

Administration Guide

Update 2 Release for
Update Manager 1.0

Update Manager Administration Guide

Revision: 20090701

Item: EN-000037-03

You can find the most up-to-date technical documentation on our 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

© 2008, 2009 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware, the VMware “boxes” logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.

3401 Hillview Ave.

Palo Alto, CA 94304

www.vmware.com

Contents

About This Book 5

1 Understanding Update Manager 7

- Update Manager Overview 7
- Security Best Practices 7
 - Benefits of Compliance 7
 - Compliance and Security Best Practices 8
- Update Manager Processes 8
 - Patch Downloading 8
 - Scanning Virtual Machines and ESX Server Hosts 9
 - Remediation 10
- Update Manager Settings 10

2 Working with Update Manager 11

- Installing, Upgrading, and Uninstalling Update Manager 11
 - Preparing the Update Manager Database 13
 - Installing the Guest Agent 16
 - Installing the Update Manager Download Service 16
 - Upgrading VI Client to Support Update Manager 17
 - Upgrading Update Manager 18
 - Uninstalling Update Manager 18
- Update Manager Network Port Requirements 19
- Configuring Update Manager 20
 - Responding to Guest Remediation Failure 20
 - Responding to a Failure to Put ESX Server in Maintenance Mode 20
 - Checking for Updates 21
 - Configuring Update Manager for Use with an Internet Proxy 22
 - Configuring the Update Manager Network Port Settings 22
 - Configuring Update Manager Patch Download Location 24
 - Using the Update Manager Download Service 24
- Working with Baselines 25
 - Creating Baselines 26
 - Editing Baselines 28
 - Attaching Baselines 28
 - Detaching Baselines 28
 - Removing Baselines 29
- Scanning Virtual Machines and ESX Server Hosts 29
 - Viewing Scan Results 30
- Remediating ESX Server Hosts and Virtual Machines 32
 - Guest Shutdown 32
 - Manual Virtual Machine Remediation 32
 - Manual ESX Server Remediation 33
 - Scheduled Virtual Machine Remediation 33
 - Scheduled ESX Server Remediation 34
- Working with Update Manager Events 34
- Working with Updates 35
 - Including Updates in a Baseline 35
 - Filtering the Updates in the Update Repository 35

- Managing Virtual Appliances 36
 - Virtual Appliances Discovery 36
 - Scanning Virtual Appliances 36
 - Remediating Virtual Appliances 37

3 Operations Reference 39

- Common Problems and Solutions 39
 - Gathering Log Files 39
 - No Baseline Updates Available 39
 - All Updates in Compliance Reports Are Not Applicable 40
 - All Updates in Compliance Reports Are Unknown 40
 - Remediated Updates Continue to Be Not Compliant 40
 - Remediating Virtual Machines with All Update or All Critical Updates Fails 40
 - ESX Server Scanning Fails 41
- Events 41
- Database Views 44
 - VUMV_VERSION 44
 - VUMV_UPDATES 44
 - VUMV_PATCHES 45
 - VUMV_BASELINES 45
 - VUMV_PRODUCTS 45
 - VUMV_BASELINE_UPDATE_ASSIGNMENT 46
 - VUMV_BASELINE_ENTITY_ASSIGNMENT 46
 - VUMV_UPDATE_PATCHES 46
 - VUMV_UPDATE_PRODUCT 46
 - VUMV_ENTITY_SCAN_HISTORY 47
 - VUMV_ENTITY_UPDATE_SCAN_HISTORY 47
 - VUMV_ENTITY_REMEDIATION_HISTORY 47
 - VUMV_UPDATE_PRODUCT_DETAILS 48
 - VUMV_BASELINE_UPDATE_ASSIGNMENT_DETAILS 48
 - VUMV_ENTITY_UPDATE_SCAN_HISTORY_DETAILS 48

- Index 49

About This Book

This manual, the *Update Manager Administration Guide*, provides information on how to configure VMware® Update Manager, including how to install the product and configure it for use in your environment.

The Update Manager works with VMware ESX Server 3.5 and later and VMware ESX Server 3i version 3.5 and later. For ease of discussion, this book uses the following product naming conventions:

- For topics specific to ESX Server 3.5, this book uses the term “ESX Server 3.”
- For topics specific to ESX Server 3i version 3.5, this book uses the term “ESX Server 3i.”
- For topics common to both products, this book uses the term “ESX Server.”
- When the identification of a specific release is important to a discussion, this book refers to the product by its full, versioned name.
- When a discussion applies to all versions of ESX Server for VMware Infrastructure 3, this book uses the term “ESX Server 3.x.”

Intended Audience

The information in this manual is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to:

docfeedback@vmware.com

Update Manager Documentation

The Update Manager documentation consists of this administration guide, online help integrated with the Update Manager client plug-in, release notes and *Update Manager – PowerShell Library Administrator’s Guide*, which contains information about running the Update Manager cmdlets in Toolkit for Windows.

You can access the most current versions of this manual and other books by going to:

<http://www.vmware.com/support/pubs>

Technical Support and Education Resources

The following sections describe the technical support resources available to you. To access the current versions of this book and other books, go to:

<http://www.vmware.com/support/pubs>.

Online and Telephone Support

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to:

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

Customers with appropriate support contracts should use telephone support for the fastest response on priority 1 issues. Go to:

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

Support Offerings

Find out how VMware support offerings can help meet your business needs. Go to:

<http://www.vmware.com/support/services>

VMware Education Services

VMware courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. For more information about VMware Education Services, go to:

<http://mylearn1.vmware.com/mgrreg/index.cfm>

Understanding Update Manager

This chapter discusses the following topics:

- [“Update Manager Overview”](#) on page 7
- [“Security Best Practices”](#) on page 7
- [“Update Manager Processes”](#) on page 8.
- [“Update Manager Settings”](#) on page 10

Update Manager Overview

VMware Update Manager compares the operating systems and applications running in your VMware Infrastructure deployment against a set of standard updates and patches. Updates you specify can be applied to operating systems, as well as applications on scanned ESX Server hosts, virtual machines, and virtual appliances. Update Manager works with ESX Server hosts, virtual machines, and virtual appliances running on ESX Server hosts. Benefits vary depending on the versions of applications in your environment. Beginning with VirtualCenter 2.5 and ESX Server version 3.5, Update Manager lets you scan for compliance and apply updates for guests, appliances, and hosts.

Update Manager can scan and remediate powered on, suspended, and powered off virtual machines and templates, in addition to scanning and remediating hosts. If the updating or patching fails, you can revert the virtual machines and templates back to their prior condition, without losing data.

Security Best Practices

Maintaining a consistent set of operating systems and applications, with particular patching levels helps reduce the number of vulnerabilities in an environment, at the same time reducing the possible range of issues requiring solutions. All systems require patching, reconfiguration, or other solutions, but reducing the diversity of systems in an environment eases management burdens and reduces security risks.

Benefits of Compliance

Many attacks take advantage of existing, well-known issues. For example, the Nimda computer worm used vulnerabilities that were identified months before the actual spread of the worm. A patch existed at the time of the outbreak, and systems to which the patch was applied were not affected. Update Manager provides a way to help ensure that the required patches are applied to the systems in your environment.

To make your environment more secure:

- Be aware of where vulnerabilities exist in your environment.
- Efficiently bring these machines into compliance with the patching standards.

In a typical large environment, many different machines run various operating systems. Adding virtual machines to an environment increases this diversity. Update Manager automates the process of determining the state of your environment and provides a way to efficiently update VMware virtual machines and ESX Server hosts in your environment.

Compliance and Security Best Practices

To achieve the goal of compliance, with its benefits of increased security and stability, regularly evaluate the following:

- Operating systems and applications permitted in your environment
- Patches required for operating systems and applications

Determine who is responsible for making these evaluations, when these evaluations are to be made, and what tactics to use to implement the plan that results from the investigation.

Update Manager Processes

Update Manager uses a set of operations to ensure effective patch management. This process begins by downloading information about a set of security updates. One or more of these updates are aggregated to form a *baseline*. A collection of virtual machines, virtual appliances, and ESX Server hosts can be scanned for compliance with a baseline and remediated (updated). These processes can be initiated manually or through scheduled tasks.

Patch Downloading

Update Manager uses the Internet to gather information about the latest patches from VMware and Shavlik. VMware provides information about updates to ESX Server, and Shavlik provides information for all major applications and operating systems.

At regular, configurable intervals, Update Manager contacts Shavlik and VMware to gather the latest information on available patches. For information about configuring download intervals, see [“Checking for Updates”](#) on page 21. Information about all patches is downloaded, regardless of whether the application or operating system to which the patch applies is currently in use in your environment.

Downloading information about all patches is a relatively low-cost operation in terms of disk space and network bandwidth. Doing so provides the flexibility to add scanning and remediation of those applications or operating systems at any time. See [“Scanning Virtual Machines and ESX Server Hosts”](#) on page 9, [“Remediation”](#) on page 10, [“Scanning Virtual Appliances”](#) on page 36, and [“Remediating Virtual Appliances”](#) on page 37.

When Update Manager examines systems for patch compliance, it checks whether the latest patch is applied based on information on that system. Patch information is used for this process; the patch itself is not required. Machines that are not compliant with baselines are identified using these comparisons. To improve efficiency and save disk space, patches for virtual machines are only downloaded after a need is identified.

The first time a virtual machine is to be remediated, the applicable patches are downloaded to the Update Manager server and the patches are applied. The details of how a patch is applied, such as whether it is applied immediately or at a later time, are determined by the combination of what is possible under the conditions, and what the user requests. For example, if Update Manager is configured to remediate machines, but those machines are not in a state in which remediation is possible (such as ESX Server hosts being powered off), the process is deferred until the action is possible.

After a patch is downloaded, it is kept indefinitely in the patch download directory. When other machines are remediated, the patch resource is already present on the server.

Update Manager might be deployed in such a way that it cannot conveniently download patches. For example, Update Manager might be deployed on an internal network segment that does not have reliable Internet access. Update Manager Download Service downloads and stores patches on the machine on which it is installed, so that Update Manager servers can use them later.

You can configure Update Manager to use an Internet proxy to download patch information and patches. See [“Configuring Update Manager for Use with an Internet Proxy”](#) on page 22.

Scanning Virtual Machines and ESX Server Hosts

Scanning is the process in which attributes of a set of hosts or virtual machines are evaluated against a standard, which is called a *baseline*. You can scan ESX Server 3.5 and later, ESX Server 3i version 3.5 and later, as well as virtual machines running Windows or Linux. You can scan an ESX Server installation to determine whether the latest patches are applied, or you can scan a virtual machine to determine whether the latest patches are applied to its operating system.

Scans for updates are operating-system specific. For example, Update Manager scans Windows virtual machines to ensure that they have a particular set of patches, but does not scan the same machines to determine whether Linux patches are installed.

In the virtual infrastructure, all objects except resource pools can be scanned.

You can perform scans on both online as well as offline virtual machines and templates.

Baselines

Scanning compares the state of a host or virtual machine against a baseline. A baseline describes a collection of one or more updates such as service packs, patches, or bug fixes. With a single baseline, checking whether all the individual updates that make up the baseline were applied to the objects being scanned, becomes a one-step procedure.

At regular intervals, Update Manager queries update repositories that vendors provide to find available patches. The server for patch information and the contents of the patches are authenticated by using a full-featured public key infrastructure. To help ensure security, patches are typically cryptographically signed by vendors and are downloaded over a secure connection.

Update Manager offers the following types of baselines:

- **Dynamic** – The significance of each update determines the content of the baseline. For Windows, updates are either critical or optional.

The contents of a dynamic baseline are determined based on available updates that meet the specified criteria. As the set of available updates changes, dynamic baselines are updated as well. You can explicitly include or exclude any updates, and these exceptions persist indefinitely.

- **Fixed** – The user manually specifies all updates included in the baseline from the total set of patches available in Update Manager. Fixed updates are typically used to check whether systems are prepared to deal with particular issues. For example, you might use fixed baselines to check for compliance with patches to prevent a worm such as Blaster.

Update Manager includes four preestablished dynamic baselines that you can use to scan any virtual machine, virtual appliance (the baselines for virtual machines and appliances are one and the same), or host to determine whether they have all patches applied for the different categories:

- **Critical Virtual Machine Updates** – Checks virtual machines for compliance with all critical Windows updates.
- **Non-critical Virtual Machine Updates** – Checks virtual machines for compliance with all optional Windows updates.
- **Critical Host Updates** – Checks ESX Server hosts for compliance with all critical updates.
- **Non-critical Host Updates** – Checks ESX Server hosts for compliance with all optional updates.

You can also create a dynamic baseline that includes both critical and optional updates.

Several baseline attributes appear in the Update Manager user interface:

- **Name** – Identifies different baselines. The name can be modified, as required. It is established when a baseline is created.

- **Updates** – Specifies the number of updates included in the baseline. Some updates, such as service packs, include many smaller patches that might have been distributed individually in the past. Because the number of updates does not directly indicate the extent of the updates included in the baseline, this information shows the quantity, rather than the quality. The number of updates might indicate how long a scan and remediation might take to complete.
- **Last Modified** – Specifies the last time updates were added to or removed from this baseline. This date reflects the last time updates changed either because of automatic changes resulting from dynamic updates or from manual user changes. Reviewing the last update information can help provide an idea of whether expected changes were made to baselines.
- **Baseline Type** – Identifies the type of the particular baseline. Possible values include Dynamic, Fixed, or Dynamic (modified). Dynamic (modified) baselines are dynamic baselines that users modify to include or exclude specific updates, counter to the basic criteria of the dynamic baseline.

Administrators can create new baselines, edit existing baselines, detach baselines, or remove (delete) baselines. For large organizations with different groups or divisions, each group can define their own baselines. Administrators can filter the list of baselines by searching for a particular string or by clicking on the headers for each column to sort by those attributes. This functionality uses the capabilities that all VirtualCenter views provides.

Remediation

Remediation is the process in which Update Manager applies updates to ESX Server hosts, virtual machines, or virtual appliances after a scan is complete. Remediation helps ensure that machines and appliances are secured against known potential attacks and have greater reliability resulting from the latest fixes. While remediation provides benefits, you might not remediate machines. For example, your organization might determine that the fix is not significant enough to warrant application, or a machine might be running legacy processes that do not function if the latest patches are applied.

You can remediate machines and appliances in much the same ways that you can scan them. As with scanning, you can not only remediate a single virtual machine or virtual appliance, but you can also initiate remediation scan on a folder of virtual machines, a cluster, or a datacenter, or all objects in your virtual infrastructure. As with scanning, resource pools are the only VMware Infrastructure object type that can never be remediated. Remediation is supported for:

- Powered on, suspended, or powered off Windows virtual machines and appliances.
- Templates for Windows virtual machines.
- Hosts running ESX Server 3.5.0 or higher.

Update Manager Settings

The virtual machine and ESX Server remediation process is configurable. Configurable options include:

- When to check for updated patch information.
- When to scan or remediate virtual machines or ESX Server hosts.
- How to handle preremediation snapshots of virtual machines. Update Manager can create snapshots of virtual machines before remediation. If you configure Update Manager to create snapshots, you can configure the snapshots to be kept indefinitely or to be deleted after a specified period.
- Whether to create snapshots of virtual machines before remediation, whether to store the snapshot, and for how long.
- How to handle failures to remediate ESX Server hosts.

For more information on security configuration, see [“Configuring Update Manager”](#) on page 20.

Working with Update Manager

Follow the procedures described in this chapter to facilitate upgrades and patching of ESX Server installations, guest operating systems, and applications. Using current versions of software helps establish a consistently secure and patched environment.

This chapter discusses the following topics:

- [“Installing, Upgrading, and Uninstalling Update Manager”](#) on page 11.
- [“Update Manager Network Port Requirements”](#) on page 19.
- [“Configuring Update Manager”](#) on page 20.
- [“Working with Baselines”](#) on page 25.
- [“Scanning Virtual Machines and ESX Server Hosts”](#) on page 29.
- [“Remediating ESX Server Hosts and Virtual Machines”](#) on page 32.
- [“Working with Update Manager Events”](#) on page 34.
- [“Working with Updates”](#) on page 35.
- [“Managing Virtual Appliances”](#) on page 36.

Installing, Upgrading, and Uninstalling Update Manager

Update Manager is installed as part of the installation process for VirtualCenter. If you have an established VMware Infrastructure environment, you can use the same installer to add Update Manager functionality.

You can install Update Manager either on the same computer as the VirtualCenter Server or on a different computer. Update Manager can be installed on computers running the following operating systems:

- Windows XP SP2
- Windows Server 2003

Update Manager is compatible with other VirtualCenter add-ons such as VMware Converter Enterprise for VirtualCenter.

The Update Manager disk storage requirements vary depending on your deployment. For more information, see the *VMware Update Manager Sizing Estimator*.

Update Manager server and Update Manager Download Service store patch metadata in Microsoft SQL Server or Oracle databases. Update Manager supports the database formats listed in [Table 2-1](#).

Table 2-1. Supported Database Formats

Database Type	Patch and Driver Requirements
SQL Server 2000 SP 4	Use SQL Server driver for the client.
SQL Server 2005 SP1	Use SQL Native Client driver for the client.
SQL Server 2005 Express	Use SQL Native Client driver for the client.
Oracle 9i	Apply patch 9.2.0.8.0 to server and client.
Oracle 10g Release 1 (10.1.0.2)	Apply patch 10.1.0.3.0 to server and client.
Oracle 10g Release 2 (10.2.0.1.0)	First apply patch 10.2.0.3.0 to server and client and then apply patch 5699495 to the client. (SEE UPDATE)

Before you install Update Manager, gather information about the environment into which you are installing Update Manager. Information to collect includes the following:

- Networking information about the VirtualCenter Server that Update Manager will work with. Defaults are provided in some cases, but you might want to ensure that you have the correct information, including:
 - IP address.
 - Port number. In most cases, the Web service ports (80 and 443 by default) are used.
- Administrative credentials required to complete the installation, including:
 - The user name for an account with sufficient privileges. This is often root or Administrator.
 - The password for the account that will be used for the installation.

To Install Update Manager

- 1 Insert the Installer CD into the CD-ROM drive of the server that will host the Update Manager server.
- 2 Click **Next**.
- 3 Click **Next**.
- 4 Accept one of the options and click **Next**.
- 5 Enter your name and organizational information and click **Next**.
- 6 Select **VMware VirtualCenter Server**.

If you have already installed components such as VMware Infrastructure Client, VirtualCenter Server, or VMware Converter Enterprise for VirtualCenter, a message appears informing you that these components are installed. You can continue the installation of other components such as Update Manager.

If you select the **Custom** option, you can configure what database VMware Update Manager uses, change proxy server settings, and customize where Update Manager is installed and where patches are stored.

- 7 Click **Next**.

The VirtualCenter Server Authorization page appears.

- 8 Enter information about the VirtualCenter Server and Administrator account that this Update Manager server will work with.
 - a In the **VC Server IP** text box, enter an IP address or accept the default.
 - b In the **VC Server Port** text box, enter a Port number or accept the default.
 - c In the **Administrator** text box, enter the name of the administrative account you will use to complete this installation.

- d In the **Password** and **Verify Password** text boxes, enter the password for the administrative account you will use to complete this installation.
 - e Click **Next**.
- 9 Click **Install** to begin the installation.

Preparing the Update Manager Database

Update Manager server requires a database to store and organize server data. Update Manager supports Oracle, Microsoft SQL Server, and Microsoft SQL Server 2005 Express.

NOTE Microsoft SQL Server 2005 Express is intended to be used for small deployments of up to 5 hosts and 50 virtual machines.

For an Update Manager database to be supported, you must create a database instance and configure it to ensure that all Update Manager database tables are placed in it.

Configuring an Oracle Connection to Work Locally

Before you begin the following procedure, review the required database patches specified in [Table 2-1](#). If you do not prepare your database correctly, the Update Manager installer might display error or warning messages.

To prepare an Oracle database to work locally with Update Manager

- 1 Download Oracle 9i, or Oracle 10g from the Oracle Web site, install it, and create a database (for example, VUM).
- 2 Download Oracle ODBC from the Oracle Web site.
- 3 Install the corresponding Oracle ODBC driver through the Oracle Universal Installer.
- 4 Increase the number of open cursors for the database. Add the entry `open_cursors = 300` to the `<ORACLE_BASE>\ADMIN\VUM\pfile\init.ora` file.

Here `<ORACLE_BASE>` is the root of the Oracle directory tree.

To connect to the Oracle database locally

- 1 Create a new tablespace specifically for Update Manager by using the following SQL statement:

```
CREATE TABLESPACE "VUM" DATAFILE '<ORACLE_BASE>\ORADATA\VUM\VUM.dat' SIZE 1000M AUTOEXTEND
ON NEXT 500K;
```

Here `<ORACLE_BASE>` is the root of the Oracle directory tree.

- 2 Create a user, such as `vumAdmin`, for accessing this tablespace through ODBC:

```
CREATE USER vumAdmin IDENTIFIED BY vumadmin DEFAULT TABLESPACE vum;
```

- 3 Either grant `dba` permission to the user, or grant the following permissions to the user:

```
grant connect to <user>
grant resource to <user>
grant create view to <user>
grant create any sequence to <user>
grant create any table to <user>
grant unlimited tablespace to <user> # To ensure space limitation is not an issue
```

- 4 Create an ODBC connection to the database. The following are example settings:

```
Data Source Name: VUM
TNS Service Name: VUM
User ID: vumAdmin
```

Configuring an Oracle Connection to Work Remotely

Before you begin the following procedure, review the required database patches specified in [Table 2-1](#). If you do not prepare your database correctly, the Update Manager installer might display error and warning messages.

To use an Oracle database as your Update Manager database and have Update Manager access the database remotely, first set up the database as described in “[Configuring an Oracle Connection to Work Locally](#)” on page 13.

To prepare an Oracle database to work remotely with Update Manager

- 1 Install the Oracle client on the Update Manager server machine.
- 2 Connect to Oracle remotely.
- 3 Create an ODBC connection to the database. The following are example settings:

```
Data Source Name: VUM
TNS Service Name: VUM
User Id: vumAdmin
```

To connect to Oracle remotely

- 1 Download and install the ODBC driver.
- 2 Edit the `tnsnames.ora` file located under `<ORACLE_HOME>\network\admin\`, as appropriate.
Here `<ORACLE_HOME>` is located under `C:\<ORACLE_BASE>`, and it contains subdirectories for Oracle software executables and network files.
- 3 Use the Net Configuration Assistant to add the following entry:

```
VUM =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS=(PROTOCOL=TCP) (HOST=<host address>) (PORT=1521))
)
(CONNECT_DATA =(SERVICE_NAME = VUM)
)
)
```

In this example, `<host address>` is the managed host the client needs to connect to.

Configuring a Microsoft SQL Server ODBC Connection

When you install Update Manager, you can establish a connection with a SQL Server database. The following procedure describes how to configure a SQL Server ODBC connection. If you use SQL Server for Update Manager, do not use the master database.

Before you begin this procedure, review the required database patches specified in [Table 2-1](#). If you do not prepare your database correctly, the Update Manager installer might display error and warning messages.

See your Microsoft SQL ODBC documentation for specific instructions regarding configuring the SQL Server ODBC connection.

To prepare a Microsoft SQL Server database to work with Update Manager

- 1 On your Microsoft SQL Server, perform the following tasks:
 - a Create a SQL Server database by using Enterprise Manager on the SQL Server.
You define the default database for the database operator (DBO) user.
 - b Create a SQL Server database user with DBO rights.

Make sure the database user has either a **sysadmin** server role or the **db_owner** fixed database role on the Update Manager database and the MSDB database.

The **db_owner** role on the MSDB database is required for installation and upgrade only. This role can be revoked after the installation or upgrade process is completed.

- 2 On your Update Manager server system, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.
- 3 Click the **System DSN** tab.
- 4 Create or modify a SQL Server ODBC connection.
 - To create a SQL Server ODBC connection:
 - i Select **Create New Data Source** and click **Add**.
 - ii For SQL Server 2000, select **SQL Server** and click **Finish**.
For SQL Server 2005, select **SQL Native Client** and click **Finish**.
 - To modify an existing SQL Server ODBC connection:
 - i Select the SQL Server ODBC DSN to modify.
 - ii Select the appropriate ODBC connection from the **System Data Source** list and click **Configure**.
- 5 Type an ODBC DSN in the **Name** field.
For example, type VUM.
- 6 (Optional) Type an ODBC DSN description in the **Description** field.
- 7 Choose the DSN server name from the **Server** drop-down menu.
Type the SQL Server machine name in the text field if you cannot find it in the drop-down menu.
- 8 Configure the SQL Server authentication page and click **Next**.
- 9 Select an authentication method:
 - If you are using local SQL Server, select **Windows NT authentication**.
 - If you are using remote SQL Server, select the appropriate SQL Server authentication method.

The authentication option you choose for a remote SQL Server must match the settings for that server.



CAUTION If you use the SQL Server authentication method, in the Update Manager installation wizard supply the same user name, password, and ODBC system data source name (DSN) that you used to configure the ODBC.

- 10 Type your SQL Server login name and password.
Ask your database administrator for this information.
- 11 Configure the default database and click **Next**.
- 12 Select a database from the **Change the default database to** menu and click **Next**.
- 13 Click **Finish**.
- 14 In the ODBC Microsoft SQL Server Setup window, click **Test Data Source**.
If the test data source is acceptable, click **OK**. If it is not acceptable, repeat the procedure to reconfigure any incorrect items.
To close the ODBC Data Source Administrator, click **Close**.
- 15 Ensure that the SQL Server Agent is running on your database server.
Double-click the SQL Server icon in the system tray and view whether the SQL Server Agent is running.
This is applicable to SQL Server 2000 and SQL Server 2005 editions.

To identify the SQL Server authentication type

- 1 Open SQL Server Enterprise Manager.
- 2 Click the **Properties** tab.
- 3 Check the connection type. The connection type indicates either Windows NT or SQL Server authentication.

Configuring Microsoft SQL Server 2005 Express

The Microsoft SQL Server 2005 Express database package is installed and configured when you select Microsoft SQL Server 2005 Express as your database during the VMware Update Manager installation. No additional configuration is required.

If Microsoft SQL Server 2005 Express is installed, review the required database patches specified in [Table 2-1](#). If you do not prepare your database correctly, the Update Manager installer might display error and warning messages.

Maintaining Your Update Manager Database

After your Update Manager database instance and Update Manager are installed and operational, perform standard database maintenance processes. These include:

- Monitoring the growth of the log file and compacting the database log file, as needed. See the documentation for the database type you are using.
- Scheduling regular backups of the database.
- Backing up the database before any Update Manager upgrade.

See your database documentation for information on backing up your database.

Installing the Guest Agent

The VMware Update Manager Guest Agent facilitates Update Manager processes. For both Linux and Windows operating systems, the Guest Agent is installed the first time a remediation is scheduled or when a scan is initiated on a powered-on virtual machine. For best results, ensure that the latest version of the Guest Agent is installed.

If the Guest Agent installation does not complete successfully, operations such as scanning and remediation fail. In such a case, manually install the Guest Agent.

The Guest Agent installation packages for Windows and Linux guests are in the directory you specified during the Update Manager installation. In that directory, the Guest Agent installation packages are located at `\docroot\vmci\guestAgent\`. For example, if Update Manager is installed in `C:\Program Files\VMware\Infrastructure\Update Manager`, the Guest Agent installers are at `C:\Program Files\VMware\Infrastructure\Update Manager\docroot\vmci\guestAgent\`.

The Guest Agent requires no user input, and the installation completes silently. For Windows, start the installer by running the `VMware-UMGuestAgent.exe` file. For Linux, install the `VMware-VCIGuestAgent-Linux.rpm` file by running the `rpm -ivh VMware-VCIGuestAgent-Linux.rpm` command.

Installing the Update Manager Download Service

Update Manager Download Service downloads updates that would not otherwise be available to Update Manager servers. For example, for security reasons and deployment restrictions, VMware Infrastructure, including Update Manager, is installed in an air gap network—a secured network that is disconnected from other local networks and the Internet. Update Manager requires access to patch information to function properly.

The Download Service provides a solution in such situations. Download Service downloads updates for:

- ESX Server 3i or higher, and ESX Server 3.5 or higher.
- All Update Manager supported versions of Windows virtual machines.

To use the Update Manager Download Service, you must set up a server to be your Update Manager Download system. This server must have Internet access.

After the Download Service downloads updates, the updates can be exported by CD or USB key device as well as automatically to a VirtualCenter Server running Update Manager.

The amount of space required to store the updates on the server on which the Download Service is installed varies based on the number of different operating systems and applications you intend to patch, as well as the number of years you intend to gather patches on this system. Allocate 50 GB for each year of ESX Server patching, and 11 GB for each virtual machine operating system and locale combination. For example, to use the server for two years to patch hosts Windows XP US English and Windows Server 2003 requires 100 GB for the hosts and 44 GB for the virtual machines for a total of 144 GB. To install the Download Service in such an environment, install it on a server with at least 144 GB of available space for patch storage.

The Download Service installer requires a database. The installation program includes an option to create a SQL Server 2005 Express database, or you can use an existing Microsoft SQL Server or Oracle database.

To install the Update Manager Download Service

Open the VMware-UMDS.exe file located in the umds folder on the installation CD. Use the VMware Update Manager Download Service installation wizard to complete the installation.

During the installation, you can modify the SOAP port, Web port, and proxy settings. If you keep the default settings during the installation and want to change the Update Manager Download Service proxy authentication settings later, use the [“To manually update proxy authentication information”](#) on page 22 procedure.

Upgrading VI Client to Support Update Manager

Starting with VirtualCenter version 2.5, Update Manager clients are delivered as a plug-in for the VI Client. The Update Manager functionality is an integral part of VirtualCenter, and the new VI Client supersedes previous VI Client releases.

After installing Update Manager, update at least one VI Client, so you can configure Update Manager. You must install the Update Manager plug-in on any VI Client that you want to use to manage Update Manager, but you do not need to update all clients if you do not want to. Any combination of VI Client with Update Manager plug-in and VI Client with some or no other plug-ins can connect to a given VirtualCenter Server without a conflict.

To enable Update Manager on a VI Client

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Choose **Plugins > Manage Plugins**.
- 3 Click **Download and install** for the Update Manager plug-in.
- 4 Complete the Update Manager client installation and click **OK**.
- 5 Click the **Installed** tab on the Plugin Manager page.

The VMware Update Manager client plug-in might not be immediately available. You might need to wait up to a minute before the Update Manager client is shown on the **Installed** tab.

- 6 Select **Enabled**.
- 7 Dismiss any **Security Warning** dialog boxes that appear by clicking **Yes** or **Ignore**, and then click **OK**.

The Update Manager button might not always immediately appear in the VI Client. After installing the VMware Update Manager plug-in, if the button does not appear, restart the VI Client.

Upgrading Update Manager

Update Manager upgrades are available from Update Manager 1.0 to the latest Update Manager release, that is Update Manager 1.0 Update 2. Before you upgrade Update Manager, be sure to upgrade both VirtualCenter Server and VI Client to a compatible version.

For a better idea of the compatibility, see the compatibility matrix in [Table 2-2](#).

Table 2-2. Compatibility Matrix

Update Manager	VirtualCenter			VI Client		
	2.5	2.5 Update 1	2.5 Update 2	2.5	2.5 Update 1	2.5 Update 2
1.0	Yes	No	No	Yes	No	No
1.0 Update 1	No	Yes	No	No	Yes	No
1.0 Update 2	No	No	Yes	No	No	Yes

Update Manager server and Update Manager client must be the same version.

To upgrade Update Manager to Update Manager 1.0 Update 2

- 1 Stop the VirtualCenter and Update Manager services.
- 2 Make a backup copy of the Update Manager database manually.
- 3 Upgrade VirtualCenter 2.5 to VirtualCenter 2.5 Update 2.
- 4 Upgrade Update Manager to Update Manager 1.0 Update 2.
- 5 Upon connecting to Update Manager, the VI Client will detect the correct Update Manager version and prompt you to install it, if you have not installed it yet.

When you upgrade Update Manager using an existing Update Manager database schema, even if you uninstall Update Manager, the installer will still upgrade the database based on the existing schema. If you want to create a fresh database schema, uninstall the old Update Manager server, install the Update Manager 1.0 Update 2 server, and create a new database during the installation.

If you use the unified installer to upgrade VirtualCenter, Update Manager will be upgraded automatically.

If you use the standalone installer to upgrade Update Manager, the installer checks the VirtualCenter version, and in case of incompatibility, the installer displays an error message and stops the installation process.

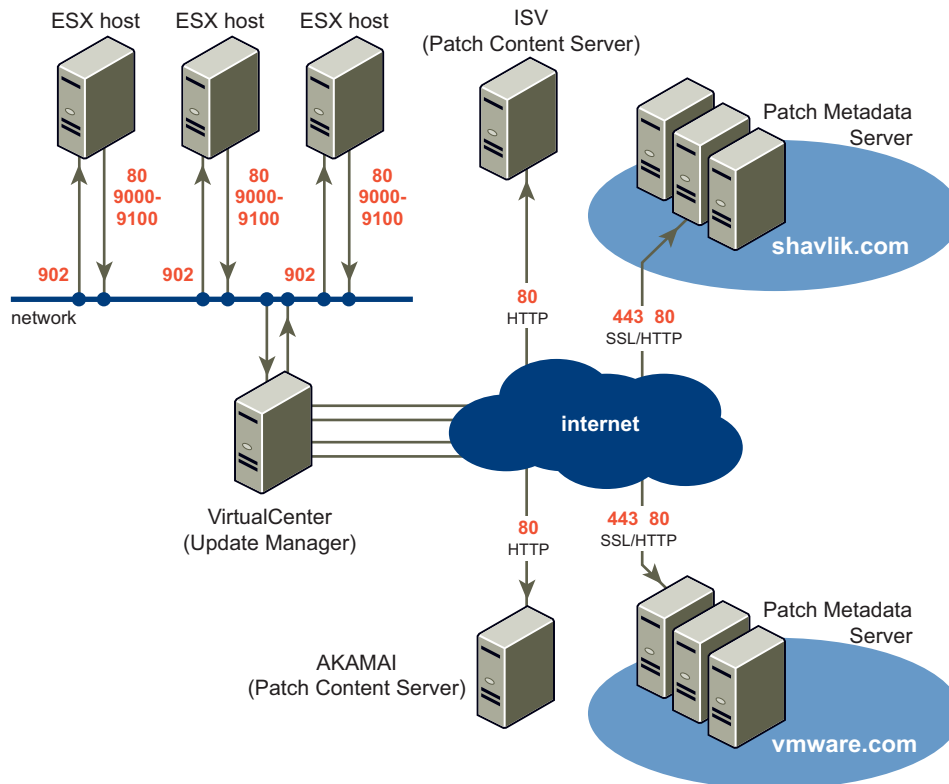
Uninstalling Update Manager

Update Manager has a relatively small impact on computing resources such as disk space, so unless you are certain that you want to remove it, leave an existing installation in place for later use. You can remove Update Manager by using the Windows Add/Remove programs functionality. If you uninstall Update Manager, you might also want to uninstall the Update Manager plug-in from the VI Client. To do this, use the Windows Add/Remove programs functionality on the machine on which the client is installed. After Update Manager client is removed from the VI Client, the Update Manager button disappears, although patch binaries and log data remain on the Update Manager servers. Update Manager has a relatively small impact on computing resources such as disk space, so unless you are certain that you want to remove it, leave an existing installation in place for later use.

Update Manager Network Port Requirements

After you install Update Manager if the default settings are kept during the installation, the Update Manager Web server listens on 9084 TCP and the Update Manager SOAP server listens on 8084 TCP. Both are accessed through a reverse proxy that listens on the standard ports 80 and 443. For more information, see [Figure 2-1](#).

Figure 2-1. Update Manager Network Port Requirements



When Update Manager and the VirtualCenter Server are installed on the same machine:

- All incoming connections to Update Manager are accessed through a reverse proxy provided by the VirtualCenter Server.
- ESX Server connects to port 80, and the VirtualCenter Server forwards the request to the Update Manager Web server listening on port 9084 for host patch downloads.
- The VirtualCenter Server directly connects to Update Manager on port 8084 because they are on the same machine.
- Update Manager connects to ESX Server on port 902 for pushing the virtual machines patches.

When Update Manager and the VirtualCenter Server are installed on two different machines:

- Update Manager has a reverse proxy listening on ports 80 and 443 if the default is not changed during the installation.
- The VirtualCenter Server connects to Update Manager through port 443. The reverse proxy forwards the request to 8084.
- ESX Server connects to Update Manager through port 80. The reverse proxy forwards the request to 9084.
- Update Manager connects to ESX Server on port 902 for pushing the virtual machines patches.

To obtain metadata for the updates, Update Manager must be able to connect to <http://www.vmware.com> and <http://xml.shavlik.com>, and requires outbound ports 80 and 443.

For more information about configuring the port settings after the installation, see “[Configuring the Update Manager Network Port Settings](#)” on page 22.

Configuring Update Manager

You can modify the administrative settings for Update Manager before you to use it. The administrative settings determine the following:

- What action Update Manager takes if a remediation fails for either a guest virtual machine or an ESX Server installation.
- How often Update Manager checks for new updates.
- How Update Manager works with an Internet proxy.
- How Update Manager can be configured to work with new port settings.
- How to change the location in which Update Manager downloads patches.

Responding to Guest Remediation Failure

Update Manager can take snapshots of virtual machines before applying updates. This ensures that if a patch cannot be applied, the state of the virtual machine before the update is easily re-established. You can elect to keep these snapshots indefinitely or for a fixed period.

- Keeping snapshots indefinitely might eventually consume a large amount of disk space and degrade virtual machine performance, but these snapshots provide protection against problems with patching.
- Keeping no snapshots saves space in your environment, ensures best virtual machine performance, and might reduce the amount of time it takes to complete remediation.
- Keeping snapshots for a set period is a compromise between the other two choices.

The configuration described in the following procedure, determines the default settings for remediation failures. You can specify alternative settings to these defaults when you configure individual remediation tasks.

To configure guest snapshot behavior

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Configuration** tab.
The **Guest Settings** link on the left is selected by default.
- 3 Select **Snapshot the virtual machines before applying updates to enable rollback**.
- 4 Configure snapshots to be kept indefinitely or for a period of time.
- 5 Click **Apply**.

Responding to a Failure to Put ESX Server in Maintenance Mode

Update Manager puts ESX Server in maintenance mode before applying updates. Virtual machines cannot continue to run when an ESX Server is in maintenance mode. To ensure a consistent user experience, the VirtualCenter Server migrates virtual machines to other ESX Server hosts within a cluster before the server being remediated is put in maintenance mode. VirtualCenter Server can migrate the virtual machines, if the cluster is configured for VMotion. For other containers or individual hosts that are not in a cluster, migration cannot be performed. If VirtualCenter server cannot migrate the virtual machines to an alternative host, Update Manager can take one of the following actions:

- **Fail Task** – Log this failure in the Update Manager logs and take no further action.
- **Retry** – Wait for the retry delay period and repeat the attempt to put the server into maintenance mode as many times as you indicate in the **Number of retries** field.

- **Power Off and Retry** – After the failure power off all of the running virtual machines, and try entering the server into maintenance mode as many times as you indicate in the **Number of retries** field. Virtual machines are shut down as though their power-off button is used, which has different results depending on configuration.
- **Suspend and Retry** – Suspend all the running virtual machines as per the virtual machine settings specified by the VirtualCenter Server user interface suspend button, and try entering the server into maintenance mode as many times as you indicate in the **Number of retries** field.

The configuration described in the following procedure determines the default settings for remediation failures. You can specify alternative settings to these defaults when you configure individual remediation tasks.

NOTE If you are managing a cluster of hosts, ensure that Distributed Power Management is disabled. Otherwise some of your hosts might not be patched.

To configure how Update Manager responds to failures to enter maintenance mode

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click **Update Manager** button.
- 2 Click the **Configuration** tab.
- 3 Click **ESX Host Settings** on the left.
- 4 Select an option from the **Failure response** drop-down menu to determine how Update Manager responds if an ESX Server host cannot be put in maintenance mode.
- 5 Configure the options to correspond to the failure response option you select.
- 6 Click **Apply**.

Checking for Updates

Update Manager is designed to check for new updates at regular intervals. Gathering current information about updates that are applicable to your environment allows Update Manager to work as expected. For most cases, accept the default settings. If you have an environment with applications that receive frequent patches or that must receive the latest patches as soon as they are released, you can decrease the duration between checks for updates. If you are not as concerned about the latest patches, want to reduce network traffic, or cannot access the patch servers, you can increase the duration between checks or stop checking for updates. Updates are downloaded according to a single schedule. You can modify this schedule.

To modify checking for updates

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Configuration** tab.
- 3 Click the **Update Downloads** link on the left.
A description of the pre-defined scheduled task to download software updates appears.
- 4 Click the **Edit Update Downloads** link in the upper-right corner.
The Schedule Update Download wizard appears.
- 5 Select the type of updates to be downloaded.
The options are: **ESX Server updates**, **All Windows updates**, and **All Linux updates**.
- 6 Click **Next**.
- 7 Specify a task name and description, and when updates will be downloaded.
- 8 Click **Next**.

- 9 (Optional) Specify one or more addresses to receive email with information about the results of the update download process when the new updates are downloaded.
To have this option working, the mail settings for the VirtualCenter Server must be configured correctly.
- 10 Click **Next**.
- 11 Click **Finish**.

Configuring Update Manager for Use with an Internet Proxy

After installing Update Manager, you can modify the configuration to work with an Internet proxy server by using the **Custom Install** option in the installation program. To do this, restart the installation process and provide new proxy configuration information. The installation process is described in [“To Install Update Manager”](#) on page 12.

You can modify the configuration both manually and through the Update Manager plug-in.

To manually update proxy authentication information

- 1 Log in to the Update Manager server as an administrator.
- 2 Stop the Update Manager service.
 - a Right-click **My Computer** and click **Manage**.
 - b In the left pane, expand **Services and Applications** and click **Services**.
 - c In the right pane, right-click the **VMware Update Manager Service**, and click **Stop**.
- 3 Open the `vum-proxyAuthCfg.exe` file in the Update Manager directory.
The default location is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- 4 Provide updated proxy authentication information.
- 5 Restart the Update Manager service.

To modify the proxy configuration through the Update Manager plug-in

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Configuration** tab.
- 3 Click the **Internet Access** link on the left.
- 4 Change the default proxy information as necessary.
If the proxy requires authentication, select the **Proxy requires authentication** check box and provide username and password.
- 5 (Optional) Test the connection.
The **Test Connection** button allows you to enter the Internet access settings, and test the connectivity of the Update Manager server with the Internet before actually applying the new settings.
- 6 Click **Apply**.

Configuring the Update Manager Network Port Settings

After you install Update Manager, you can configure its port settings to avoid conflicts with other programs installed on the same machine.

If VirtualCenter is installed on the same machine, you cannot change the HTTP and HTTPS ports. Update Manager doesn't open these ports, but VirtualCenter does. If VirtualCenter is not installed on the same machine, Update Manager starts its own reverse proxy. In this case, you are able to change both the HTTP and HTTPS ports.

If Update Manager and VirtualCenter are installed on the same machine and the VirtualCenter HTTP port is not in the 80 or 9000–9100 range, the access patch depot through Web port (not through reverse proxy) must be enabled and the Web port must be in the 80, 9000–9100 range.

ESX Server hosts use only HTTP and not HTTPS. The range limitation for the HTTP port depends on the option to access patch depot through Web port. ESX Server hosts can only open the outbound connections on port in the 80 or 9000–9100 range for accessing patch depot Web servers.

The benefits of the access patch depot through Web port, are the improved performance for large files due to elimination of data copying in reverse proxy and the leverage of any advanced features of the Web server.

Before changing the port settings, check for conflicts with other port settings.

To change the port settings

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Configuration** tab.
- 3 Click the **Port Settings** link on the left.
- 4 Change the network port settings as necessary.
 - a **Port used by client to communicate with VMware Update Manager server (SOAP port)** – This is the port that Update Manager client uses to communicate with the Update Manager server. There are no limitations except for the non-conflicting requirement.
 - b **Port used to provide plugin client installer and access to patch depot (Web port)** – This is the listening port for the Web server that provides access to the plug-in client installer (VirtualCenter makes the request), and provides access to the ESX Server hosts patch depot (the ESX Server hosts make the request). The port range limitation depends on the option to access patch depot through Web port.
 - c **Port used as reverse proxy (HTTP port)** – Port used as reverse proxy. This port may not be opened by Update Manager, depending on whether VirtualCenter is installed on the same machine as Update Manager.
 - d **Port used as reverse proxy with SSL connection (HTTPS port)** – Port used as reverse proxy. This port may not be opened by Update Manager, depending on whether VirtualCenter is installed on the same machine as Update Manager.
 - e **Access patch depot through Web port (not through reverse proxy)** – Use this option to direct ESX Server hosts which port to use for host scanning.
 - If you select the check box, the ESX Server hosts use the Update Manager’s Web port to access the patch depot. There is no restriction for the HTTP port, but the Web port must be in the range of 80 or 9000–9100.

Before selecting the check box, make sure that any firewall on the Update Manager host does not block its listening port.
 - If you do not select the check box, the ESX Server hosts use the reverse proxy port to access the patch depot, and the HTTP port must be in the range of 80 or 9000–9100. There is no restriction for the Web port.
- 5 Click **Apply**.

NOTE Any change in the port setting requires a restart of the Update Manager server to take effect.

Configuring Update Manager Patch Download Location

When you install Update Manager, the installation wizard allows you to change the location for downloading patches. If you keep the default location during the installation, and want to change it later, without reinstalling Update Manager, you have to do it manually.

To configure the Update Manager patch download location

- 1 Stop the Update Manager service.
- 2 Find the `vci-integrity.xml` file in the Update Manager installation directory.
The default location is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- 3 Create a backup copy of this file in case you need to revert to the previous configuration.
- 4 Edit the file by changing the following fields:

```
<patchStore>yournewlocation</patchStore>
```

The default patch download location is:

```
C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\
Data\
```

The directory path must end with `\`.

Save the file in UTF-8 format, and replace the existing file.

- 5 Copy the contents from the old patchstore directory to the new folder.
- 6 Restart the Update Manager service.

Using the Update Manager Download Service

Use the Update Manager Download Service to initiate downloads of updates and to transfer the updates to Update Manager. Establish a depot in which to place the updates. After the updates are in the depot, export the newly downloaded updates to some portable storage device such as a CD or USB key and import them to the Update Manager server. If Update Manager is installed on a machine that is not connected to the Internet, the scheduled update checks fail. In such a case, disable the scheduled update checks and use the Update Manager Download Service as the only means to download and transfer updates to Update Manager.

You can automate the Update Manager Download Service in a semi air gap deployment – a deployment in which you can transfer files from the machine on which Update Manager Download Service is installed to a machine on which Update Manager server is installed using a shared folder. This shared folder can be on the same machine on which Update Manager is installed or on a remote server.

The best practise is to create a script to download the updates manually and set it up as a Windows Scheduled Task that downloads the updates automatically.

To use the Update Manager Download Service (SEE UPDATE)

- 1 Log in to the machine on which Update Manager Download Service is installed.
- 2 Choose **Start > Run**, type `cmd` and press Enter.
- 3 Change to the directory where Download Service is installed.
The default folder is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- 4 Setup what updates to download:
 - To setup a download of all ESX Server host updates, enter the following command:
`vmware-umds --set-config -enable-host 1 --enable-win 0 --enable-lin 0`
 - To setup a download of all Windows updates, enter the following command:
`vmware-umds --set-config -enable-host 0 --enable-win 1 --enable-lin 0`

- To setup a download of all Linux updates, enter the following command:

```
vmware-umds --set-config --enable-host 0 --enable-win 0 --enable-lin 1
```
 - To setup a download of all available updates, enter the following command:

```
vmware-umds --set-config --enable-host 1 --enable-win 1 --enable-lin 1
```
- 5 Run the program to download updates by entering the following command:

```
vmware-umds --download
```

If you have already downloaded updates and want to download some of them again, include start and end time, to restrict the updates to download. For example, if you want to download the updates released in May, 2008, enter the following command:

```
vmware-umds --re-download --start-time 2008-05-01T00:00:00 --end-time 2008-05-31T23:59:59
```

6 To export the downloads repeat [Step 1 – Step 3](#).

For example, if you want to export all updates for the year 2007, enter the following command:

```
vmware-umds --export --dest <repository_path> --start-time 2007-01-01T00:00:00 --end-time 2007-12-31T23:59:59
```

Here, `<repository_path>` is the full path to your export directory.

If your deployment is a semi air gap one, `<repository_path>` points to the shared folder on the remote server. If the shared folder is on the machine on which Update Manager server is installed, continue with [Step 9](#).

7 After exporting downloads to a folder, physically move them to a portable media drive.

8 Connect the portable drive to the machine on which the Update Manager is installed.

9 Repeat [Step 2](#) and change to the directory where Update Manager is installed.

The default folder is `C:\Program Files\VMware\Infrastructure\Update Manager`.

10 To import Windows and ESX Server host updates, enter the command:

```
vmware-updateDownloadCli.exe --update-path <local_path> --config-import windows esx --vc <IP_address:port> --vc-user <vc_user>
```

Here, `<local_path>` is the path to the folder or drive where the software updates are exported, `<IP_address:port>` are the Virtual Center Server IP and port (if the Update Manager and VirtualCenter Server are installed on different machines), and `<vc_user>` is your VirtualCenter username.

NOTE You can also use the Windows Scheduled Task wizard to schedule Download Service to run at regular intervals.

Working with Baselines

Update Manager includes four standard baselines:

- Non-critical host updates
- Non-critical virtual machine updates
- Critical host updates
- Critical virtual machine updates

You can benefit from customized baselines to meet the needs of your specific deployment. Creating additional, customized baselines allows updates to be grouped into logical sets. You administer baselines by using the **Update Manager** button in the VI Client. This button appears in the VI Client installations that have the Update Manager plug-in installed.

You can view the default baselines by clicking the **Update Manager** button of the VI Client and clicking the **Baselines** tab.

Creating Baselines

You can create additional baselines by using Update Manager through the New Baseline wizard. These baselines can be either dynamic or fixed. Dynamic baselines consist of a set of updates that meet user-defined criteria. The contents of the set of updates that make up dynamic baselines vary as available updates change. Fixed baselines are composed of a set of updates that users choose.

To create a fixed baseline using the New Baseline Wizard

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.

- 2 On the **Baselines** tab, click **New Baseline**.

The New Baseline wizard appears.

- 3 Provide a name and a description for the baseline, and select a target.

Update Manager does not support baselines that apply to both ESX Server hosts as well as virtual machines. Baselines must apply to either target type.

- 4 Click **Next**.

- 5 Select **Fixed** for the type of baseline.

- 6 Click **Next**.

The Updates page appears.

- 7 Customize the baseline.

- a Select individual updates to include or from your baseline and click the down arrow.

- b To find specific updates to choose from, click **Filter**.

- c In the Updates Filter page, enter search criteria and click **Find**.

- **Text contains** – Enter text to restrict the updates displayed. Text entered in this field is searched for conformity in all text fields of the available updates.

- **Product** – Select operating systems or products for which this baseline will include patches. You can select multiple products or operating systems, but only updates applicable to the product or operating system of the machine being evaluated are scanned.

- **Severity** – Select the severity of updates to be included in this baseline.

- **Language** – Select which language versions of patches to include.

- **Released Date** – Provide **After** and **Before** dates to specify a range for the release dates of the updates.

- **Update Vendor** – Select one of the listed update vendors.

- d Select any further updates.

- 8 Click **Next**.

- 9 Review the Ready to Complete page and click **Finish**.

To create a dynamic baseline using the New Baseline wizard

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 On the **Baselines** tab, click **New Baseline**.
The New Baseline wizard appears.
- 3 Provide a name and a description of the baseline, and select a target.
Update Manager does not support baselines that apply to both target types. Baselines must apply to either ESX Server hosts or virtual machines.
- 4 Click **Next**.
- 5 Select **Dynamic** for the type of baseline.
- 6 Click **Next**.
The Dynamic Baseline Criteria page appears.
- 7 Customize the baseline by entering specific criteria to filter the updates.
 - **Text contains** – Enter text to restrict the updates displayed. Text entered in this field is searched for conformity in all text fields of the available updates.
 - **Product** – Select operating systems or products for which this baseline includes patches. You can select multiple products or operating systems, but only updates applicable to the product or operating system of the machine being evaluated are scanned.
 - **Severity** – Select the severity of updates to be included in this baseline.
 - **Language** – Select which language versions of patches to include.
 - **Released Date** – Provide **Before** and **After** dates to specify a range for the release dates of the updates.
 - **Update Vendor** – Select one of the listed update vendors.
 - **Add or remove specific updates to/from this baseline** – Select the check box to add or remove specific updates.
- 8 Click **Next**.
Depending on the choices you make, one of the following pages appears:
 - The Ready to Complete page, if you just filtered the updates
 - The Exclusions page, if you selected to add or remove specific updates from the baseline.
- 9 In the Exclusions page, select individual updates to exclude from your baseline and click the down arrow.
- 10 Click **Next**.
The Inclusions page appears.
- 11 Select individual updates that do not meet the filter criteria set up in [Step 7](#), to include them in the baseline, and click **Next**.
- 12 Review the Ready to Complete page, and click **Finish**.

Editing Baselines

You can edit existing baselines by using the VI Client.

To edit an existing baseline

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.

- 2 On the **Baselines** tab, select an existing baseline and click **Edit Baseline**.

The Edit Baseline wizard displays.

- 3 Click **Baseline Name** to modify the name and description of the baseline.
- 4 Click **Baseline Type** to change the type of updates included in the baseline.
- 5 Depending on the type of baseline, do one of the following:

- If the baseline is fixed, click **Updates** to add or remove specific updates from the baseline.
- If the baseline is a dynamic one, click **Criteria** to change the dynamic baseline criteria.

Additionally, if some updates are excluded from or included in the baseline, click **Exclusions**, or **Inclusions** to change the excluded or included updates.

Attaching Baselines

You can attach existing baselines to objects in the VirtualCenter inventory. You can attach baselines to individual objects, but a more efficient approach is to attach baselines to container objects, such as folders, hosts, clusters, and datacenters, instead of attaching them to individual virtual machines and hosts. Attaching a baseline to a container object such as a folder, host, cluster or datacenter transitively attaches the baseline to all objects in the container.

To attach a baseline

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Navigate to the virtual infrastructure object to attach the baseline to, click the **Update Manager** tab, and click the **Attach Baseline** link in the upper-right corner.
- 3 Select one or more baselines to be attached and click **OK**.

Detaching Baselines

You can detach baselines from certain objects in the inventory. These are objects to which the baselines were directly attached in a previous attach operation. VMware Infrastructure objects often have inherited properties, including baseline associations, so to detach a baseline from an object, you might have to navigate to the parent object, to which the baseline is attached, and remove it from there.

To detach a baseline

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Navigate to the virtual infrastructure object to remove the baseline from, and click the **Update Manager** tab.
- 3 Find the baseline to remove, and review where the baseline is attached.

This information is contained in the **Attached At** column.

- 4 Right-click the baseline to remove, and click **Detach Baseline(s)**.

The baseline is detached from the VMware Infrastructure inventory object.

Removing Baselines

You can remove baselines and delete them from VI Client.

To remove a baseline

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click the **Update Manager** button.
- 3 On the **Baselines** tab, select the baselines to remove.
- 4 Click **Remove Baseline**.
- 5 When prompted to confirm deletion of the selected baselines, click **Yes**.

Scanning Virtual Machines and ESX Server Hosts

You can get Update Manager to automatically scan virtual machines and ESX Server hosts by using preestablished tasks or you can manually initiate scans, as required by users. To produce compliance information, you can run scans against objects that have baselines attached to them. When you scan an object, the scan is performed against all updates, but compliance information is produced only for the updates included in a baseline attached to the object. See [“Attaching Baselines”](#) on page 28.

To manually initiate a scan

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** in the navigation bar. For virtual machines, click **Virtual Machines and Templates**. For ESX Server hosts, click **Hosts and Clusters**.
- 3 In the left pane, right-click a container object to be scanned and click **Scan for Updates**.

All child objects of the object on which the scan is initiated are also scanned. The larger the virtual infrastructure and the higher up in the object hierarchy you initiate the scan, the longer the scan takes.

If the ESX Server hosts within a container object are disconnected, they are not scanned. Even if all ESX Server hosts are disconnected, when you right-click the container, the **Scan for Updates** option is available, but actual scanning is never performed.

- 4 When prompted to confirm that you want to scan all the objects and child objects, click **Yes**.

For the results of the scan, see [“Viewing Scan Results”](#) on page 30.

To schedule a scan

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed, and click **Scheduled Tasks**.
- 2 Click **New** in the toolbar to open the Select a Task to Schedule dialog box.
- 3 From the drop-down menu, select **Scan for Updates** and click **OK**.
- 4 Select the type of scan to schedule. Click **Next**.
- 5 Select the objects to be scanned. Click **Next**.

For all objects selected, all child objects are scanned as well.

- 6 Configure when the task will run based on the state of the virtual machine or ESX Server. Click **Next**.
- 7 Review the summary information for the task to be completed and click **Finish**.

Viewing Scan Results

Update Manager provides a means to quickly check how machines comply with baselines. You can review compliance either by examining results for a single virtual machine or ESX Server, or by reviewing the results for a grouping of virtual machines or ESX Server hosts. Compliance information is available on the **Update Manager** tab in the VI Client. For ESX Server hosts, you can view compliance in the Hosts and Clusters view. For virtual machines, you can view compliance in the Virtual Machines and Templates view.

Supported groupings include virtual infrastructure container objects such as folders, clusters and datacenters.

Baselines interact with virtual machines in the following ways:

- If a user does not have permissions to view an object, an object's contents, or a virtual machine, the results of those scans are not displayed.
- Compliance with baselines is assessed at the time of viewing. This means a brief pause might occur while information is gathered about virtual machines' compliance, to ensure that all information is current.
- Only information about compliance with relevant baselines is provided. For example, if a baseline is not attached to the container in question, compliance is not assessed. Similarly, consider the case in which a container has Windows XP and Windows Vista virtual machines, and baselines for Windows XP and Windows Vista patches are attached to this container. In such a case, the Windows Vista virtual machines are assessed for compliance with Windows Vista baselines, and the results are displayed. The same Windows Vista virtual machines are not assessed for compliance with Windows XP patches, and as a result, the status of their compliance is displayed as not applicable.
- Compliance status is displayed based on permissions. Users with permission to view a container but not all of the containers' contents are shown the aggregate compliance of all entities under that container, but the individual counts for compliant, not compliant and unknown entities only appear as the user's permissions permit. To view the compliance status, user also must have permissions to view the baseline or software update compliance status for an object in the inventory.

When you scan an ESX Server host against a fixed baseline containing only updates obsoleted by newer ones, and the newer updates are already installed on the ESX Server host, the compliance status of the old updates is not applicable. If the newer updates are not installed on the ESX Server, the compliance status of the old updates is not compliant. You can install the non-compliant updates after starting a remediation process.

When you scan an ESX Server host against a fixed baseline, containing both obsolete and newer updates, the old updates are displayed as not compliant. Only the newer updates are installed after starting a remediation process.

Reviewing Scan Results for Virtual Machines Contained in a Virtual Infrastructure Object

When scans are completed on all machines contained within a virtual infrastructure object, the results are displayed in a summary. Information that is displayed explains the degree of conformance with baselines, rather than the details. The following information is included:

- When the last scan was completed at this level.
- The total number of compliant and non-compliant updates.
- For each baseline, the number of virtual machines or hosts that are compliant or not compliant.
- For each baseline, the number of patches that are not applicable to particular virtual machines or hosts.

To review scan results for virtual machines or ESX Server hosts

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** in the navigation bar. For virtual machines, click **Virtual Machines and Templates**. For ESX Server hosts, click **Hosts and Clusters**.
- 3 Click the object whose scan results you want to view.
- 4 Click the **Update Manager** tab.

The results for scans completed on virtual machines in that container appear at the right.

You can receive more information about the results of the scans of particular baselines.

To receive more information about baseline compliance of virtual machines in an object

Click the hyperlink indicating how many virtual machines are in a particular state of compliance.

The Baseline Details window appears.

You can receive more information about a specific machine's compliance with the updates contained in a baseline.

To receive more information about baseline compliance of a virtual machine with specific updates

Click the hyperlink indicating the number of updates that are or are not in compliance.

The Virtual Machine Baseline Details window appears.

Reviewing Scan Results for Individual Virtual Machines and ESX Hosts

When scans are completed on specific virtual machines or ESX Server hosts, detailed results are provided. Information that is displayed explains the degree of conformance with baselines, rather than the details of conformance. Some information included is:

- When the last scan was completed at this level.
- The total number of baselines and updates that are compliant or not compliant.

To review scan results for a virtual machines

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory**, and click **Virtual Machines and Templates**.
- 3 Select an individual virtual machine or select a VMware Infrastructure object such as a datacenter to see the status for all virtual machines in that object.
- 4 Click the **Update Manager** tab.

To review scan results for an ESX Server host

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory**, and click **Hosts and Clusters**.
- 3 Select an individual ESX Server host or select a VMware Infrastructure object such as a datacenter to see the status for all hosts in that object.
- 4 Click the **Update Manager** tab.

Remediating ESX Server Hosts and Virtual Machines

You can remediate machines either through user-initiated remediation or through regularly scheduled remediation.

For the ESX Server hosts in a cluster, the remediation process is sequential. When you remediate a cluster of ESX Server hosts and one of the hosts fails to enter maintenance mode, the Update Manager reports an error and the process fails. The remaining ESX Server hosts in the same cluster that did get remediated stay at the updated level. The ones that were to be remediated after this host are not updated.

For multiple clusters under a datacenter, the remediation processes are parallel. If the remediation process fails for one of the clusters within a datacenter, the remaining clusters are still remediated.

Templates are a type of virtual machine, so they can be remediated. VMware recommends taking snapshots of templates before remediation, especially if the templates are sealed. A template that is sealed is stopped before operating system installation is completed, and special registry keys are used so that virtual machines created from this template start in setup mode. When such a virtual machine starts, the user completes the final steps in the setup process, allowing for final customization.

To complete remediation of a sealed template, the template must be started as a virtual machine. For this to happen, the special registry keys that start the virtual machine in setup mode are noted and removed. After a template is started and remediated, the registry keys are restored and the machine is shut down, returning the template to its sealed state.

If errors occur, a template might not be returned to its sealed state. For example, if Update Manager loses its connection with the VirtualCenter Server during remediation, the template cannot be returned to its sealed state. Creating a snapshot before remediation provides for easy recovery from such issues.

After remediation is completed, but the baseline is still not compliant, repeat the remediation.

Guest Shutdown

Machines are rebooted at the end of the remediation process, if a reboot is required. A dialog box tells the users logged in to the remediated machines of the upcoming shutdown.

Users can postpone the shutdown for up to a maximum of 60 minutes. After clicking **OK**, a reboot reminder dialog box appears in the task bar. After the specified time elapses, a final timer before shutdown appears.

Manual Virtual Machine Remediation

You can manually remediate virtual machines on a case-by-case basis.

To manually initiate a remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** and click **Virtual Machines and Templates**.
- 3 Click the **Update Manager** tab.
- 4 Right-click the object to be remediated, and click **Remediate**.

All child objects of the object on which the remediation is initiated are also remediated. The larger the virtual infrastructure and the higher in the object hierarchy you initiate the remediation, the longer the process takes.

- 5 Select the baselines you want to apply, and click **Next**.
- 6 All updates are included by default. To exclude individual updates from the remediation process, deselect their check boxes and click **Next**.
- 7 (Optional) Review the excluded updates and click **Next**.
- 8 In the Schedule page, select the time to initiate the remediation actions based on the state of the virtual machine and click **Next**.

- 9 Specify whether you would like to enable rollback before performing the update. If you enable rollback, a snapshot of the virtual machine is created.
Select the snapshot options, including a name and description for the snapshot, as well as whether to take a snapshot of the virtual machine's memory. Click **Next**.
- 10 Review the summary information for the task to be completed and click **Finish**.

Manual ESX Server Remediation

You can manually remediate ESX Server hosts on a case-by-case basis.

To manually initiate a remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** and click **Hosts and Clusters**.
- 3 Click the **Update Manager** tab.
- 4 Right-click the object to be remediated and click **Remediate**.
All child objects of the object on which the remediation is initiated are also remediated. The larger the virtual infrastructure and the further up in the object hierarchy you initiate the remediation, the longer the process takes.
If the ESX Server hosts within a container object are disconnected, they are not remediated. Even if all ESX Server hosts are disconnected, when you right-click the container, the **Remediate** option is available, but actual remediation is not performed.
- 5 Select the baselines to apply and click **Next**.
- 6 To exclude individual updates from the remediation process, deselect their check boxes and click **Next**.
- 7 (Optional) Review the list of updates to be excluded, and click **Next**.
- 8 Select the host remediation options, including the time to initiate the remediation actions as well as the remediation failure response options, and click **Next**.
- 9 Review the summary information for the task to be completed, and click **Finish**.

Scheduled Virtual Machine Remediation

You can remediate virtual machines at predetermined times by using scheduled tasks.

To schedule virtual machine remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click the **Scheduled Tasks** button.
- 3 Right-click the **Scheduled Tasks** pane and click **New Scheduled Task**.
- 4 Select **Remediate** and click **OK**.
- 5 Select **Virtual Machines / Guest Operating Systems** and click **Next**.
- 6 Select the objects to which this remediation applies, and click **Next**.
All virtual machines under the selected object are remediated as well.
- 7 In the Baselines page, select the baselines to apply, and click **Next**.
- 8 To exclude individual updates from the remediation process, deselect their check boxes in the Updates page and click **Next**.
- 9 (Optional) Review the list of updates that are excluded, and click **Next**.
- 10 In the Schedule page, select the time to initiate the remediation actions based on the state of the virtual machine, and click **Next**.

- 11 Specify whether you would like to enable rollback before performing the update. If you enable rollback, a snapshot of the virtual machine is created.
Select the snapshot options, including a name and description for the snapshot, as well as whether to take a snapshot of the virtual machine's memory, and click **Next**.
- 12 Review the summary information for the task to be completed, and click **Finish**.

Scheduled ESX Server Remediation

You can remediate ESX Server hosts at predetermined times by using scheduled tasks.

To schedule ESX Server remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click the **Scheduled Tasks** button.
- 3 Right-click the **Scheduled Task** pane and click **New Scheduled Task**.
- 4 Select **Remediate**, and click **OK**.
- 5 Select **ESX Servers**, and click **Next**.
- 6 Select the objects to which this remediation are applied, and click **Next**.
All ESX Server hosts under the selected object are remediated as well.
The Baselines page appears.
- 7 Select the baselines to apply, and click **Next**.
- 8 To exclude individual updates from the remediation process, deselect their check boxes and click **Next**.
- 9 (Optional) Review the list of updates to be excluded, and click **Next**.
- 10 Select the host remediation options, including when the remediation takes place as well as how remediation failures is handled, and click **Next**.
- 11 Review the summary information for the task to be completed, and click **Finish**.

Working with Update Manager Events

Update Manager stores data about events. You can review this event data to gather information about the Update Manager operations that are in progress or have finished. For reference information about all events, see "[Events](#)" on page 41.

To review events

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Events** tab.
Information about the recent events appears.

To export events

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Events** tab, and click **Export Events**.

- 3 Provide information about how to export the events, and click **Save**.
 - Provide a name for the file in which to save the events.
 - Select a format in which to save the events. Available formats include Excel Workbook, Web page with or without external CSS, comma-delimited files, or XML.

Review the exported events using a viewer of your choice.

Working with Updates

To manage the available updates, use the **Update Repository** tab. The **Update Repository** tab allows you to see the new updates that are downloaded, what are the baselines, if any, that a given update belongs to.

To review the Update Repository

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Update Repository** tab.

The **Update Repository** tab shows a table of all available updates.

The updates that are displayed in bold are part of the most recent download. They stay bold until another download takes place and new updates are downloaded.

Including Updates in a Baseline

The Baseline(s) column displays the baseline that a given update belongs to. To view the baseline, click the **Show Containing baselines** link. The Include update in baseline(s) window appears.

You can include a selected update in a baseline.

To include an update in a baseline

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click the **Update Manager** button.
- 2 Click the **Update Repository** tab.
- 3 Click the **Show containing baselines** link.
- 4 In the Include update in baseline(s) window, select the baselines in which you want to include this update. Click **OK**.

Filtering the Updates in the Update Repository

You can apply simple and advanced filter of the updates.

To perform a simple search within the updates

Enter search criteria in the text field in the upper-right corner, and press Enter.

To perform an advanced search within the updates

- 1 Click **Advanced** next to the text field.
- 2 In the Updates Filter page enter search criteria:
 - **Text contains** – Enter text to restrict the updates displayed. Text entered in this field is searched for conformity in all text fields of the available updates.
 - **Product** – Select operating systems or products for which this baseline will include patches. You can select multiple products or operating systems, but only updates applicable to the product or operating system of the machine being evaluated are scanned.
 - **Severity** – Select the severity of updates to be included in this update.

- **Language** – Select which language versions of patches to include.
- **Released Date** – Provide **Before** and **After** dates to specify a date range for updates.
- **Update Vendor** – Select one of the listed update vendors.

3 Click **Find**.

Managing Virtual Appliances

A virtual appliance is a software solution that is composed of one or more virtual machines, is packaged as a unit by an appliance vendor, and is deployed, managed, and maintained as a unit.

The Update Manager support for online VMware Virtual Appliances Development Toolkit (VADK) based virtual appliance is an experimental feature. Offline and suspended virtual appliances cannot be scanned and remediated. If a virtual appliance is not VADK compatible, it is treated as a regular virtual machine for guest patching and the same limitations (such as no remediation for Linux virtual machines) still apply.

All virtual appliances are required to have Internet connection for discovery, scan, and remediation operations. If the virtual appliance needs to access Internet through a proxy, the proxy server settings can be configured via the appliance's own Web UI.

Virtual Appliances Discovery

After you import a VADK-based virtual appliance in the VI Client, and power it on for the first time, it is discovered as a virtual appliance.

To view the information about a virtual appliance

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** and click **Virtual Machines and Templates** to view the virtual machines.
- 3 Select a virtual appliance and click the **Update Manager** tab.

You can see virtual-appliance information such as vendor, product, and version.

Scanning Virtual Appliances

You can enable Update Manager to automatically scan virtual appliances using preestablished tasks, or you can manually initiate scans. Best practice is to put the virtual appliances in a separate folder so that they are managed easily and checked for compliance.

To scan a virtual appliance

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** and click **Virtual Machines and Templates** to view the virtual machines.
- 3 In the left pane, right-click a virtual appliance object to be scanned and click **Scan for Updates**.

To schedule a scan

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed and click **Scheduled Tasks**.
- 2 Click **New** in the toolbar to open the Select a Task to Schedule dialog box.
- 3 From the drop-down menu, select **Scan for Updates** and click **OK**.
- 4 Select the type of scan to schedule, and click **Next**.
- 5 Select the virtual appliance to be scanned, and click **Next**.
- 6 Enter the task name as well as the task description, configure when the task will run, and click **Next**.
- 7 Review the summary information for the task to be completed, and click **Finish**.

Viewing the scan results for virtual appliances is the same as the one for virtual machines. For more information, see [“Viewing Scan Results”](#) on page 30.

Remediating Virtual Appliances

Updates for a virtual appliance are downloaded by the virtual appliance itself during the remediation process. Update Manager only controls when and what to download. The download URL is set by the independent software vendor providing the virtual appliance.

To download the updates for virtual appliances, Update Manager uses the following approach:

- 1 Update Manager scans the virtual appliances to return product and vendor information, information about the current version, and the missing updates.
- 2 Update Manager directs the virtual appliances to download the missing updates. Update Manager controls the remediation process like when and how to remediate, but the virtual appliance remediates itself.

After remediation, the virtual appliance can be rebooted if the update package requires that.

Virtual appliances have their own Web UI for self-managed update mode. If the auto install updates option is turned on in a certain virtual appliance, Update Manager only runs reporting mode against it. This means that Update Manager scans the virtual appliance, but skips remediation and the remediation operation fails with an event indicating the reason.

You can either remediate virtual appliances manually, or can schedule a remediation process.

To manually initiate a remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click **Inventory** and click **Virtual Machines and Templates**.
- 3 Click the **Update Manager** tab.
- 4 Right-click the virtual appliance to be remediated, and click **Remediate**.
- 5 Select the baselines you want to apply, and click **Next**.
- 6 All updates are included by default. To exclude individual updates from the remediation process, deselect their check boxes and click **Next**.
- 7 (Optional) Review the excluded updates and click **Next**.
- 8 In the Schedule page, select the time at which to initiate the remediation actions, and click **Next**.
- 9 Specify whether you would like to enable rollback before performing the update. If you enable rollback, a snapshot of the virtual appliance is created.

Select the snapshot options including a name and description for the snapshot, and click **Next**.

- 10 Review the summary information for the task to be initiated, and click **Finish**.

To schedule virtual appliance remediation

- 1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.
- 2 Click the **Scheduled Tasks** button.
- 3 Right-click the **Scheduled Tasks** pane and click **New Scheduled Task**.
- 4 Select **Remediate** and click **OK**.
- 5 Select **Virtual Machines / Guest Operating Systems** and click **Next**.
- 6 Select the virtual appliances to which this remediation will apply, and click **Next**.
- 7 In the Baselines page, select the baselines to apply and click **Next**.

- 8 To exclude individual updates from the remediation process, deselect their check boxes in the Updates page and click **Next**.
- 9 (Optional) Review the list of updates that will be excluded and click **Next**.
- 10 In the Schedule page, select the time to complete the remediation actions, and click **Next**.
- 11 Specify whether you would like to enable rollback before performing the update. If you enable rollback, a snapshot of the virtual appliance will be created.
Select the snapshot options including a name and description for the snapshot. Click **Next**.
- 12 Review the summary information for the task to be completed and click **Finish**.

Operations Reference

You can leave established deployments of Update Manager to automatically run with minimal administrative intervention. If, however, Update Manager requires further optimization, this chapter includes information that might help achieve that goal.

This chapter discusses the following topics:

- “Common Problems and Solutions” on page 39.
- “Events” on page 41.
- “Database Views” on page 44.

Common Problems and Solutions

This section includes information about the more common problematic conditions that might occur with Update Manager.

Gathering Log Files

To gather information about recent events on the Update Manager server for diagnostic purposes, use the **Generate Update Manager log bundle** functionality that the support script `vum-support.wsf` provided.

To generate a Update Manager log bundle

- 1 Log in to the VirtualCenter Server on which Update Manager is installed.
- 2 Choose **Start > All Programs > VMware > Generate Update Manager log bundle**.

Log files are generated as a ZIP package, which is stored on the current user’s desktop.

No Baseline Updates Available

Baselines are based on metadata that Update Manager downloads from the Shavlik and VMware Web sites. Shavlik provides metadata for virtual machines and applications, while VMware provides metadata for ESX Server hosts. A common reason having no updates available for baselines might be that Update Manager cannot contact the Shavlik servers. The connection between Update Manager and the Web site includes several links, the failure of any of which might cause updates in baselines to be unavailable. Some possible causes and solutions include:

- Web server proxy misconfiguration. See “Configuring Update Manager for Use with an Internet Proxy” on page 22.
- Shavlik servers being unavailable. Check the Shavlik Web site (<http://www.shavlik.com>) to determine whether it is available.

- VMware update service being unavailable to provide information about ESX Server updates.
- Poor network connectivity. Check whether other applications that use networking are functioning as expected. Consult your network administrator to best assess whether the network is working as expected.

All Updates in Compliance Reports Are Not Applicable

The results of a scan might be that all baselines are marked as Not Applicable. Such a condition typically indicates an error in scanning. Examine the server logs for Scan Tasks that are marked as Failed, or retry the scan operation. If problems persist, collect logs and contact VMware support for further assistance. To collect logs, see [“To generate a Update Manager log bundle”](#) on page 39.

The results of scans are normally composed of a mix of Installed, Missing, and Not Applicable results. For example, it is normal for a baseline composed of Linux patches to be Not Applicable to a Windows machine. Not Applicable entries are typically only a concern when this is the universal result or when it is the result for patches that you know should be applicable.

All Updates in Compliance Reports Are Unknown

The results of a scan might be listed as Unknown. Such a condition typically indicates an error at the start of the scanning process. This might also indicate that no scan occurred. Scheduling a scan or manually starting a scan might address this issue.

Remediated Updates Continue to Be Not Compliant

For Windows virtual machines, check the registry to make sure that the updates were not installed. Search for the Microsoft Knowledge Base (KB) number that pertains to the update in question. These numbers are in:

- The virtual machine’s registry in: HKLM\Software\Microsoft\Updates\<KB_number>
- The virtual machine’s file system in: C:\Windows\NTUninstall\<KB_number>

Common explanations for this problem include:

- Insufficient disk space for Service Pack installation. Retry remediation after freeing up disk space.
- Conflicts with running applications. Reboot the virtual machine and then retry the remediation operation.

Remediating Virtual Machines with All Update or All Critical Updates Fails

In some instances, remediating virtual machines with the All Updates or All Critical Updates default baselines fails. This typically occurs in one of the following ways:

- **Remediation fails to complete** – Remediation might stop on a particular virtual machine. In rare cases, this results from patch application displaying a message box after it is partially completed. Patches are applied by the Update Manager Guest Agent, which runs in the Local System context. Running the Guest Agent in this context prevents users from interfering with the patch application process, but in this case, error messages are never displayed in a form where they can be acknowledged and dismissed. Consequently, the patch application process cannot be completed.

To resolve the issue, end the patch process from the Task Manager in the guest. To identify the patch that created the problem, inspect the events for that virtual machine in the VI client. Update Manager posts events to identify the start and completion of a patch installation, along with the error code, if applicable. If the most recent events indicate the start of a patch installation, but not its completion, use the name of the update to identify the patch process. Microsoft patches are easier to identify because they typically contain the KB number in their filenames.

- **Remediation fails for some patches** – Patches might not be readily available. For example, testing indicates that versions of Windows localized for languages other than English or patches for 64-bit applications might be unavailable. Review the **Tasks** and **Events** tabs to determine if patches that were not applied were not downloaded.
- **Remediation is completed, but the baseline is still not compliant** – This condition might occur when applying patches that subsequently make other patches applicable. For example, a patch might be applicable only after a service pack is applied, so applying that service pack might address all known issues from when the remediation started, but the act of applying the service pack made other patches applicable.

In such a case, repeat the remediation.

ESX Server Scanning Fails

ESX Server scanning typically fails as a result of insufficient permissions or problems with SSL configuration. Check to make sure that the account being used to do the scanning has sufficient permissions and that your SSL connections are properly configured. For more information about Update Manager network port settings and how to configure them, see [“Update Manager Network Port Requirements”](#) on page 19 and [“Configuring the Update Manager Network Port Settings”](#) on page 22.

Events

Update Manager produces events that help you monitor the processes that the system is completing.

Table 3-1. Update Manager Events

Type	Message Text	Action
Info	Successfully downloaded guest update metadata. New updates: <number_of_updates>.	
Error	Failed to download guest update metadata.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded guest update metadata for UNIX. New updates: <number_of_updates>.	
Error	Failed to download guest update metadata for UNIX.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded host update metadata. New updates: <number_of_updates>.	
Error	Failed to download host update metadata.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded guest update packages. New packages: <number_of_packages>.	
Error	Failed to download guest update packages.	Check your network connections to make sure that your update source is reachable.
Info	Successfully downloaded guest update packages for UNIX. New packages: <number_of_packages>.	
Error	Failed to download guest update packages for UNIX.	Check your network connections to make sure that your update source is reachable.
Info	Successfully downloaded host update packages. New packages: <number_of_packages>.	
Error	Failed to download host update packages.	Check your network connections to make sure that your update source is reachable.

Table 3-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Successfully scanned <virtual_machine_or_ESX_Server_host_name> for updates.	
Error	Scanning <virtual_machine_or_ESX_Server_host_name> has been cancelled by a user.	
Error	Failed to scan <virtual_machine_or_ESX_Server_host_name> for updates.	
Warning	Warning during scanning <virtual_machine_or_ESX_Server_host_name>, found missing update: <update_name>. Re-downloading updates might resolve this problem.	
Error	Failed to scan <virtual_machine_name> for updates because of an invalid state: <virtual_machine_state>.	Check the state of the virtual machine. Reboot the virtual machine to facilitate scanning.
Error	Failed to scan <ESX_Server_host_name> for updates because of an invalid state: <ESX_Server_host_state>	Check the state of the ESX Server. Reboot the host to facilitate scanning.
Info	Remediation succeeded for <virtual_machine_or_ESX_Server_host_name>.	
Error	Remediation failed for <virtual_machine_or_ESX_Server_host_name> with <error_message>.	Check the target's state. Restart the target to facilitate remediation.
Error	Failed to remediate <virtual_machine_name> for updates because of an invalid state: <virtual_machine_state>.	Check the virtual machine's state. Restart the virtual machine to facilitate remediation.
Error	Failed to remediate <ESX_Server_host_name> for updates because of an invalid state: <ESX_Server_host_state>.	Check the state of the ESX Server. Restart the host to facilitate remediation.
Error	Failed to scan or remediate <virtual_machine_name> because of unsupported or unknown OS: <operating_system_name>.	
Error	Can't remediate <virtual_machine_name>: Remediation of Linux virtual machines is not supported.	
Info	VMware Update Manager download alert (critical/total): ESX <code>data.esxCritical/data.esxTotal</code> ; Windows <code>data.windowsCritical/data.windowsTotal</code> ; Linux <code>data.linuxCritical/data.linuxTotal</code> .	Provides information about the number of updates downloaded.
Error	Failed to scan <virtual_machine_name> for updates because host <ESX_Server_host_name> is of unsupported version <ESX_Server_host_version>.	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Failed to remediate <virtual_machine_name> for updates because host <ESX_Server_host_name> is of unsupported version <ESX_Server_host_version>.	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Failed to scan <ESX_Server_host_name> for updates because it is of unsupported version <ESX_Server_host_version>.	Hosts with ESX Server versions later than ESX Server 3.5 and ESX Server 3i can be scanned. For the latest information on which virtual machines can be scanned, see the release notes.
Error	Failed to remediate <ESX_Server_host_name> for updates because it is of unsupported version <ESX_Server_host_version>.	Hosts with ESX Server versions later than ESX Server 3.5 and ESX Server 3i can be scanned. For the latest information on which virtual machines can be scanned, see the release notes.
Info	VMware Update Manager Guest Agent successfully installed on <virtual_machine_name>.	

Table 3-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Failed to install VMware Update Manager Guest Agent on <virtual_machine_name>.	Update Manager Guest Agent is required for remediating virtual machines. For more information on installing Update Manager Guest Agent, see "Installing the Guest Agent" on page 16.
Error	Failed to install VMware Update Manager Guest Agent on <virtual_machine_name> because VMware Tools is not installed or is of an incompatible VMware Tools version. The required version is <required_version_number> and the installed version is <installed_version_number>.	
Error	There is no VMware Update Manager license for <virtual_machine_or_ESX_Server_host_name> for the required operation.	Obtain the required licenses to complete the desired task.
Warning	VMware Update Manager is running out of storage space. Location: <path_location>. Available space: <free_space>.	Add more storage.
Warning	VMware Update Manager is critically low on storage space! Location: <path_location>. Available space: <free_space>.	Add more storage.
Error	VMware Update Manager Guest Agent failed to respond in time on <virtual_machine_name>. Please check if the virtual machine is powered on and Guest Agent is running.	
Error	An internal error occurred in communication with Update Manager Guest Agent on <virtual_machine_name>. Please check if the virtual machine is powered on and retry the operation.	
Error	VMware Update Manager Guest Agent failed to access DVD drive on <virtual_machine_name>. Please check if a DVD drive is available and retry the operation.	
Error	An unknown internal error occurred during the required operation on <virtual_machine_name>. Please check the logs for more details and retry the operation.	
Error	Failed to install update <update_name> on <virtual_infrastructure_entity_name>.	
Info	Install of update <update_name> on <virtual_infrastructure_entity_name> <message>.	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Failed to scan orphaned virtual machine <virtual_machine_name>.	
Info	Failed to remediate orphaned virtual machine <virtual_machine_name>.	
Error	Failure in downloading patches for following updates: <message>.	Check your network connections to make sure that your patch source is reachable.
Warning	<virtual_machine_name> contains an unsupported volume <volume_label>. Scan results for this virtual machine may be incomplete.	
Info	Initiating the task cancellation on <virtual_machine_or_ESX_Server_host_name>	
Warning	There are running tasks for the entity <virtual_infrastructure_entity_name> that cannot finish within a specific time. The operation will be aborted.	

Table 3-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Action is not supported for offline or suspended virtual appliance <virtual_appliance_name>.	A scan or remediation process is not supported for offline virtual appliance.
Info	Successfully discovered virtual appliance <virtual_appliance_name>.	
Info	Failed to discover virtual appliance <virtual_appliance_name>.	An error occurred during the discovery of the virtual appliance.
Error	Auto update is set to ON for virtual appliance <virtual_appliance_name>.	If auto-update is set to ON in virtual appliance, Update Manager cannot perform remediation.
Error	Repository address not set for virtual appliance <virtual_appliance_name>, it doesn't support updates by VirtualCenter.	
Info	Open <virtual_machine_or_ESX_Server_host_name> firewall ports.	
Info	Close <virtual_machine_or_ESX_Server_host_name> firewall ports.	
Info	Patch metadata for <virtual_machine_or_ESX_Server_host_name> missing. Please download updates metadata first.	
Info	Patch metadata for <virtual_machine_or_ESX_Server_host_name> corrupted. Please check the logs for more details. Re-downloading update metadata may resolve this problem.	

Database Views

Update Manager uses SQL Server and Oracle databases to store information. The database views for Microsoft SQL Server and Oracle databases are the same. Due to limitations in the length of the names for Oracle database, some of the database views in Oracle are with shorter names.

VUMV_VERSION

Update Manager version information.

Table 3-2. VUMV_VERSION

Field	Notes
VERSION	The Update Manager version in x.y.z format, for example 1.0.0
DATABASE_SCHEMA_VERSION	The Update Manager database schema version (an increasing integer value), for example 1

VUMV_UPDATES

Software update metadata.

Table 3-3. VUMV_UPDATES

Field	Notes
UPDATE_ID	Software update unique ID generated by the Update Manager
TYPE	The entity type: a virtual machine or ESX Server host
TITLE	Title

Table 3-3. VUMV_UPDATES (Continued)

Field	Notes
DESCRIPTION	Description
META_UID	A unique ID provided by the vendor for this update (for example, MS12444 for Microsoft updates)
SEVERITY	Update severity information. The values of this field are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity.
RELEASE_DATE	The date on which this update was released by the vendor
DOWNLOAD_TIME	The date and time this update was downloaded by the Update Manager server into the Update Manager database
SPECIAL_ATTRIBUTE	Any special attribute associated with this update (for example, all Microsoft Service packs will be marked as Service Pack)

VUMV_PATCHES

Patch binary metadata.

Table 3-4. VUMV_PATCHES

Field	Notes
PATCH_ID	Unique ID for the current patch, generated by the Update Manager server
TYPE	The entity type: a virtual machine or an ESX Server host
NAME	Name of the patch
DOWNLOAD_TIME	A URL for the patch binary
PATCH_SIZE	Size of the patch in KB

VUMV_BASELINES

The Update Manager baseline details.

Table 3-5. VUMV_BASELINES

Field	Notes
UPDATE_ID	Unique ID generated for this baseline by the Update Manager server
NAME	Name of the baseline
TYPE	The baseline type: Fixed or Dynamic
TARGET_TYPE	Type of targets that this baseline applies to: a virtual machine or an ESX Server host

VUMV_PRODUCTS

Product metadata, including operating systems and applications.

Table 3-6. VUMV_PRODUCTS

Field	Notes
PRODUCT_ID	Unique ID for the product generated by the Update Manager server
NAME	Name of the product

Table 3-6. VUMV_PRODUCTS

Field	Notes
VERSION	Product version
FAMILY	Windows, Linux, ESX Server host, or Embedded ESX Server host

VUMV_BASELINE_UPDATE_ASSIGNMENT

The software updates that are part of a certain baseline.

For Oracle, the name of this database view is VUMV_BASELINE_UPDATE, due to restrictions in the name length.

Table 3-7. VUMV_BASELINE_UPDATE_ASSIGNMENT

Field	Notes
BASELINE_ID	Baseline ID (foreign key, VUMV_BASELINES)
UPDATE_ID	Software update ID (foreign key, VUMV_UPDATES)

VUMV_BASELINE_ENTITY_ASSIGNMENT

Objects that a certain baseline is attached to.

For Oracle, the name of this database view is VUMV_BASELINE_ENTITY.

Table 3-8. VUMV_BASELINE_ENTITY_ASSIGNMENT

Field	Notes
BASELINE_ID	Baseline ID (foreign key, VUMV_BASELINES)
ENTITY_UID	Update ID of the entity (the managed object ID generated by the VirtualCenter Server)

VUMV_UPDATE_PATCHES

Patch binaries that correspond to a software update.

Table 3-9. VUMV_UPDATE_PATCHES

Field	Notes
UPDATE_ID	Software update ID (foreign key, VUMV_UPDATES)
PATCH_ID	Patch ID (foreign key, VUMV_PATCHES)

VUMV_UPDATE_PRODUCT

Products (operating systems and applications) that this software update applies to.

Table 3-10. VUMV_UPDATE_PRODUCT

Field	Notes
UPDATE_ID	Software update ID (foreign key, VUMV_UPDATES)
PRODUCT_ID	Product ID (foreign key, VUMV_PRODUCTS)

VUMV_ENTITY_SCAN_HISTORY

History of the scan operations

Table 3-11. VUMV_ENTITY_SCAN_HISTORY

Field	Notes
SCAN_ID	Unique ID generated by the Update Manager server
ENTITY_UID	Unique ID of the entity the scan was initiated on
START_TIME	Start time of the scan operation
END_TIME	End time of the scan operation
SCAN_STATUS	Result of the scan operation (for example Success, Failure, or Cancelled)
FAILURE_REASON	An error message describing the failure reason

VUMV_ENTITY_UPDATE_SCAN_HISTORY

History of the status of a given entity for an update.

For Oracle, the name of this database view is VUMV_ENTITY_UPDATE_SCAN_HIST.

Table 3-12. VUMV_ENTITY_UPDATE_SCAN_HISTORY

Field	Notes
SCAN_ID	Unique ID (foreign key VUMV_SCAN_HISTORY)
UPDATE_ID	Unique ID (foreign key VUMV_UPDATES)
ENTITY_UID	Unique ID of the entity the scan was initiated on
ENTITY_STATUS	Status of this entity for this update (for example, Missing Installed, Unknown or Not Applicable)

VUMV_ENTITY_REMEDIATION_HISTORY

History of remediation operations.

For Oracle, the name of this database view is VUMV_ENTITY_REMEDIATION_HIST.

Table 3-13. VUMV_ENTITY_REMEDIATION_HISTORY

Field	Notes
REMEDIAION_ID	Unique ID, generated by the Update Manager server
ENTITY_UID	Unique ID of the entity that the remediation was initiated on
START_TIME	Start time of the remediation
END_TIME	End time of the remediation
REMEDIAION_STATUS	Result of the remediation operation (for example, Success, Failure, or Cancelled)
IS_SNAPSHOT_TAKEN	Indicates whether snapshot is created prior to the remediation

VUMV_UPDATE_PRODUCT_DETAILS

A convenient view of the products (operating systems and applications) that a certain software update applies to.

Table 3-14. VUMV_UPDATE_PRODUCT_DETAILS

Field	Notes
UPDATE_METAUID	Software Update ID (foreign key, VUMV_UPDATES)
UPDATE_TITLE	Update Title
UPDATE_SEVERITY	Update impact information. The values of this field are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity.
PRODUCT_NAME	Product name
PRODUCT_VERSION	Product version

VUMV_BASELINE_UPDATE_ASSIGNMENT_DETAILS

A convenient view of the software updates that are part of a baseline.

For Oracle, the name of this database view is VUMV_BASELINE_UPDATE_DET.

Table 3-15. VUMV_BASELINE_UPDATE_ASSIGNMENT_DETAILS

Field	Notes
BASELINE_NAME	Baseline name
BASELINE_TYPE	Baseline type: Fixed or Dynamic
BASELINE_TARGET_TYPE	Baseline target type, for example, a virtual machine or an ESX Server host
UPDATE_METAUID	Update meta ID
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update severity. The values of this field are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity.

VUMV_ENTITY_UPDATE_SCAN_HISTORY_DETAILS

A convenient view of the status history of a given entity for an update.

The name of this database view for Oracle is VUMV_ENTITY_UPD_SCANHIST_DET.

Table 3-16. VUMV_ENTITY_UPDATE_SCAN_HISTORY_DETAILS

Field	Notes
ENTITY_UID	Entity unique ID (a managed object ID assigned by the VirtualCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
UPDATE_METAUID	Update meta unique ID
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update severity. The values of this field are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity.
ENTITY_STATUS	Status of the entity with regard to the update. This field has values Missing, Installed, Unknown, and Not Applicable.

Index

A

attaching baselines **28**

B

baselines

- attaching **28**
- creating **26**
- detaching **28**
- editing **28**
- none available **39**
- overview **9–10, 25**
- removing **29**

C

client, installing **17**
compliance, unknown **40**
configuration options, overview **10**
configuring

- network port settings **22**
- Oracle database **13–14**
- proxy settings **22**
- SQL database **14–16**
- Update Manager **20**
- Update Manager Download Service **24**

creating baselines **26**

D

Database views **44–48**
detaching baselines **28**
downloading

- patches **8**
- updates **8**

E

editing baselines **28**
ESX Server host

- remediation failure **20**
- scan results, reviewing **31**
- scanning **29**
- scanning failure **40, 41**

events

- exporting **34**
- list of **41**
- reviewing **34**
- tasks **34**

exporting events **34**

G

generating

- log bundles **39**
- log files **39**

Guest Agent, installing **16**

I

installing

- client **17**
- Guest Agent **16**
- Update Manager **11–13**
- Update Manager Download Service **16**

L

log bundles, generating **39**
log files, generating **39**

M

modifying baselines **28**

N

network port settings

- configuring **22**
- overview **19**

O

overview of

- baselines **9–10, 25**
- configuration options **10**
- network port settings **19**
- remediation **10, 32**
- scanning **9**
- VMware Update Manager **8**

P

patches, downloading **8**
proxy settings, configuring **22**

R

remediation

- manual **32, 33**
- overview **10, 32**
- scheduling **33**
- virtual appliances **37**

removing

- baselines **29**
- Update Manager **18**

reviewing

- ESX Server host scan results **31**
- scan results **30**
- updates **35**
- virtual machine scans **31**

virtual machine

- remediation failure **20**
- reviewing scans **31**
- scanning **29**
- shutdown warning **32**

S

scanning

- ESX Server host **29**
- manual **29**
- overview **9**
- results, reviewing **30**
- scheduled **29**
- virtual appliances **36**
- virtual machine **29**

scheduling

- remediation **33**
- scanning **29**

shutdown warning **32**

T

troubleshooting

- baselines **39**
- compliance **40**
- ESX Server host applicable **40**
- ESX Server host scanning failure **41**
- generating log bundles **39**
- scanning **40**
- virtual machines non-compliant **40**

U

uninstalling Update Manager **18**

Update Manager

- configuring **20**
- installing **11–13**
- network port requirements **19**
- uninstalling **18**
- VI Client support **17**

Update Manager Download Service

- configuring **24**
- installing **16**

updates

- downloading **8**
- filtering **35**
- include in a baseline **35**
- reviewing **35**

V

virtual appliances

- discovery **36**
- remediation **37**
- scanning **36**

Updates for the Update Manager Administration Guide

Last Updated: July 01, 2009

This document provides updates to the Update 2 Release for Update Manager 1.0 version of the *Update Manager Administration Guide*. Updated descriptions, procedures, and graphics are organized by page number so that you can easily locate the areas of the guide that have changes. If the change spans multiple sequential pages, this document provides the starting page number only.

The following is a list of updates to the *Update Manager Administration Guide*:

- [Updates for the Table of Supported Database Formats on Page 12](#)
- [Updates for the To use the Update Manager Download Service procedure on Page 24](#)

Updates for the Table of Supported Database Formats on [Page 12](#)

[Table 2-1](#) does not mention support for versions later than 10.2.0.3.0 of Oracle 10g Enterprise Release 2. The row should appear as follows:

Oracle Database 10g Release 2 (10.2.0.1.0)	After applying patch 10.2.0.3.0 to the client and server, apply patch 5699495 to the client. Also apply patches 6085625 and 6452485 to the server. Note: VMware supports 10.2.0.3.0 and later versions of Oracle Database 10g Release 2.
--	--

Updates for the To use the Update Manager Download Service procedure on [Page 24](#)

In the [To use the Update Manager Download Service](#) procedure the commands included with the steps are incorrect. The correct procedure is the following:

To use the Update Manager Download Service

- 1 Log in to the machine on which Update Manager Download Service is installed.
- 2 Click **Start > Run**, type **cmd**, and press Enter.
- 3 Change to the directory where Download Service is installed.

The default folder is C:\Program Files\VMware\Infrastructure\Update Manager.

- 4 Set up what updates to download:
 - To setup a download of all ESX Server host updates, run the following command:
`vmware-umds --set-config --enable-host 1 --enable-win 0 --enable-lin 0`
 - To setup a download of all Windows updates, run the following command:
`vmware-umds --set-config --enable-host 0 --enable-win 1 --enable-lin 0`
 - To setup a download of all Linux updates, run the following command:
`vmware-umds --set-config --enable-host 0 --enable-win 0 --enable-lin 1`
 - To setup a download of all available updates, run the following command:
`vmware-umds --set-config --enable-host 1 --enable-win 1 --enable-lin 1`

- 5 Run the program to download updates by running the following command:

```
vmware-umds --download
```

If you have already downloaded updates and want to download some of them again, include start and end time, to restrict the updates to download. For example, if you want to download the updates released in May, 2008, enter the following command:

```
vmware-umds --re-download --start-time 2008-05-01T00:00:00 --end-time 2008-05-31T23:59:59
```

- 6 Repeat [Step 1](#) – [Step 3](#).

- 7 Export the downloaded updates by running the following command:

```
vmware-umds --export --dest <repository_path>
```

If you want to export all updates for the year 2007, enter the following command:

```
vmware-umds --export --dest <repository_path> --start-time 2007-01-01T00:00:00 --end-time 2007-12-31T23:59:59
```

Here, `<repository_path>` is the full path to your export directory.

If your deployment is a semi air gap deployment, `<repository_path>` points to the shared folder on the remote server. If the shared folder is on the machine on which Update Manager 1.0 server is installed, continue with [Step 10](#).

- 8 After exporting the downloads to a folder, move them to a portable media drive.

- 9 Connect the portable drive to the machine on which the Update Manager 1.0 is installed.

- 10 In the command prompt, change to the directory where Update Manager 1.0 is installed.

The default folder is `C:\Program Files\VMware\Infrastructure\Update Manager`.

- 11 To import Windows and ESX Server host updates, run the following command:

```
vmware-updateDownloadCli.exe --update-path <local_path> --config-import windows esx --vc <IP_address:port> --vc-user <vc_user>
```

Here, `<local_path>` is the path to the folder or drive where the software updates are exported, `<IP_address:port>` are the VirtualCenter Server IP and port (if the Update Manager 1.0 and VirtualCenter Server are installed on different machines), and `<vc_user>` is your VirtualCenter user name.

NOTE You can also use the Windows Scheduled Task wizard to schedule Download Service to run at regular intervals.
