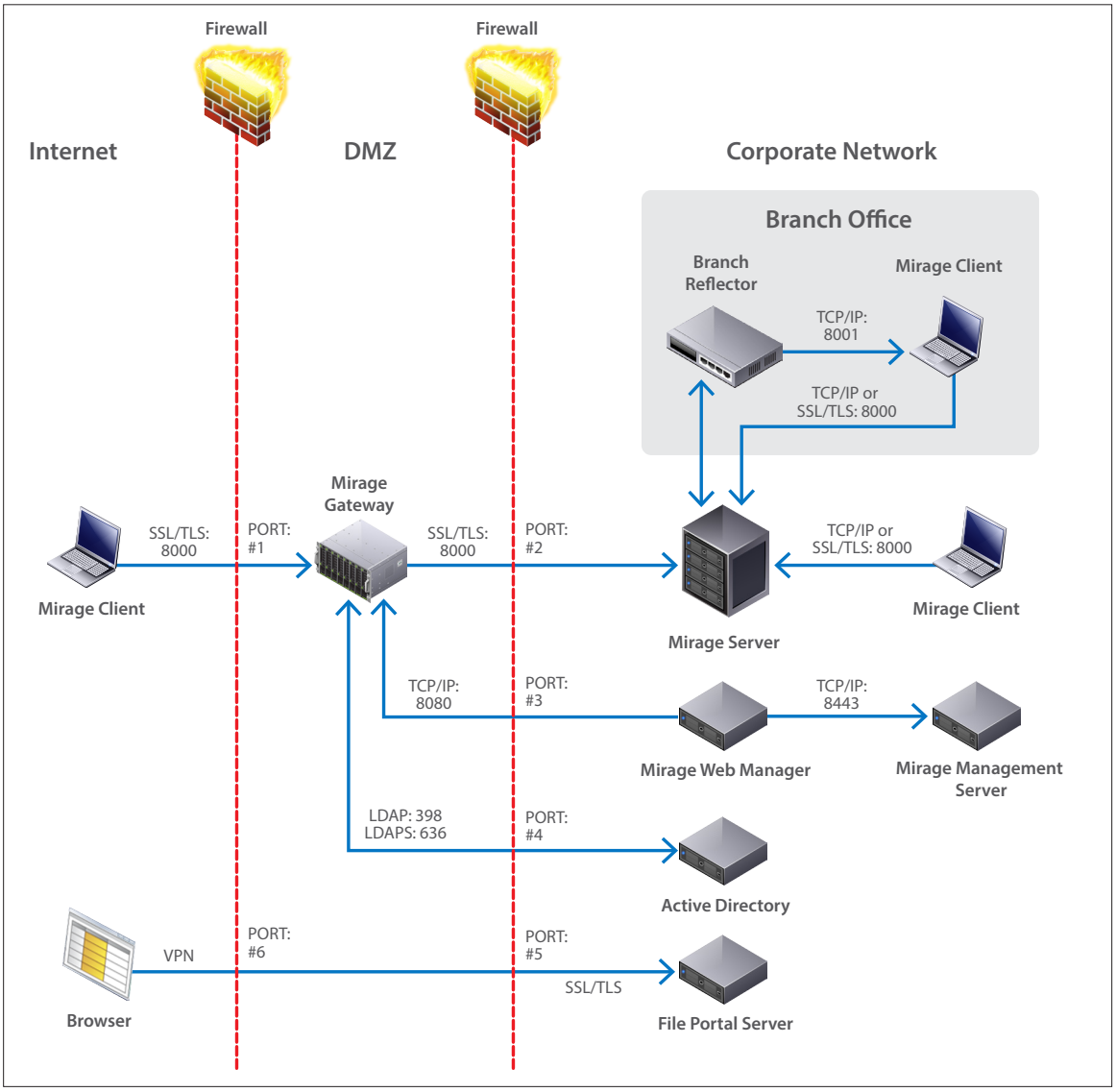

Figure 4: Ports Required by Mirage

Mirage ports and protocols are further described in Table 4.

PORT #	SOURCE	DEFAULT PORT	PROTOCOL	DESTINATION	NOTES
1	Mirage client (software)	8000	SSL/TLS	Mirage Gateway	Destination program: `/opt/MirageGateway /bin/MirageGateway`
2	Mirage Gateway	8000	SSL/TLS	Mirage server	Destination program: `C:\Program Files \Wanova\Mirage Server\wanova. mirage.server.exe`
3	Mirage Web Manager	8080	TCP/IP	Mirage Gateway	
4	Mirage Gateway	389 or 636	LDAP or LDAPS	Active Directory	LDAP uses port 389 LDAPS uses port 636
5	Browser	6443	TCP/IP	Mirage file portal server	
6	Browser	Port used by VPN	Protocol used by VPN	File portal server	

Table 4: Ports and Protocols Required by Mirage

SSL Configuration

Secure Sockets Layer (SSL) is highly recommended for Mirage. If you use Mirage Gateway, SSL is required for Mirage servers as well as for the Mirage Gateway.

To set up SSL for Mirage, consider the decisions in the following subsections.

Public CA or Internal CA

Make sure that your chosen Certificate Authority (CA) is trusted by your Mirage servers, gateways, and endpoints. Usually, a public CA is trusted by default, but it is often necessary to import an SSL certificate signed by an internal CA into the Personal certificate store and import the root certificate of the internal CA into the Personal and Trusted Root Certification Authorities certificate stores.

FQDN

The common name should be the fully qualified domain name (FQDN) for the Mirage cluster, and the Subject Alternative Names (SAN) should list all the Mirage servers. For more information, see the VMware Mirage Installation Guide.

Single or Separate SSL Certificates for Mirage Servers and Mirage Gateway

If you use separate SSL certificates for the Mirage Gateway and for Mirage servers, you can have two certificates with the same Common Name (CN) and use different name resolutions for the internal LAN as opposed to the Internet. For example, for access from the Internet, the CN should resolve to the Mirage Gateway so that when the endpoint is part of an internal LAN , the enterprise DNS can point to the Mirage cluster. Another way is to manually change the server address used by the Mirage client when moving between a WAN and LAN, because the server's FQDN must match the CN of the SSL certificate.

If you use the same SSL certificate for Mirage servers and Mirage Gateway, the endpoints can automatically connect to the correct server when moving between WAN and LAN connections. However, you must configure split-zone DNS for endpoints in WAN and LAN environments, as shown in Figure 5.

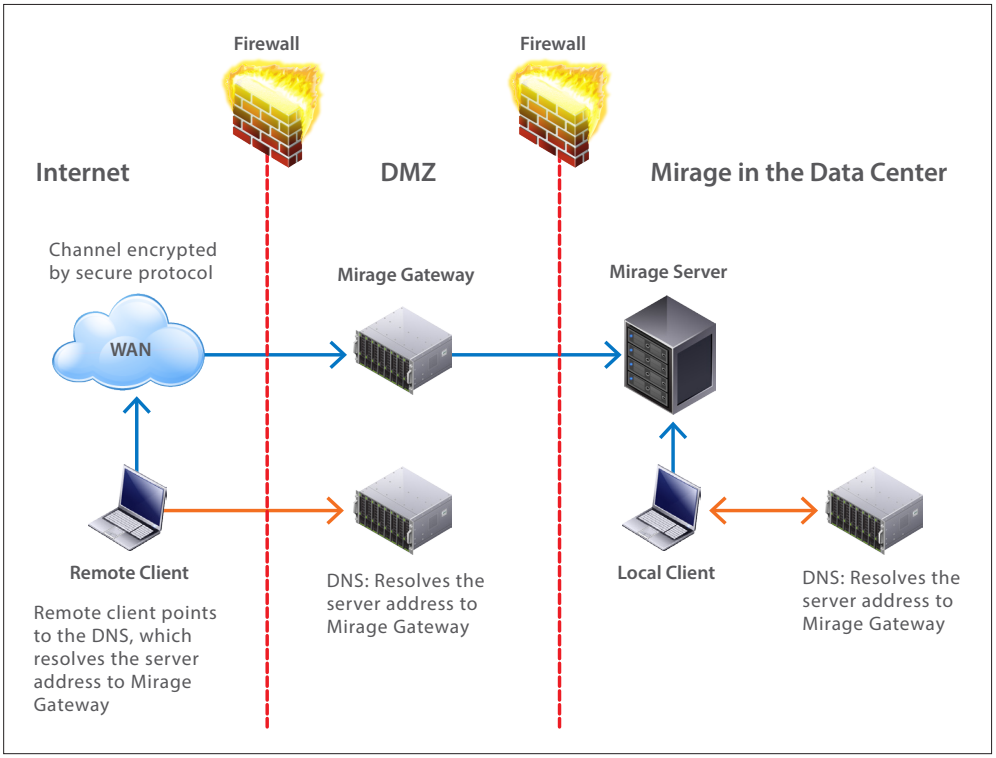

Figure 5: Using Split-Zone DNS for Remote Endpoints and Local Endpoints

For more information, see VMware Mirage Server and Horizon Mirage Edge Server install fails with a certificate error.

Load Balancer
A load-balancing environment is required if you have multiple Mirage servers or Mirage Gateways. You can use an enterprise load balancer from a supplier such as F5 Networks or a round-robin DNS configuration.

Load balancers used with Mirage

- Must support 2 TCP connections per endpoint and up to 40,000 TCP connections for each Mirage cluster.
- Must have a minimum throughput of 1 Gbps.

Note: Many open-source and evaluation load-balancer solutions limit throughput to less than 1 Gbps.

- Should be configured to optimize TCP traffic, because Mirage network communication is based on TCP.

Mirage is compatible with the maximum segment size tuning in F5 LTM VE 9 and later. For more information, see Horizon Mirage Client uploads through an F5 load balancer or IPSec VPN network device fail due to frequent disconnects.

Branch Reflectors
A branch reflector is an endpoint located at a remote site, such as a branch office. It downloads base layers, app layers, driver libraries, and USMT files from the Mirage server, making the data available for peer-to-peer transfers to other endpoints at the remote site. For restore operations, the branch reflector can be part of the process for downloading the base layer, app layers, and driver libraries.

Branch reflectors are useful when many users share a WAN link to the data center where the Mirage server or cluster is located. At least one branch reflector is recommended for each subnet.

Branch reflectors do not accelerate centralization or steady state.

You can set any endpoint as a branch reflector as long as it has enough space to store the images of layers, driver libraries, and USMT files. Branch reflectors have the following requirements:

- The branch reflector endpoint needs about 40 GB of free space.
- The endpoint must be a desktop connected to the network at all times. It cannot be a laptop or other system that disconnects frequently.
- Do not use an endpoint that is used for other purposes. Dedicating an endpoint for exclusive use as a branch reflector is optimal.

When determining the number of branch reflectors required, take into account the following considerations:

- At least one branch reflector should be provisioned for each geographical location. A branch office can have multiple subnets and still be served by one branch reflector. However, as noted, at least one branch reflector is recommended for each subnet.
- A branch reflector can serve around 40 endpoints concurrently or as many as 100 to 250 or even more, assuming that only a fraction of the endpoints are connected at the same time. If a branch reflector is serving the maximum number of connections at any given time, it manages a queue of other endpoints and serves them in turn.

Endpoints select branch reflectors according to the following algorithm:

1. Search for branch reflectors in the same subnet.
2. Search for branch reflectors that serve endpoints outside of their subnets.
3. Search for branch reflectors in the same AD site.
4. If multiple candidates are found, check for latency.

To configure a batch of branch reflectors, use the following command:

```
c:\Program Files\Wanova\Mirage Management Server
\Wanova.Server.Tools.exe ConfigureBranchReflector
```

Mirage Gateway
A Mirage Gateway is located in the DMZ. Mobile endpoints connect to the data center through the Mirage Gateway without having to use a VPN.

A Mirage Gateway virtual appliance can support up to 5,000 mobile endpoints, but for maximum performance, it is recommended that you deploy one Mirage Gateway per 3,000 mobile endpoints. In addition, it is always necessary to consider failover requirements. Therefore, the recommended number of Mirage Gateways is

(M/3000)+1

where *M* is the total number of mobile endpoints.

Note: Use a load balancer if multiple Mirage Gateways are needed.

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

Database

Mirage uses SQL Servers to store environmental metadata, such as information about Mirage servers, endpoints, CVDs and their snapshots, operations and transactions, and names and versions of layers. The number of CVDs determines the recommended SQL configuration.

If the total number of CVDs is less than 5,000, use one of the following SQL versions on a system with at least one CPU at 2.0 GHz or faster and memory equivalent to the RAM requirement of the OS plus 1 GB:

• Microsoft SQL Express 2008 R2

• Microsoft SQL Express 2012

• Microsoft SQL Express 2014

If the total number of CVDs is greater than 5,000, use one of the following SQL versions on a system with least two CPUs at 2.0 GHz or faster and at least 4 GB of RAM:

• Microsoft SQL 2008 R2, Standard or Enterprise Edition

• Microsoft SQL 2012, Standard or Enterprise Edition

• Microsoft SQL 2014, Standard or Enterprise Edition

In summary:

(OS RAM requirement) + (500 KB x (total number of CVDs))

Note: If you install SQL Server 2008 R2 on Windows Server 2012, you must install SQL Server 2008 R2 SP1 or later.

Microsoft SQL Servers must be configured with Windows Authentication.

For more information about requirements for Microsoft SQL Server, see the following Microsoft documents:

• Hardware and Software Requirements for Installing SQL Server 2008 R2

• System Requirements and Installation Information for Windows Server 2012 R2

About the Authors and Contributors

This paper was updated for Mirage 5.7 by Yaniv Weinberg, R&D Manager, VMware, and Gary Sloane, VMware Consulting Editor, and reviewed by Chris White, End-User-Computing Architect, VMware.

The original version of this document was written by

- Stephane Asselin, End-User-Computing Architect, VMware
- Yaniv Weinberg, R&D Manager, VMware
- Alexander West, former Technical Writer, End-User Computing, VMware
- Judy Wu, Solution Engineer, VMware

To comment on this paper, contact the End-User-Computing Technical-Marketing Center of Excellence team at euc_tech_content_feedback@vmware.com.

References

A heavily fragmented file in an NTFS volume may not grow beyond a certain size

Configuring antivirus and computer protection software exclusions for VMware Horizon Mirage

Hardware and Software Requirements for Installing SQL Server 2008 R2

Horizon Mirage Client uploads through an F5 load balancer or IPSec VPN network device fail due to frequent disconnects

Limitations of using VMware Mirage to manage endpoints protected by Kaspersky Endpoint Security

Limitations of using VMware Mirage to manage endpoints protected with Sophos SafeGuard full disk encryption

Mirage MongoDB location and sizing best practices

System Requirements and Installation Information for Windows Server 2012 R2

VMware Mirage Large-Scale Reference Architecture

VMware Mirage Documentation

VMware Mirage Server and Horizon Mirage Edge Server install fails with a certificate error

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com