Virtualization Guide

McAfee Vulnerability Manager Virtualization

COPYRIGHT

TRADEMARKS

LICENSE INFORMATION

License Agreement

Issued 5/18/2012 14:02 / McAfee Vulnerability Manager Virtualization Guide
700-27201--00

Contents

McAfee Vulnerability Manager virtualization

McAfee® Vulnerability Manager can run in a virtual VMware ESX environment or in a virtual VMware workstation. Using VMware ESX allows you to use your McAfee Vulnerability Manager software while maximizing the use of your hardware. Using VMware workstation allows you to use McAfee Vulnerability Manager software on a laptop, connect the laptop to a remote network for scanning, and then import the scan data into your main database using the data synchronization service.

Installing and running McAfee Vulnerability Manager in a virtual environment is the same as using a physical server.

Supported VMware platforms

- McAfee Vulnerability Manager 7.5 is compatible with VMware ESX versions 4.0 and 4.1.
- McAfee Vulnerability Manager 7.5 is compatible with VMware Workstation versions 7.0.x.

  This guide does not contain information about setting up a virtual environment; that information must be obtained from the virtualization vendor VMware, for their ESX server product.

Advantages to using VMware ESX

- You can maximize the use of your hardware by setting the resources allocated for each virtual machine on the physical server. For example: a physical server with 4 CPUs (or cores) could have 2 virtual machines with 2 CPUs (or cores) allocated to each virtual machine.
- It is possible to create a VMware template for your scan engines (page 14), so long as you have the proper license for Microsoft Windows and McAfee Vulnerability Manager.
- When running an Asset Discovery scan, the performance of a virtual server and a physical server are almost identical.

Disadvantages to using VMware ESX

- When running a Windows Host Assessment Module (WHAM) scan or Full Vulnerability scan, the McAfee Vulnerability Manager virtual machine requires more time to complete the scan.
- While it is possible to run multiple virtual machines that have a combined resource requirement larger than what is actually available on the physical server, this negatively impacts performance.

Note: Installing a database on a physical system produces better results than running the database on a virtual system.

Advantages to using VMware workstation

- McAfee Vulnerability Manager can run on a laptop computer and scan remote or air-gapped networks by connecting the laptop to the network.
- You can import the McAfee Vulnerability Manager data to your main database.

Disadvantages to using VMware workstation

- You can only deploy McAfee Vulnerability Manager components on one system (All-in-One). McAfee Vulnerability Manager does not support installing components on separate VMware workstations.
- You are limited on the number of IP addresses you can scan with reasonable performance from the host system.

McAfee Vulnerability Manager components and VMware ESX

McAfee Vulnerability Manager consists of five main components.

- Enterprise manager – Uses Microsoft Internet Information Services (IIS) to provide authorized users with access to McAfee Vulnerability Manager through their web browsers. It allows them to manage and run McAfee Vulnerability Manager from anywhere on the network. Access is protected by user identification and authentication. Secure Socket Layers (SSL) can be set up through the Web server to provide encrypted communications to browsers.
- Database – The data repository for the McAfee Vulnerability Manager system. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and scan engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.
- API server – Provides the communication between the enterprise manager and the database.
- Scan controller – Provides the communication to the scan engines. One or more scan controllers can control multiple scan engines. The scan controller should be installed on a virtual machine running a scan engine.
- Scan engines – Scan the network environment. The scan engine is the server that scans your network. Depending on the logistics and size of your network, you might need more than one scan engine to scan the network.

On large networks, install the enterprise manager, database, and scan engine on separate, dedicated virtual machines. This is due to the amount of resources required by each of these components when displaying the data to the user, processing data, or scanning the network. It is possible to combine the scan engine and database when installing on smaller networks. Each virtual server should contain a fresh installation of the operating system with updated security patches.

The API server and scan controller are main components but do not require a dedicated virtual machine.

Users log on to the enterprise manager through their web browser to access the system.

Note: For dedicated virtual machines, do not run other main components on these virtual machines. You can run Additional Modules with McAfee Vulnerability Manager main components.

Additional modules

Four additional modules are available in McAfee Vulnerability Manager. These do not require separate, dedicated virtual servers, but can run on the database virtual server if it is a dedicated database server, or on the scan engine virtual server. See *Deployment architectures* (page 8) for details.

- The configuration manager distributes initial certificates to the other McAfee Vulnerability Manager components and manages updates to the components.
- The notification service provides SNMP and email (SMTP) notification messages for integration with third-party helpdesk management systems and email servers. The notification service can be installed on any server that meets the system requirements – it does not have to be installed on a virtual server running other McAfee Vulnerability Manager components.
- The report engine generates both scan-based and asset-based reports.

- The McAfee Vulnerability Manager Data Synchronization Service gathers information from McAfee ePO databases, LDAP servers, and other McAfee Vulnerability Manager databases. For McAfee ePO databases, it provides data to McAfee Vulnerability Manager for host and OS identification. For LDAP servers, it provides assets that can be added to scan configurations. For McAfee Vulnerability Manager databases, you can import data and generate reports. The McAfee Vulnerability Manager databases must be the same version.
- The McAfee Vulnerability Manager web application scanner provides a scan configuration, vulnerability checks, and scan reports for web applications.

  This is a separate module that is available for purchase.

Number of servers required

The number, type, and placement of product servers depend on the total amount of address space, total number of live devices, network topology, desired scan performance, network constraints, and network policies.

Note: McAfee Vulnerability Manager supports only servers running English-language operating systems.

The following matrix provides guidelines for determining the number of McAfee Vulnerability Manager servers.

Number of live IPs	Number of servers	Notes
0 – 2,500	One product server with an All-in-One configuration	Ideal for small networks and product evaluations
2,500 – 10,000	Two product servers: One configured as enterprise manager web portal and the other configured as a database, API server, scan controller, and a scan engine with additional components.	Very common configuration for small to mid-sized deployments
10,001 – 20,000	Two product servers: One configured as enterprise manager web portal and the other configured as database, API server, scan controller, and scan engine with additional components. One product server configured as a dedicated scan engine.	Well-suited for large, distributed environments

Number of live IPs	Number of servers	Notes
20,001 - >100,000	Three product servers: One configured as enterprise manager web portal, one configured as database, and one configured as API server, scan controller, and scan engine with additional components. *n* product servers configured as dedicated secondary scan engines.	Ideal for large, global, distributed and diverse networks

Consider these factors:

- **Number of IP addresses to be scanned.** The primary factor is the number of IP addresses to be scanned. Small to medium-sized networks, as well as installations for product evaluation purposes, can deploy a single product server. Larger networks are better accommodated with additional hardware.
- **Network connectivity to, and reachability of, all desired target environments.** A scan engine must be able to reach its targets for the results to provide value. When placing scan engines, consider the networks that are to be scanned and place the scan engine so that it is able to reach the maximum number of assets with as few firewalls or packet filtering devices as possible.
- **Firewall traversing.** The purpose of a firewall is to restrict traffic to legitimate users and prohibit traffic that might be malicious. Depending upon the nature of the vulnerability and the discovery methodology, vulnerability scanning signatures might resemble malicious traffic and be blocked or filtered by a firewall or port filter. The result of such well-intentioned security devices might be that the quality of data returned from a vulnerability scan is adversely affected. For example, hosts behind a firewall might not be discovered correctly or at all, or a firewall might make it appear that every host behind the firewall is present when they are not. Another possible effect is that discovery and assessments might take longer to complete when having to traverse a firewall compared to scans that do not have to traverse firewalls. A common technique to mitigate the impact is to either avoid sending the assessment traffic through a firewall altogether, or to create an exception rule in the firewall rule base to allow any and all packets to and from the scan engine to traverse the firewall unaltered.
- **WAN links and latency.** To ensure a manageable vulnerability assessment schedule, McAfee Vulnerability Manager employs various timing and monitoring components. Such components monitor the total time a thread has taken to run a check against a host. If a certain threshold is exceeded, the thread is terminated under the assumption that the host is down, or that packets have been lost in transit to or from the host. This technique is necessary to ensure that a scan is not in an infinite waiting state. Therefore, WAN links, or heavily congested networks in general, might need special consideration in a deployment. Tests have shown that scanning via WAN links with a latency of more than 150 milliseconds is likely to produce results of an improper quality. For example, a set of systems can only be reached via a WAN link, then consider placing a scan engine in the remote environment so scanning is done locally and not be subject to packet loss and timeouts that are common on a congested WAN link.

- **Other network traffic (business-critical data/sessions).** Any active scanning technology, such as McAfee Vulnerability Manager, sends some amount of data to assets on the network. This is an unavoidable consequence of any vulnerability scanning technology. McAfee Vulnerability Manager provides robust and detailed controls that allow customers to optimize the scanning behavior and speed of McAfee Vulnerability Manager. The product has default settings that have proved safe and effective in most networks. However, no matter how McAfee Vulnerability Manager is deployed and configured, you should always pay attention to network segments, WAN links, firewalls, and so on, where particularly important data is passing. Consider a remote site that is transmitting transactions from a website through a congested or slow WAN link during local business hours. Since this system only operates during certain hours, you should configure scans so that the environment is scanned while the web server is not processing transactions and not relying on bandwidth on the WAN link.
- **Security or performance.** When two product servers are used, McAfee recommends that you deploy the enterprise manager on one system and the other product components on the second system. This provides more security because the enterprise manager can be placed outside your firewall, so users can access it, while the second system can be placed inside the firewall to gather accurate data from scanned systems. However, having the scan engine and scan controller on the same system as the database can slow performance, based on the amount of data being processed. To improve performance when using two product servers, you could separate the scan engine and scan controller from the database. For example: the enterprise manager, scan engine, and scan controller on one system and the database and other McAfee Vulnerability Manager components on the second system.

Deployment architectures

McAfee Vulnerability Manager is typically set up in one of the following architectures:

- Single virtual server architecture (page 8)
- Dual virtual server architecture (page 9)
- Three virtual server architecture (page 10)
- Distributed virtual server architecture (page 10)

Use these general guidelines to determine the architecture for your network. The deployment architectures for running McAfee Vulnerability Manager in a virtual environment are the same as deploying McAfee Vulnerability Manager on physical servers. By installing McAfee Vulnerability Manager components on separate virtual servers, you can configure the virtual server settings to ensure each component is allocated the required amount of physical resources.

Note: McAfee Vulnerability Manager supports using both physical systems and virtual systems in the different deployment architectures. To improve performance, McAfee recommends running the database on a physical system rather than a virtual system.

Single virtual server architecture

This architecture is appropriate for small (class C) networks. All components are installed on the same server.

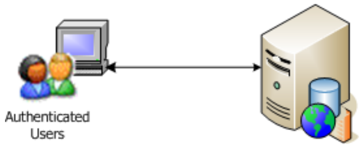

Figure 1: All-in-one architecture

Virtual system: web portal, database, API server, and scan engine

- Enterprise manager
- Report server
- Database
- API server
- Scan controller
- Scan engine
- Notification service
- Data synchronization service
- Configuration manager

Dual virtual server architecture

This architecture is appropriate for small to medium (class C and class B) networks. The scan engine and the database are installed on the same server; the enterprise manager is installed on its own server. This allows fast, efficient communication between the scan engine and database, while a dedicated server runs the enterprise manager interface that most of your users will see.

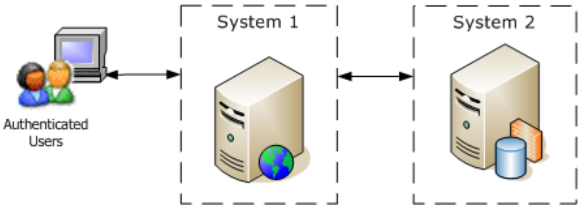

Figure 2: Dual server architecture

Virtual system 1: web portal

- Enterprise manager
- Report server

Virtual system 2: database, API server, and scan engine

- Database
- API server
- Scan controller
- Scan engine
- Notification service
- Data synchronization service
- Configuration manager

Three virtual server architecture

This architecture is designed for large, global enterprises, and is appropriate for scanning multiple class B and class A networks. In this configuration, all three components reside on individual virtual servers.

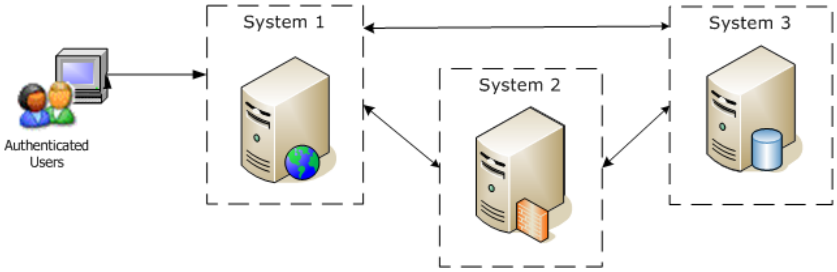

Figure 3: Three server architecture

Virtual system 1: web portal

- Enterprise manager

Virtual system 2: API server and scan engine

- API server
- Scan controller
- Scan engine
- Notification service
- Data synchronization service

Virtual system 3: database

- Database
- Report server
- Configuration manager

Distributed virtual server architecture

Larger, more complicated environments need multiple scan engines. Each engine generates scan traffic on their local network segments, and sends the resulting scan data back over the WAN to the database. This dramatically reduces the amount of traffic on the WAN resulting from network scans.

Multiple virtual, secondary scan engines can be added to this architecture.

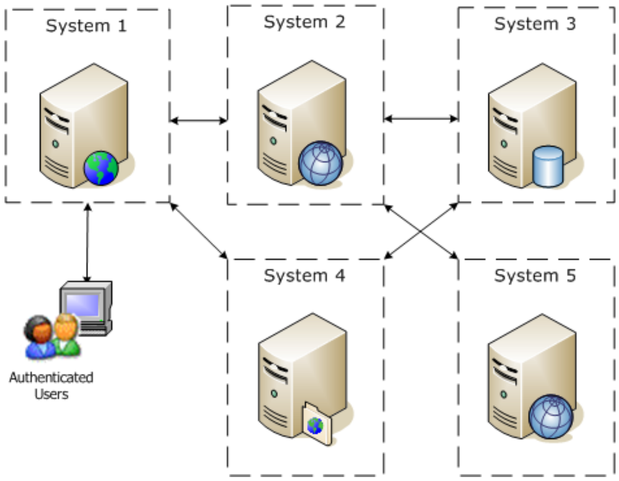

Figure 4: Distributed server architecture

Virtual system 1: web portal • Enterprise manager	**Virtual system 2: API server and scan engine** • API server • Scan controller • Scan engine • Notification service • Data synchronization service	**Virtual system 3: database** • Database • Configuration manager
	Virtual System 4: report server • Report server	**Virtual System 5: scan engine** • Scan engine

System requirements

Operating system requirements

- Microsoft Windows Server 2008 R2, without a service pack, or with Service Pack 1 or later. McAfee Vulnerability Manager supports only systems running English-only operating systems.
- Current security updates, including the JScript update provided in Microsoft Security Bulletin MS06-023
- Static IP addresses and fencing policies should be utilized in the virtual environment

Software requirements

- Microsoft .NET Framework v2.0 or later is required when installing any of the McAfee Vulnerability Manager components.

Note: McAfee Vulnerability Manager does not support installing the database with .NET 4.0. If you must use .NET 4.0, install the database first.

Web portal (enterprise manager) system requirements

Component	Requirement
Processor	2 virtual CPUs **Note**: Server processors must be dual Xeon 2 GHz, dual Core Xeon 2.33 GHz, or better.
Memory	4 GB RAM
Disk space	80 GB partition
Additional software	• IIS 7.5 • Current IIS security patches • World Wide Web Publishing must be running
Dedicated virtual machine	• Yes • Administrator account
Disk partition formats	NTFS
Network card	Ethernet

Database system requirements

Component	Requirement
Processor	2 virtual CPUs **Note**: Server processors must be dual Xeon 2 GHz, dual Core Xeon 2.33 GHz, or higher.
Disk space	80 GB partition **Tip**: 250 GB of disk space is recommended for large networks.
Memory	4 GB
Additional software	• Microsoft SQL Server 2008 SP1 or later • All SQL hotfixes and patches • All .NET hotfixes and patches
Dedicated virtual machine	• Yes • Administrator account
Virtual memory	2.0 GB minimum
Disk partition formats	NTFS
SQL Server memory settings	900 MB
Network card	Ethernet

SQL Server memory recommendations

McAfee recommends using the following SQL memory settings:

- When the database is the only component on the system, set the Maximum SQL memory to 1.4 GB.
- When the database and the Report Server are both running on the same system, use 900 MB.
- When the database and the scan engine are both running on the same system, use 750 MB.

Scan engine system requirements

Component	Requirements
Processor	2 virtual CPUs **Note**: Server processors must be dual Xeon 2 GHz, dual Core Xeon 2.33 GHz, or higher.
Memory	2 GB RAM
Disk space	80 GB partition
Additional software	MDAC 2.8
Dedicated system	Recommended when running large scans
Virtual memory	2.0 GB minimum
Disk partition formats	NTFS
TCP/IP connection	NetBIOS over TCP/IP
Required services	Print spooler
Network card	Ethernet

Report server system requirements

Components	Requirements
Memory	2 GB RAM
Disk space	80 GB partition
Additional software	MDAC 2.8
Dedicated virtual machine	Recommended for report-intensive environments
Network card	Ethernet

System requirements for other product components

Components	Requirements
Memory	2 GB RAM
Disk space	80 GB partition
Additional software	MDAC 2.8

Components	Requirements
Dedicated virtual machine	No
Network card	Ethernet

Note: McAfee Vulnerability Manager performance can negatively be affected by running on a single CPU and/or having multiple services (outside what is required by McAfee Vulnerability Manager) running.

Clone a scan engine

Using a virtual environment does allow you to clone some of your setups. With McAfee Vulnerability Manager, the only component you might want to clone is the scan engine. Other McAfee Vulnerability Manager components (enterprise manager, database, McAfee Vulnerability Manager Data Synchronization Service, etc.) only require one to be installed.

When cloning a scan engine, an FCM agent is also included.

1. Create a virtual machine.
2. Install Microsoft Windows Server 2008 R2.
3. Install scan engine only.
   An FCM agent is automatically installed with the scan engine.
4. Copy the scan engine virtual machine.
5. Give the copied scan engine a unique name.
6. Launch the virtual scan engine and delete the following registry keys:
   Microsoft Windows Server 2008 R2:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\FCM\Agent\AgentID
   - This is used by an FCM agent to identify itself to the FCM Server.
   - If it does not exist, it is created when the agent is started.
   - If you fail to delete this, the FCM Server shows one node for both systems (the original and the clone) and the information displayed toggles between the two systems, depending on which one last reported information to the FCM server.

   Microsoft Windows Server 2008 R2:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\Foundscan\Identification\ID
   - This is used by the engine to identify itself to the database. You will see this ID listed in the **Engines** table of the database.
   - If it does not exist, it is created when the engine is started.
   - If you fail to delete this, McAfee Vulnerability Manager might not function properly.
7. Restart the virtual machine.

If you are using multiple virtual servers to run scan engines, you can create a VMware template and then clone the template to create your scan engines.

1. Create a new virtual machine in VMware.
2. Install Microsoft Windows Server 2008 R2.
3. Install the scan engine.
4. Delete the following registry keys:

   Microsoft Windows 2008 R2:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432\Foundstone\FCM\Agent\AgentID

   - This is used by an FCM agent to identify itself to the FCM Server.
   - If it does not exist, it is created when an agent is started.
   - Failure to delete this causes the FCM Server to show one node for both systems (the original and the clone) and the information displayed toggles between the two systems, depending on which one last reported information to the FCM server.

   Microsoft Windows 2008 R2:
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\Foundscan\Identification\ID

   - This is used by the engine to identify itself to the database. This ID is listed in the *Engines* table of the database.
   - If it does not exist, it is created when and engine is started.
   - Failure to delete this could cause problems when running McAfee Vulnerability Manager.
5. Run the System Preparation tool for the selected operating system.

   The System Preparation tool can be downloaded from the Microsoft website.
6. Set this virtual machine to Template.
   a. In VMware, select **VM | Settings | Options | Advanced | Enable Template mode**.
   b. Click **OK**.
7. Take a snapshot of the scan engine template.
   a. Right-click the scan engine template.
   b. Select **Take Snapshot**.
   c. Type a name for this snapshot. The description is optional.
   d. Click **OK**.

After creating a VMware template, you can create multiple scan engines from the template.

1. Right-click the scan engine template.
2. Select **Clone**.

   Follow the steps in the VMware wizard to create a clone.

   Note: If you create a Linked Clone, this clone must be on the same server as the original virtual machine (the scan engine template).
3. Start the cloned virtual machine.
4. Follow the Windows wizard to set up this virtual machine.

   This might require a product key.
5. Register the scan engine.

   Select **Start | Programs | Foundstone | Register FoundScan**.

VMware ESX virtualization notes

For optimal performance, use the following guidelines.

- When running multiple virtual servers on the same physical server, launch the virtual servers in small batches instead of all at once. Launching in small batches ensures that the physical server doesn't drop any data packets due to the resource consumption of starting multiple virtual servers.
- Limit the number of scans running concurrently to 40 or less per virtual server. Higher scan numbers might cause data packet loss due to the higher amount of CPU usage

McAfee Vulnerability Manager and VMware workstation

McAfee Vulnerability Manager can be installed on a VMware workstation and is recommended for use with a laptop for scanning remote networks that do not have a dedicated scan engine and are too difficult to scan remotely. Trying to scan through a firewall can result in inaccurate or incomplete scan data. Or maybe you have an air-gapped network, one that is not connected to any other network or to the Internet. In these cases, you can connect your McAfee Vulnerability Manager laptop to the remote or air-gapped network, run a scan to gather system information, then import the laptop data into your main database.

If you want to use a server and VMware, McAfee recommends that you use VMware ESX. The performance of McAfee Vulnerability Manager using VMware ESX and a server closely matches the performance of installing McAfee Vulnerability Manager directly on the server.

System requirements

Single server system requirements

Component	Requirement
Processor	Intel Core i3 or better
Memory	4 GB RAM
Disk space	80 GB Partition
Dedicated system	• Yes • Administrator account
Disk partition formats	NTFS
Network card	Ethernet

Single server software requirements

- Microsoft Windows Server 2008 R2, without a service pack, or with Service Pack 1 or later.
  - McAfee Vulnerability Manager supports only systems running English-only operating systems
  - Current security updates
- Microsoft SQL Server 2008, with Service Pack 1 or later, or
  Microsoft SQL Server 2008 Express R2 or later
  - All Microsoft SQL and .Net hotfixes and patches
  - McAfee recommends using 750 MB for the SQL memory setting
- Additional software (covered by default Microsoft Windows and Microsoft SQL installations)
  - IIS 7.5, including current IIS security patches
  - MDAC 2.8
  - World Wide Web Publishing must be running
  - SQL Client Tools
- Additional VMware settings
  - A bridged network is required

Note: If you use SiteMinder, McAfee Vulnerability Manager 7.5 supports SiteMinder 6.x.

VMware workstation virtualization notes

The following is a known issue that might impact McAfee Vulnerability Manager functionality.

- VMware workstations can cause corrupt files during heavy I/O use. This can happen when conducting a scan that returns a large amount of data. Details can be found at the VMware communities and at this blog website.
- When setting up VMware workstation, a bridged network is required for McAfee Vulnerability Manager to function properly.

Troubleshooting

The following information might apply to your network.

Hosts appear that do not exist when using VMware Lab Manager

When running under VMware Lab Manager with Virtual to Physical network mapping enabled, McAfee Vulnerability Manager 7.5 is able to identify hosts being alive that do not exist.

This is due to a VMware virtual router being created that returns address resolution protocol requests (ARP requests) for systems that don't exist as if they do exist.