Administration Guide

Update Manager

Administration Guide
Revision: 20090709

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

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

Contents

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.

Update Manager Administrative Guide works with VMware ESX Server 3.5 and VMware ESX Server 3i version 3.5. 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 VI Client plug-in, and release notes.

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 1

This chapter discusses the following topics:

Update Manager Overview

Update Manager compares the operating systems and applications running in your Virtual Infrastructure deployment against a set of standard updates and patches. Updates you specify can be applied to operating systems and applications on scanned ESX Server hosts and virtual machines. Update Manager works with ESX Server hosts and virtual machines 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 and hosts.

Update Manager is scalable to existing Virtual Infrastructure deployment sizing standards.

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 application of the patches that you require to the systems in your environment.

To make your environment more secure, it is important to:

- 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 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 and ESX 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 other applications and operating systems. Shavlik supplies information about a range of operating system and application vendors such as Microsoft, Adobe, and Mozilla.

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 15. 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 and "Remediation" on page 10.

The information about the patches is used while scanning machines. When Update Manager examines systems for patch compliance, it checks to determine whether the latest patch is applied based on information on that system. Patch information is required for this process, but the patch itself is not. 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 patches are applied, such as whether it is applied immediately or at a later time, is 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 hosts being powered off), the process is deferred until the action is possible. After a patch is downloaded, it is kept indefinitely. When other machines are remediated, the patch resource is present on the server.

You can configure Update Manager to use an Internet proxy to download patch information and patches. See "Configuring Update Manager to Use with an Internet Proxy" on page 15. 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 for Update Manager servers to use later.

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, and Windows and Linux virtual machines. For example, you can scan an ESX Server 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 are performed only for updates that apply to the operating system in question. For example, Update Manager scans Windows virtual machines to ensure that they have a particular set of patches but does not scan that same machines to determine whether Linux patches are installed.

You can initiate scans on objects in the virtual infrastructure including:

- Single virtual machines
- Folders
- Clusters
- Datacenters
- Templates
- Hosts

Resource pools are the only VMware Infrastructure object type that you can never scan.

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. Checking a single baseline makes it possible with one step to determine whether all the individual updates that make up the baseline were applied to the objects being scanned.

At regular intervals, Update Manager queries update repositories that our vendors provide to find which patches are available. 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 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 hosts for compliance with all critical updates.
  - **Non-critical Host Updates** – Checks ESX 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 is established when a baseline is created and can be modified, as required.
- **Updates** – Specifies the number of updates included in this baseline. Some updates, such as service packs, include many smaller patches, which 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 is more qualitatively suggestive, rather than quantitatively specific. 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 modified to include or exclude specific updates, counter to the basic criteria of the dynamic baseline.

Administrators can create new baselines, edit baselines, detach baselines, or remove 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 or virtual machines. After a scan is complete, you can remediate machines so that they comply with the standards of your organization. Remediation helps ensure that machines 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 in much the same ways that you can scan them. As with scanning, you can remediate a single virtual machine, 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.
- Templates for Windows virtual machines.
- ESX Server hosts beginning with version 3.5.0.

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, and if so, whether to store the snapshot, and if so, for how long.
- How failures to remediate ESX Server hosts are handled.

For more information on security configuration, see “Configuring Update Manager” on page 15.

Working with Update Manager 2

Use 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

(SEE UPDATE) 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 on the same computer as VirtualCenter Server or on a different computer. Update Manager can be installed on computers running the following operating systems:

- Windows XP SP2 or later
- Windows Server 2003

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

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 (SEE UPDATE)

Database Type	Patch and Driver Requirements
SQL Server 2000	Use SQL Server driver for the client.
SQL Server 2005	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 (10.1.0.3.0)	None
Oracle 10g Release 2 (10.2.0.1.0)	First apply patch 10.2.0.3.0 to client and then patch 5699495.

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 port is used. The default for the web service port is 443.
- 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 server that will host the Update Manager server.

2 Click **Next**.

3 Click **Next**.

4 Select the appropriate option and click **Next**.

5 Enter your name and organizational information and click **Next**.

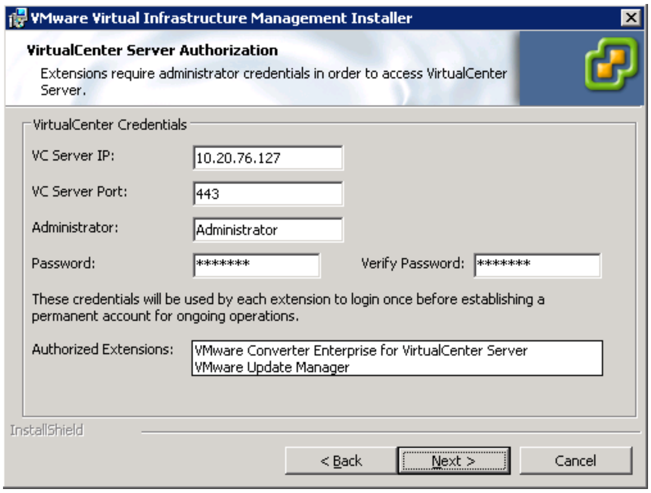
6 Select **VMware VirtualCenter Server**.

If you have already installed components such as VMware Infrastructure Client, VMware VirtualCenter Server, or VMware Converter Enterprise for VirtualCenter, a message appears informing you that these components are installed and allowing you to 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 VMware Update Manager is installed and where patches are stored.

7 Click **Next**.

The VirtualCenter Server Authorization page appears.



VMware Virtual Infrastructure Management Installer

VirtualCenter Server Authorization

Extensions require administrator credentials in order to access VirtualCenter Server.

VirtualCenter Credentials

VC Server IP: 10.20.76.127

VC Server Port: 443

Administrator: Administrator

Password: ******* Verify Password: *******

These credentials will be used by each extension to login once before establishing a permanent account for ongoing operations.

Authorized Extensions: VMware Converter Enterprise for VirtualCenter Server
VMware Update Manager

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 the IP address you collected or accept the default.

b In the VC Server Port text box, enter the Port you collected 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.

Installing the Guest Agent

Update Manager Guest Agent facilitates Update Manager processes. The Guest Agent is installed at different times depending on the operating system the virtual machine is running. For Linux, the Guest Agent is installed when a powered-on virtual machine is added to the Virtual Infrastructure inventory. For Windows, 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, for some reason, 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 location you specified when installing Update Manager server. In that directory, Guest Agent installation packages are at `\docroot\vci\guestAgent\`. For example, if Update Manager was installed in `C:\Program Files\VMware\Infrastructure\Update Manager`, the Guest Agent installers are at
`C:\Program Files\VMware\Infrastructure\Update Manager\docroot\vci\guestAgent\`.

The Guest Agent requires no user input, so that the installation completes silently. In Windows, start the installer by running the `VMware-UMGuestAgent.exe` file. In Linux, install the `VMware-VCIGuestAgent-Linux.rpm` file by issuing 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 reasons such as security, deployments install VMware Infrastructure, including Update Manager, on a network that is disconnected from the Internet. In such a case, for Update Manager to continue to function properly, it needs access to patch information. The Download Service provides a solution in such situations. Download Service downloads updates for:

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

After the Download Service downloads updates, they can then be exported to a 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 will be patching and the number of years you will be gathering patches on this system. Expect to need 50 gigabytes (GB) for each year of ESX Server patching and 11GB 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 100GB for the hosts and 22GB for the virtual machines for a total of 122GB. Therefore, to install in such an environment, install it to a server with at least 122GB of available space for patch storage. (SEE UPDATE)

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 database or an existing Oracle database.

To install the Update Manager Download Service

Open the `VMware-UMDS.exe` file which is in the `umds` folder on the installation CD. Use the wizard to complete the installation.

Upgrading VirtualCenter Clients to Support Update Manager

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

After installing Update Manager, update at least one client so you can configure Update Manager. You do not need to update all clients. Any mixture of Update Manager enabled-VI Clients and clients with some or no other plug-ins can connect to a given VirtualCenter server without conflict.

To enable Update Manager on VI Clients

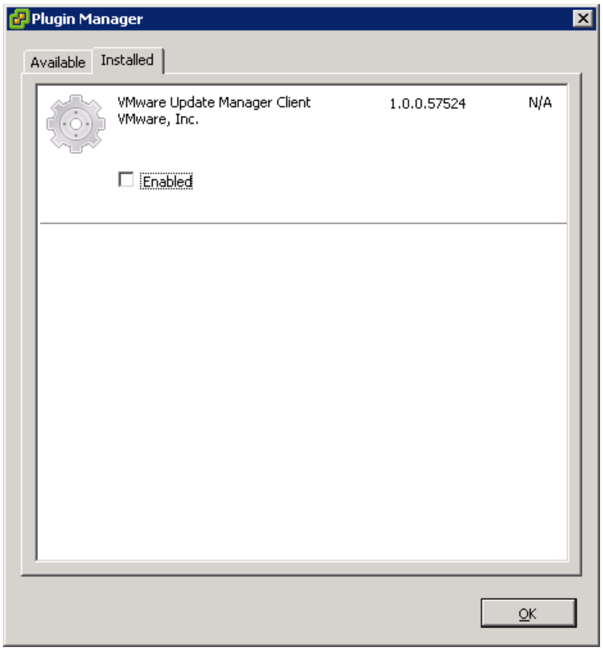
1 Connect the VI Client to a VirtualCenter Server on which VMware Update Manager is installed.

2 Choose **Plugins** > **Manage Plugins**.

3 Click **Download and install** for the Update Manager plug-in.

4 Complete the Update Manager Client installation wizard and click **OK**.

5 Click the **Installed** tab on the Plugin Manager page.



VMware Update Manager Client 1.0.0.57524 N/A
VMware, Inc.

□ Enabled

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

6 Click **Enabled**.

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

8 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.

Uninstalling Update Manager

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 a 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, you might want to leave an existing installation in place for later use.

Configuring Update Manager

You can modify the administrative settings for Update Manager before beginning to use this plug-in. The administrative settings determine:

- How often Update Manager checks for new updates.
- What action Update Manager takes if a remediation fails for either a guest virtual machine or an ESX Server.

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 quickly, 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 **Update Manager**.
2. Choose **Plugins** > **Update Manager** > **Schedule Update Download**.
3. Select the type of downloads to be updated and click **Next**.
4. Specify when updates will be downloaded and click **Next**.
5. You can specify addresses to receive email about the results of the update download process.
6. Click **Next**.
7. Click **Finish**.

Configuring Update Manager to 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.

After providing the proxy information, you might need to provide authentication information.

To update proxy authentication information

1. Log in to the VMware Update Manager server as an administrator.
2. Stop the VMware 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, select **VMware Update Manager**, click **Action**, and click **Stop**.
3. Open the vum-`proxyAuthCfg.exe` file in the Update Manager directory.
4. Provide updated proxy authentication information.
5. Restart the Update Manager service.

Alternatively, you can modify the XML file that stores information about the proxy server.

To manually modify proxy configuration (SEE UPDATE)

1. Find the `vci-integrity.xml` file in the Update Manager installation directory.
2. Create a backup copy of this file in case you need to revert to the previous configuration.
3. Edit the file by changing the following fields:

   ```
   <proxyServer>yournewproxy.companydomain.com</proxyServer>
   ```

   ```
   <proxyPort>3128</proxyPort>
   ```

Using Update Manager Download Service

If you elected to use the Update Manager Download Service, initiate downloads and exports. Establish a depot on which to place the updates. After updates are on the depot, export the newly downloaded updates to some portable storage device like 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 Download Service as the only means to download and transfer updates to Update Manager.

To use the Update Manager Download Service

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.
4. Enter commands to start a Download Service process. For example:
   - To download updates: `vmware-umds --download`
   - To export updates for the year 2007 to `e:\export-depot:`

     ```
     vmware-umds -E --dest e:\export-depot -s 2007-01-01T00:00:00 -t
     2007-12-31T23:59:59
     ```
5. After exporting downloads to a folder, physically move them to the Update Manager machine.
6. Import the updates to Update Manager using the `vmware-updateDownloadCli.exe` utility in the Update Manager installation folder. For example, to import Windows and ESX host updates from the D: drive, use the following command:

   ```
   vmware-updateDownloadCli.exe --update-path d:\ --config-import windows esx --vc-user
   administrator
   ```

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

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 reestablished. 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 additional 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 "To configure guest snapshot behavior," 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**.

2 Click **Plugins** > **Update Manager** > **Settings**, and click the **Guest Settings** entry in the left pane.

3 Select **Snapshot the virtual machines before applying updates to enable rollback**.

4 Configure snapshots to be kept indefinitely or for a period and click **OK**.

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, Update Manager migrates virtual machines to other ESX Server hosts before the server being remediated is put in maintenance mode. If virtual machines cannot be migrated to an alternative host, Update Manager can take one of the following actions:

- **Fail Task** – Log this failure in the VirtualCenter logs and take no further action.
- **Retry** – Wait for the Retry delay period and repeat the attempt to put the server into maintenance mode.
- **Power off/Shut down virtual machines and retry** – Power off or shut down all of the running virtual machines following the failure and try entering maintenance mode. Virtual machines are shut down as though their power-off button is used, which has different results depending on configuration.
- **Suspend virtual machines and retry** – Suspend all the running virtual machines following the VM Settings specified by the VirtualCenter Server user interface suspend button, and try entering maintenance mode.

The configuration described in "To configure how Update Manager responds to failures to enter maintenance mode," determines the default settings for remediation failures. You can specify alternative settings to these defaults when you configure individual remediation tasks.

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**.

2 Choose **Plugins** > **Update Manager** > **Settings** and click **ESX Host Settings** in the left pane.

3 Select a choice from **Failure Response** to determine how Update Manager responds if an ESX Server cannot be put in maintenance mode.

4 Configure the options to correspond to the Failure Response option you select and click **OK**.

Working with Baselines

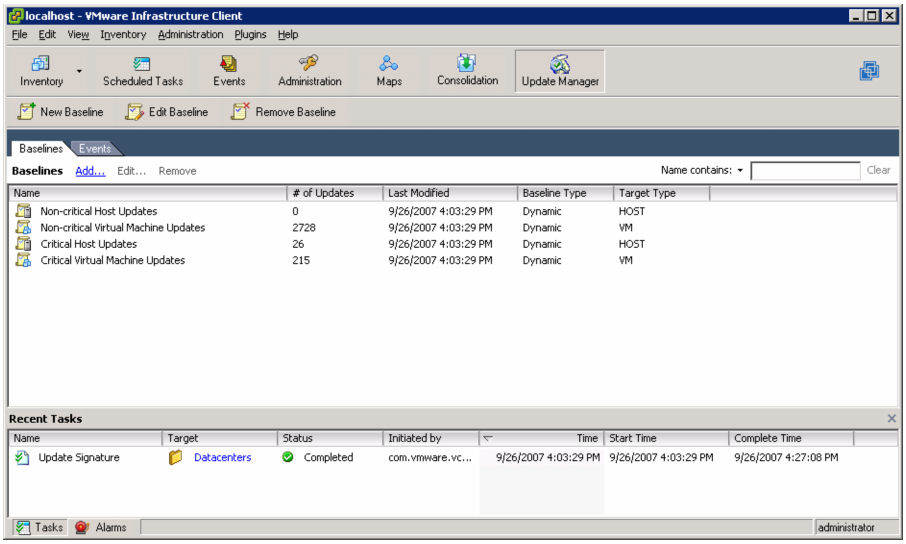
Update Manager includes four standard baselines:

- Non-critical Host Updates
- Non-critical Virtual Machine Updates
- Critical Host Updates
- Critical Virtual Machine Updates

Most deployments can benefit from customized baselines to meet the needs of your specific deployment. Creating additional 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 Clients for those clients that have the Update Manager plug-in installed.

You can view the default baselines by clicking the **Update Manager** button of the VirtualCenter client, as is shown in Figure 2-1.

Figure 2-1. An example of Baselines available on Update Manager



Name	# of Updates	Last Modified	Baseline Type	Target Type
Non-critical Host Updates	0	9/26/2007 4:03:29 PM	Dynamic	HOST
Non-critical Virtual Machine Updates	2728	9/26/2007 4:03:29 PM	Dynamic	VM
Critical Host Updates	26	9/26/2007 4:03:29 PM	Dynamic	HOST
Critical Virtual Machine Updates	215	9/26/2007 4:03:29 PM	Dynamic	VM

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Update Signature	Datacenters	Completed	com.vmware.vc...	9/26/2007 4:03:29 PM	9/26/2007 4:03:29 PM	9/26/2007 4:27:08 PM

Creating Baselines

You can create additional baselines by using Update Manager. You can achieve this through the **Update Manager** tab or by using the **Baseline Creation Wizard**, which you can start from the **Update Manager** tab. These baselines can be either dynamic or fixed. Dynamic baselines consist of a set of updates that meet user-defined criteria. For example, a dynamic baseline might include all critical updates. 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 baseline by using the Baseline Creation wizard (SEE UPDATE)

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

2 Click **Add**.

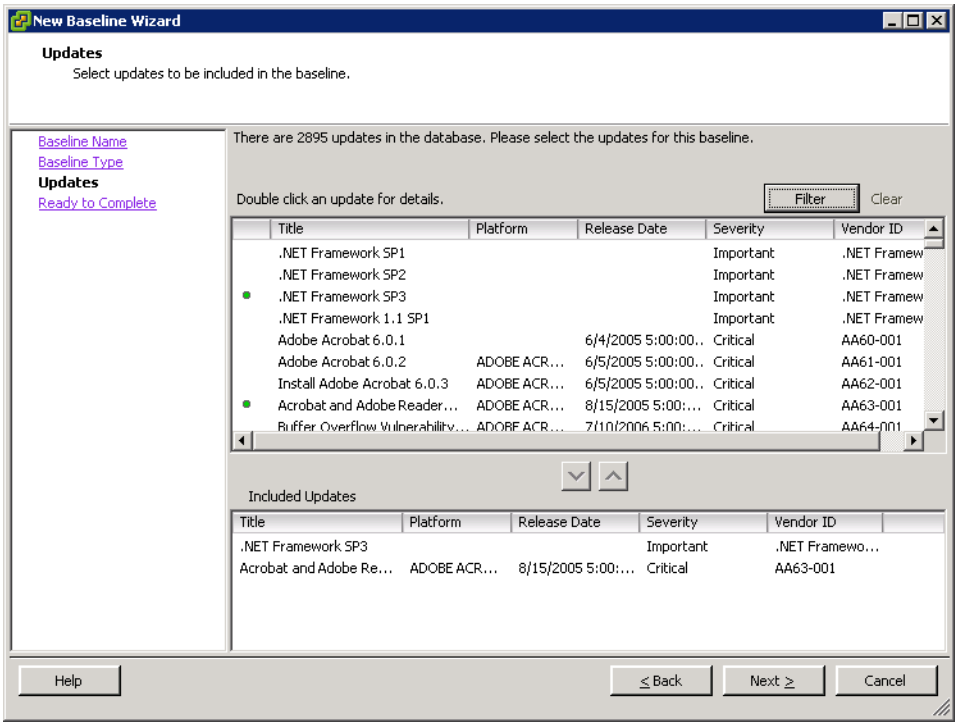
3 Provide information about this baseline.

Update Manager does not support single baselines that apply to both target types. Baselines must apply to either ESX Server hosts or virtual machines.

4 Click **Next**.

5 Select the type of updates to be included in this baseline.

6 Click **Next**.



Updates

Select updates to be included in the baseline.

There are 2895 updates in the database. Please select the updates for this baseline.

Double click an update for details.

	Title	Platform	Release Date	Severity	Vendor ID
	.NET Framework SP1			Important	.NET Framew
	.NET Framework SP2			Important	.NET Framew
●	.NET Framework SP3			Important	.NET Framew
	.NET Framework 1.1 SP1			Important	.NET Framew
	Adobe Acrobat 6.0.1		6/4/2005 5:00:00..	Critical	AA60-001
	Adobe Acrobat 6.0.2	ADOBE ACR...	6/5/2005 5:00:00..	Critical	AA61-001
	Install Adobe Acrobat 6.0.3	ADOBE ACR...	6/5/2005 5:00:00..	Critical	AA62-001
●	Acrobat and Adobe Reader...	ADOBE ACR...	8/15/2005 5:00:...	Critical	AA63-001
	Buffer Overflow Vulnerability...	ADOBE ACR...	7/10/2006 5:00:...	Critical	AA64-001

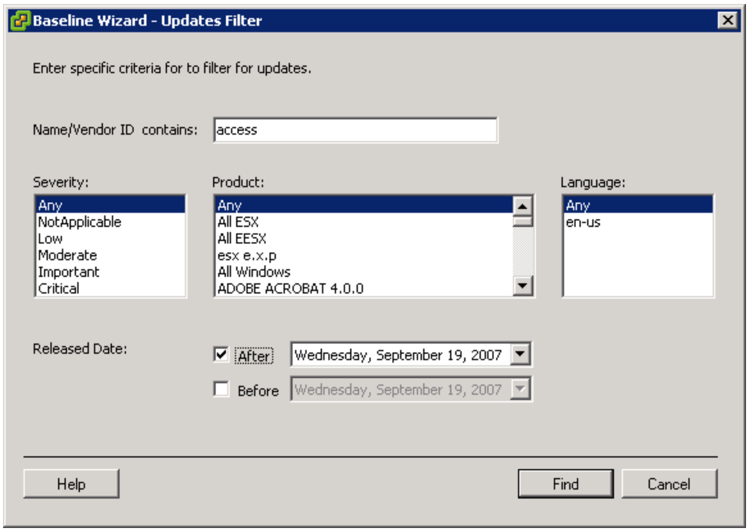
Included Updates

Title	Platform	Release Date	Severity	Vendor ID
.NET Framework SP3			Important	.NET Framewo...
Acrobat and Adobe Re...	ADOBE ACR...	8/15/2005 5:00:...	Critical	AA63-001

7 Customize the dynamic update.

a Select individual updates to be included from this baseline and click the down arrow.

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



Enter specific criteria for to filter for updates.

Name/Vendor ID contains: access

Severity: Any, NotApplicable, Low, Moderate, Important, Critical

Product: Any, All ESX, All EESX, esx e.x.p, All Windows, ADOBE ACROBAT 4.0.0

Language: Any, en-us

Released Date:

☑ After Wednesday, September 19, 2007

☐ Before Wednesday, September 19, 2007

8 Enter search criteria and click **Find**.

- **Name/Vendor ID Contains** – Enter text to restrict the updates displayed. Text entered in this field searches update names and ID numbers. Standard wildcard logic is used in assessing these names. You can enter multiple names using commas to separate each item. This field is assessed cumulatively, so as more strings are entered, more updates are likely to be included in the baseline.

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

- **Product** – Select operating systems or products for which this baseline will include patches. Only applicable patches are evaluated. In other words, 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.
- **Language** – Select which language versions of patches to be included.
- **Released Date** – Provide **Before** and **After** dates to specify a date range for updates. When the range is bounded by single criteria, all updates before or after the specified date are included.

9 Click **Find**.

10 Select any further updates.

11 Click **Next**.

12 Click **Finish**.

Editing Baselines

You can edit existing baselines by using the VI Client.

To edit an existing baseline (SEE UPDATE)

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

2 Right-click an existing baseline and click **Edit Baseline**.

   a Click **Baseline Name** to modify the name and description of the baseline.

   b Click **Baseline Type** to change the types of updates included in the baseline.

   c Click **Updates** to add or remove specific updates from the baseline.

Attaching Baselines

You can attach existing baselines to objects in the VirtualCenter inventory. You can attach baselines to individual objects, but it is typically more efficient to attach baselines to objects containing virtual machines. Attaching a baseline to an object such as a folder or datacenter transitively attaches the baseline to all virtual machines contained in the object.

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 **Attach Baseline**.

3 Select one or more baselines to be attached and click **OK**.

Removing Baselines

(SEE UPDATE) You can remove attached baselines. You can remove baselines only from the object to which they were attached. VMware infrastructure objects often have inherited properties, including baseline associations, so to remove a baseline from an object, you might have to navigate to the parent object to which the baseline is attached and remove it there.

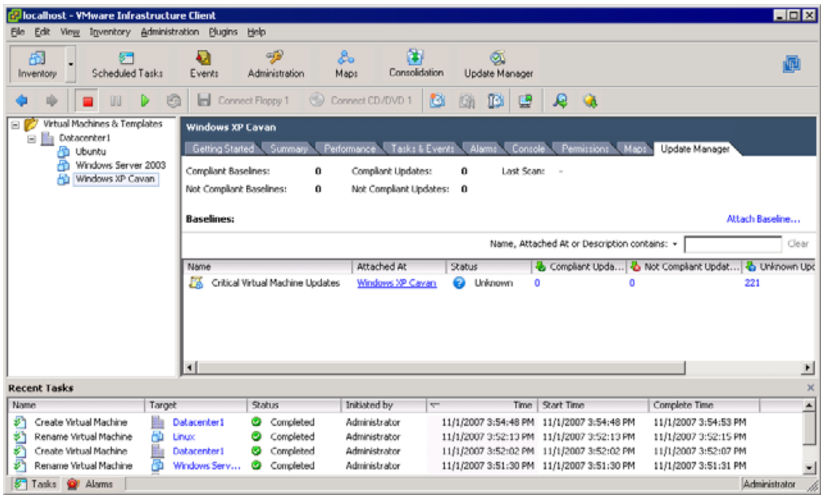
To remove a baseline

1 Connect the VI Client to a VirtualCenter server on which Update Manager is installed.

2 Navigate to the virtual infrastructure object want to remove the baseline from and click **Update Manager**.

3 Find the baseline to remove and review where the baseline is attached.

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



Compliant Baselines: 0
Not Compliant Baselines: 0
Compliant Updates: 0
Not Compliant Updates: 0
Last Scan: -

Baselines:

Name, Attached At or Description contains:

Name	Attached At	Status	Compliant Upda...	Not Compliant Updat...	Unknown Upc
Critical Virtual Machine Updates	Windows XP Cavan	Unknown	0	0	221

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Create Virtual Machine	Datacenter1	Completed	Administrator	11/1/2007 3:54:48 PM	11/1/2007 3:54:48 PM	11/1/2007 3:54:53 PM
Rename Virtual Machine	Linux	Completed	Administrator	11/1/2007 3:52:13 PM	11/1/2007 3:52:13 PM	11/1/2007 3:52:15 PM
Create Virtual Machine	Datacenter1	Completed	Administrator	11/1/2007 3:52:02 PM	11/1/2007 3:52:02 PM	11/1/2007 3:52:07 PM
Rename Virtual Machine	Windows Serv...	Completed	Administrator	11/1/2007 3:51:30 PM	11/1/2007 3:51:30 PM	11/1/2007 3:51:31 PM

4 Navigate to the object that the baseline is attached to.

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

The baseline is removed from the Virtual Infrastructure.

Scanning Virtual Machines and ESX Server Hosts

You can automatically scan virtual machines and ESX Server hosts using preestablished tasks or you can manually initiate scans, as required by users. Best practice is to run scans against objects that have baselines attached to them because this produces compliance information. You can scan objects without attaching baselines, but no compliance information is created. See “Attaching Baselines” on page 20.

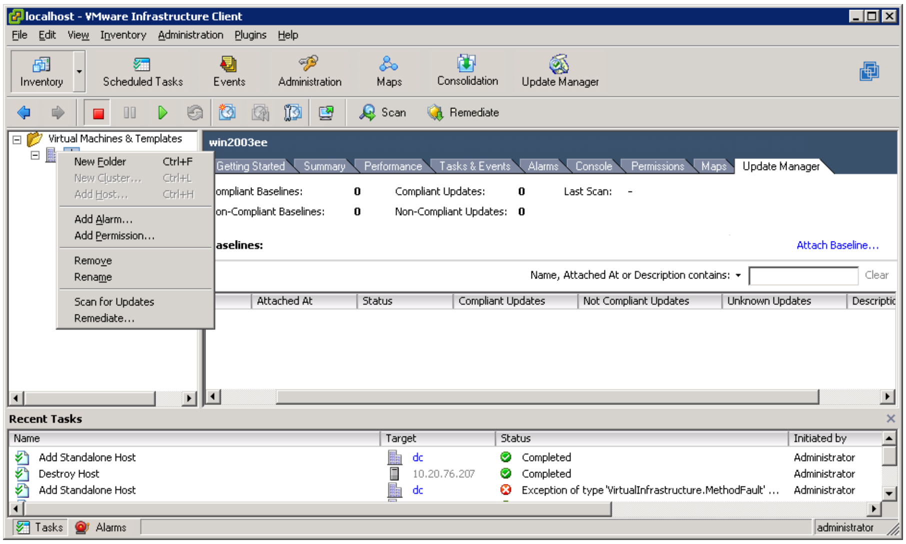
To manually initiate a scan

1 Connect the VI Client to a VirtualCenter server on which Update Manager is installed.

2 Click **Inventory** and click **Virtual Machines and Templates** for virtual machines or click **Hosts and Clusters** for ESX Server hosts.

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.



ompliant Baselines: 0
on-Compliant Baselines: 0
Compliant Updates: 0
Non-Compliant Updates: 0
Last Scan: -

aselines:

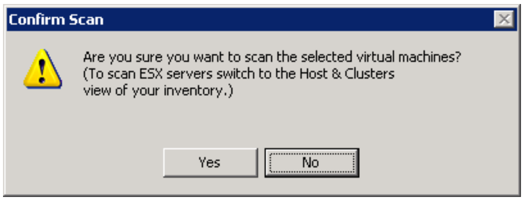
Name, Attached At or Description contains:

Attached At	Status	Compliant Updates	Not Compliant Updates	Unknown Updates	Descriptic

Recent Tasks

Name	Target	Status	Initiated by
Add Standalone Host	dc	Completed	Administrator
Destroy Host	10.20.76.207	Completed	Administrator
Add Standalone Host	dc	Exception of type 'VirtualInfrastructure.MethodFault' ...	Administrator

A message appears to confirm that you want to scan all the objects and child objects.



Confirm Scan

Are you sure you want to scan the selected virtual machines?
(To scan ESX servers switch to the Host & Clusters
view of your inventory.)

4 Click **Yes**.

For the results of the scan, see "Viewing Scan Results" on page 22.

To schedule a scan

1 Connect the VI Client to a VirtualCenter server on which Update Manager is installed and click **Scheduled Tasks**.

2 Right-click the **Scheduled Task** pane and click **New Scheduled Task.**

3 Select **Scan for Updates**.

4 Select the type of scan to schedule.

5 Click **Next**.

6 Select the objects to be scanned.

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

7 Click **Next**.

8 Configure when the task will run based on the state of the virtual machine or ESX Server.

9 Click **Next**.

10 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. You view compliance viewed in the VI Client. For ESX Server hosts, you view compliance in the Host and Cluster view. For virtual machines, you view compliance in the Virtual Machines and Templates view.

Supported groupings include Virtual Infrastructure container objects such as:

- Folders
- Clusters
- 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, but this also ensures 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 appear. The same Windows Vista virtual machines are not assessed for compliance with Windows XP patches, and as a result, the status of their compliance does not appear.
- 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, Non-Compliant and Unknown entities only appear as the user's permissions permit.

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

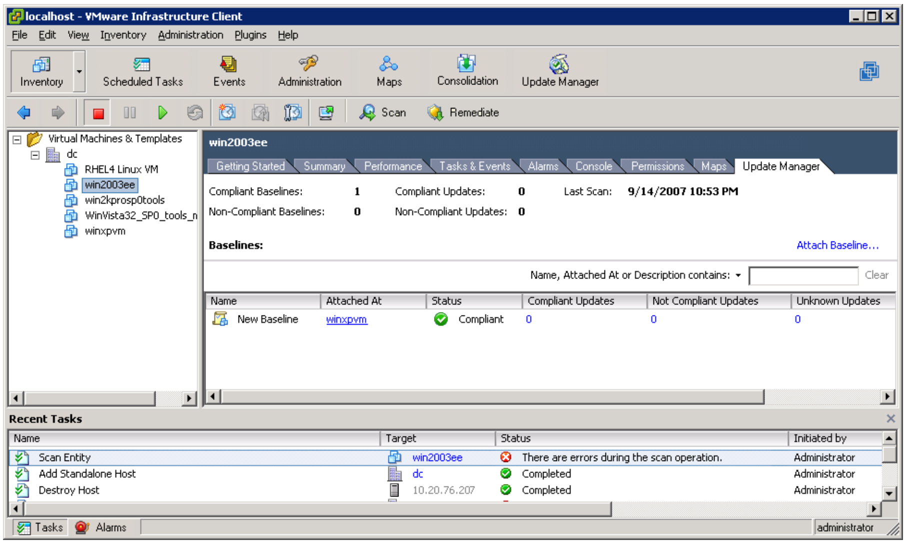
When scans are completed on all machines contained within a virtual infrastructure object, the results are a summary. Information that is displayed explains the degree of conformance with baselines, rather than the details. Information included is:

- When the last scan was completed at this level.
- The total number of compliant and noncompliant 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** and click **Virtual Machines and Templates** for virtual machines or click **Hosts and Clusters** for ESX Server hosts.
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.



Compliant Baselines: 1
Non-Compliant Baselines: 0
Compliant Updates: 0
Non-Compliant Updates: 0
Last Scan: 9/14/2007 10:53 PM

Baselines:

Name	Attached At	Status	Compliant Updates	Not Compliant Updates	Unknown Updates
New Baseline	winxpvm	Compliant	0	0	0

Recent Tasks

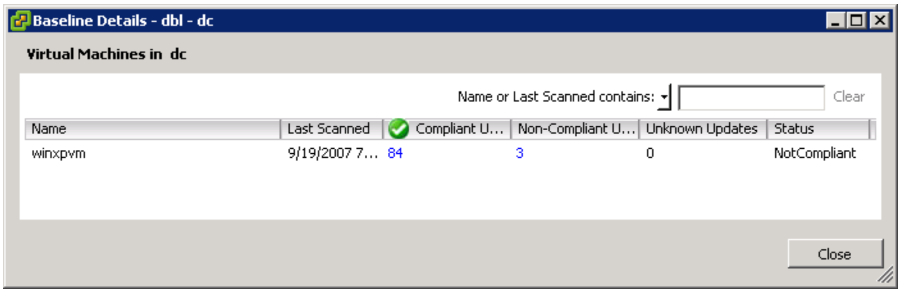
Name	Target	Status	Initiated by
Scan Entity	win2003ee	There are errors during the scan operation.	Administrator
Add Standalone Host	dc	Completed	Administrator
Destroy Host	10.20.76.207	Completed	Administrator

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.



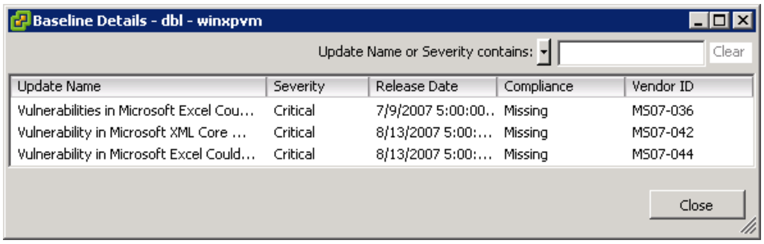
Name	Last Scanned	✓ Compliant U…	Non-Compliant U…	Unknown Updates	Status
winxpvm	9/19/2007 7…	84	3	0	NotCompliant

You can receive more information about a specific machines compliance with all updates 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 Compliance Details window appears.


Baseline Details - dbl - winxpvm
Update Name or Severity contains:
Clear
Close

Update Name	Severity	Release Date	Compliance	Vendor ID
Vulnerabilities in Microsoft Excel Cou…	Critical	7/9/2007 5:00:00..	Missing	MS07-036
Vulnerability in Microsoft XML Core …	Critical	8/13/2007 5:00:…	Missing	MS07-042
Vulnerability in Microsoft Excel Could…	Critical	8/13/2007 5:00:…	Missing	MS07-044

Reviewing Scan Results for Individual Virtual Machines and ESX Hosts

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

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 **Virtual Machines and Templates** and then 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.
3. Click the **Update Manager** tab.

To review scan results for an ESX hosts

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

Remediating ESX Hosts and Virtual Machines

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

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 may 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 makes it easy to recover from these.

Guest Shutdown

If you complete remediations immediately, machines are rebooted at the end of the remediation process if a reboot is required. A dialog box tells 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 time specified elapses, a final timer before shutdown appears.

Manual Virtual Machine Remediation

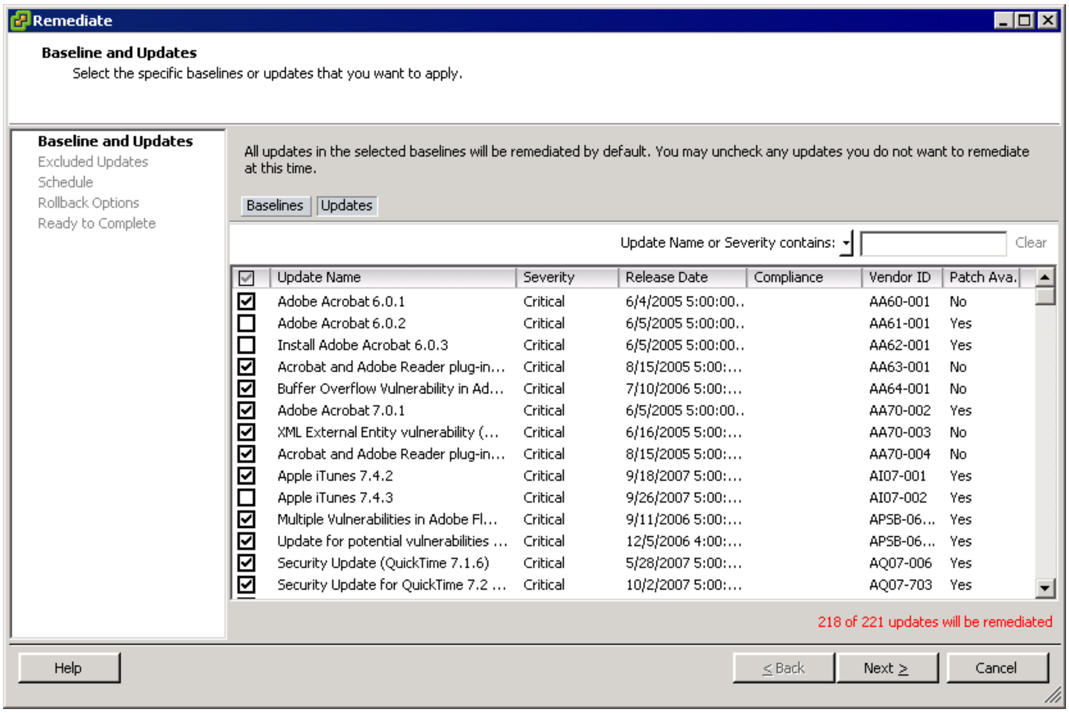
Users can manually remediate virtual machines on a case-by-case basis.

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 to remediate.
6. To exclude individual updates from the remediation process, click **Updates**.

The Baselines and Updates page of the Remediation wizard appears.



Remediate

Baseline and Updates

Select the specific baselines or updates that you want to apply.

All updates in the selected baselines will be remediated by default. You may uncheck any updates you do not want to remediate at this time.

Update Name or Severity contains:

☑	Update Name	Severity	Release Date	Compliance	Vendor ID	Patch Ava.
☑	Adobe Acrobat 6.0.1	Critical	6/4/2005 5:00:00..		AA60-001	No
☐	Adobe Acrobat 6.0.2	Critical	6/5/2005 5:00:00..		AA61-001	Yes
☐	Install Adobe Acrobat 6.0.3	Critical	6/5/2005 5:00:00..		AA62-001	Yes
☑	Acrobat and Adobe Reader plug-in...	Critical	8/15/2005 5:00:...		AA63-001	No
☑	Buffer Overflow Vulnerability in Ad...	Critical	7/10/2006 5:00:...		AA64-001	No
☑	Adobe Acrobat 7.0.1	Critical	6/5/2005 5:00:00..		AA70-002	Yes
☑	XML External Entity vulnerability (...	Critical	6/16/2005 5:00:...		AA70-003	No
☑	Acrobat and Adobe Reader plug-in...	Critical	8/15/2005 5:00:...		AA70-004	No
☑	Apple iTunes 7.4.2	Critical	9/18/2007 5:00:...		AI07-001	Yes
☐	Apple iTunes 7.4.3	Critical	9/26/2007 5:00:...		AI07-002	Yes
☑	Multiple Vulnerabilities in Adobe Fl...	Critical	9/11/2006 5:00:...		APSB-06...	Yes
☑	Update for potential vulnerabilities ...	Critical	12/5/2006 4:00:...		APSB-06...	Yes
☑	Security Update (QuickTime 7.1.6)	Critical	5/28/2007 5:00:...		AQ07-006	Yes
☑	Security Update for QuickTime 7.2 ...	Critical	10/2/2007 5:00:...		AQ07-703	Yes

218 of 221 updates will be remediated

7 Select which updates will be included or excluded from the remediation and click **Next**.

8 Review the list of updates that will be excluded and click **Next**.

9 Select the time to complete the remediation actions based on the state of the virtual machines and click **Next**.

10 Select the snapshot options including a name and description for the snapshot that is created to support rollbacks. Click **Next**.

11 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.

5 Select the baselines to remediate.

6 To exclude individual updates from the remediation process, click **Updates**.

7 Select which updates to include or exclude from the remediation and click **Next**.

8 Review the list of updates that will be excluded and click **Next**.

9 Select the time to complete the remediation actions and the remediation failure response options and click **Next**.

10 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 Right-click the **Scheduled Task** pane and click **New Scheduled Task**.

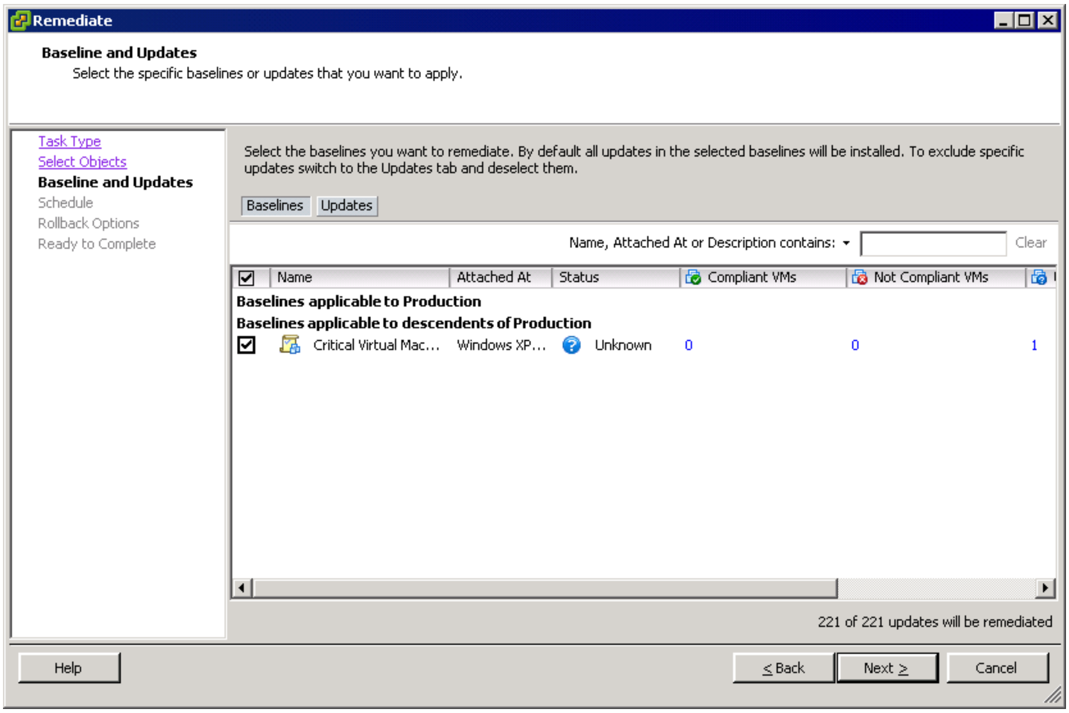
2 Select **Remediate** and click **OK**.

3 Select **Virtual Machines / Guest Operating Systems** and click **Next**.

4 Select the objects to which this remediation will apply.

All child objects of the selected object are remediated as well.

5 Click **Next**.



Remediate

Baseline and Updates

Select the specific baselines or updates that you want to apply.

Task Type
Select Objects
Baseline and Updates
Schedule
Rollback Options
Ready to Complete

Select the baselines you want to remediate. By default all updates in the selected baselines will be installed. To exclude specific updates switch to the Updates tab and deselect them.

Baselines | Updates

Name, Attached At or Description contains: ▾ Clear

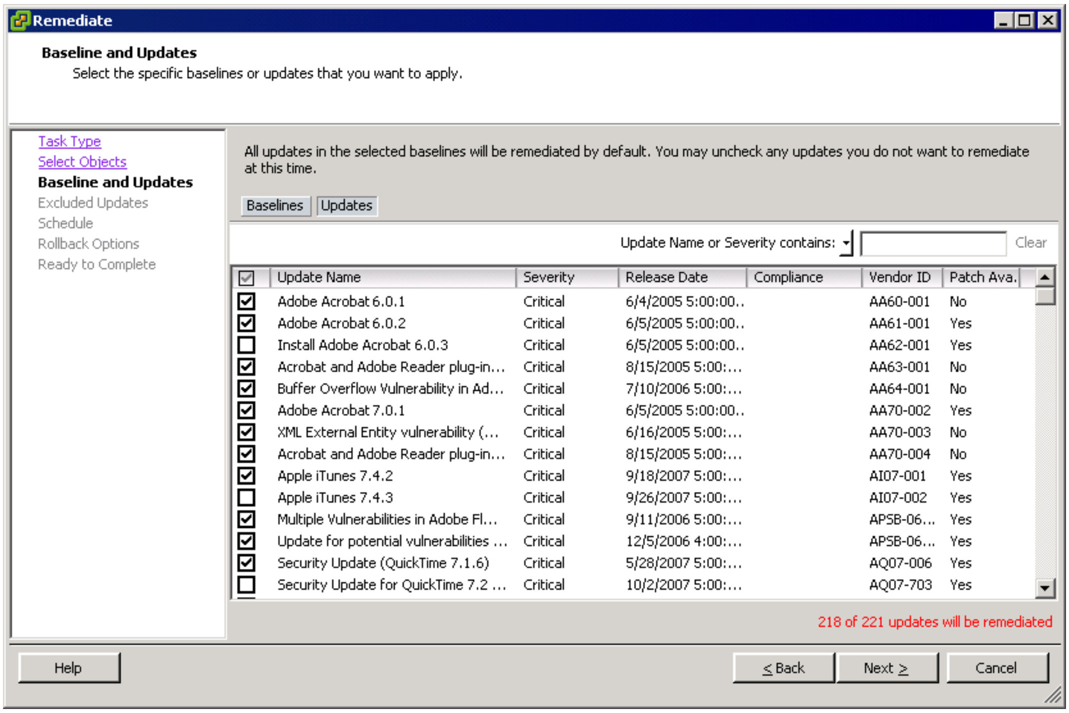
☑	Name	Attached At	Status	Compliant VMs	Not Compliant VMs	
	Baselines applicable to Production					
	Baselines applicable to descendents of Production					
☑	Critical Virtual Mac...	Windows XP...	Unknown	0	0	1

221 of 221 updates will be remediated

6 Select the baselines to remediate.

7 To exclude individual updates from the remediation process, click **Updates**.

The Updates page of the Remediate wizard appears.



Baseline and Updates

Select the specific baselines or updates that you want to apply.

All updates in the selected baselines will be remediated by default. You may uncheck any updates you do not want to remediate at this time.

Update Name or Severity contains:

☑	Update Name	Severity	Release Date	Compliance	Vendor ID	Patch Ava.
☑	Adobe Acrobat 6.0.1	Critical	6/4/2005 5:00:00..		AA60-001	No
☑	Adobe Acrobat 6.0.2	Critical	6/5/2005 5:00:00..		AA61-001	Yes
□	Install Adobe Acrobat 6.0.3	Critical	6/5/2005 5:00:00..		AA62-001	Yes
☑	Acrobat and Adobe Reader plug-in...	Critical	8/15/2005 5:00:...		AA63-001	No
☑	Buffer Overflow Vulnerability in Ad...	Critical	7/10/2006 5:00:...		AA64-001	No
☑	Adobe Acrobat 7.0.1	Critical	6/5/2005 5:00:00..		AA70-002	Yes
☑	XML External Entity vulnerability (...	Critical	6/16/2005 5:00:...		AA70-003	No
☑	Acrobat and Adobe Reader plug-in...	Critical	8/15/2005 5:00:...		AA70-004	No
☑	Apple iTunes 7.4.2	Critical	9/18/2007 5:00:...		AI07-001	Yes
□	Apple iTunes 7.4.3	Critical	9/26/2007 5:00:...		AI07-002	Yes
☑	Multiple Vulnerabilities in Adobe Fl...	Critical	9/11/2006 5:00:...		APSB-06...	Yes
☑	Update for potential vulnerabilities ...	Critical	12/5/2006 4:00:...		APSB-06...	Yes
☑	Security Update (QuickTime 7.1.6)	Critical	5/28/2007 5:00:...		AQ07-006	Yes
□	Security Update for QuickTime 7.2 ...	Critical	10/2/2007 5:00:...		AQ07-703	Yes

218 of 221 updates will be remediated

8 Select which updates to include or exclude from the remediation and click **Next**.

9 Review the list of updates that will be excluded and click **Next**.

10 Configure when the task will run depending on virtual machine state and click **Next**.

11 Select the snapshot options including a name and description for the snapshot that is created to support rollbacks 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 Right-click the **Scheduled Task** pane and click **New Scheduled Task**.

2 Select **Remediate** and click **OK**.

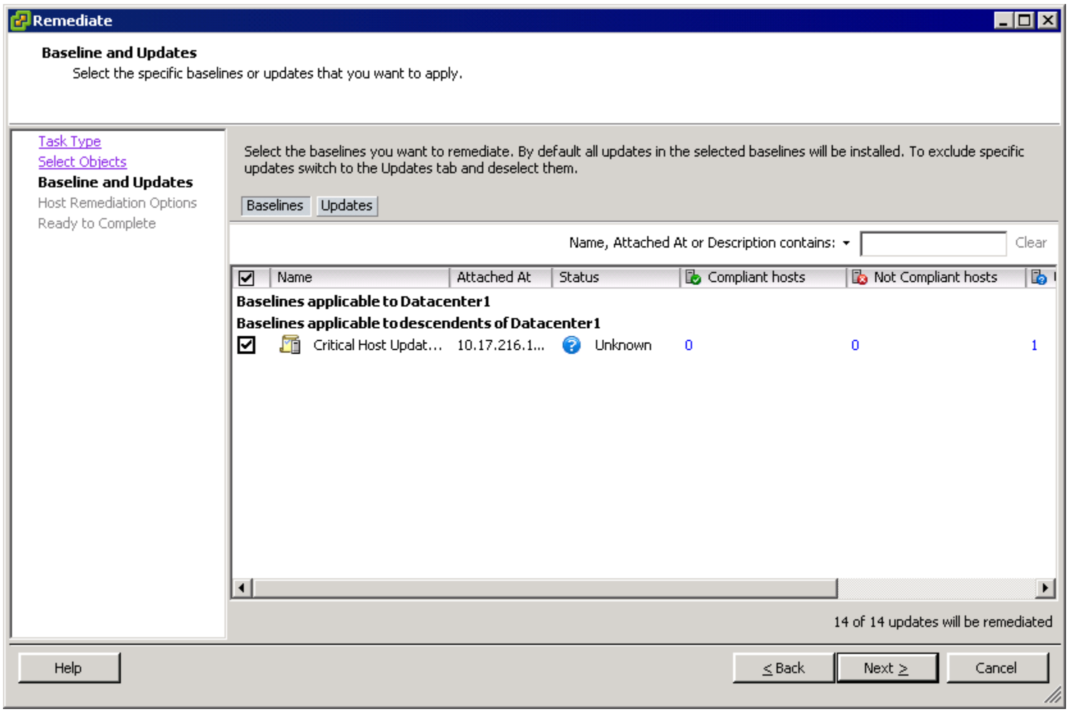
3 Select **ESX Servers** and click **Next**.

4 Select the objects to which this remediation will apply.

All child objects of the selected object are remediated as well.

5 Click **Next**.

The Baselines and Updates page appears.



Remediate

Baseline and Updates

Select the specific baselines or updates that you want to apply.

Select the baselines you want to remediate. By default all updates in the selected baselines will be installed. To exclude specific updates switch to the Updates tab and deselect them.

Name, Attached At or Description contains: ▾ Clear

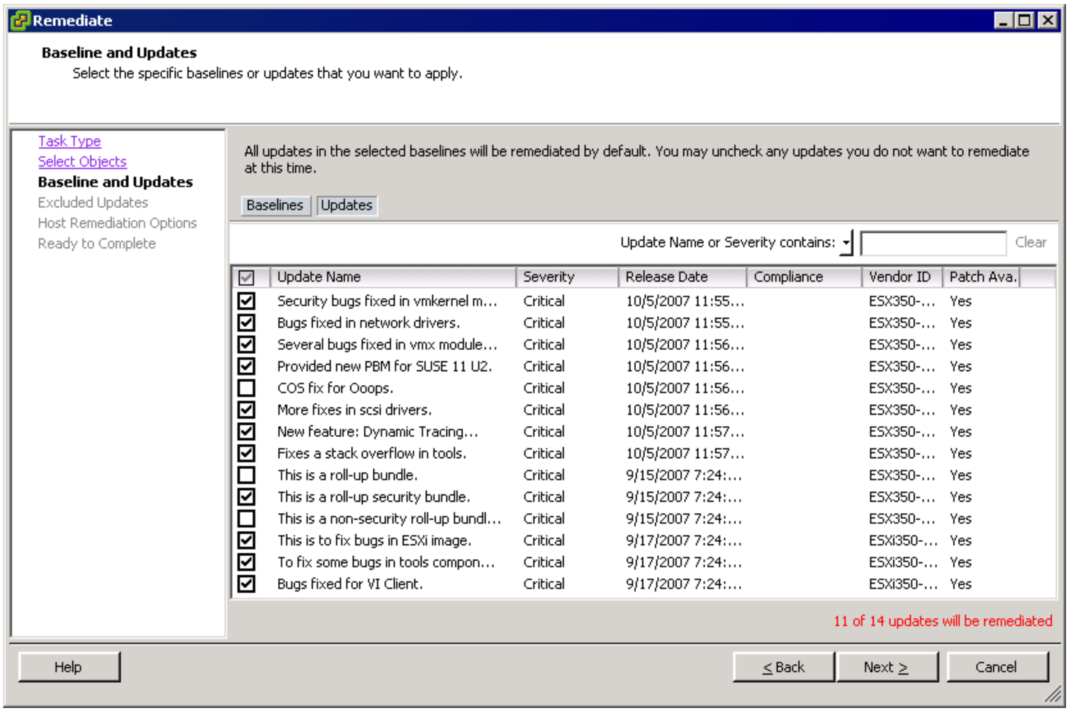
☑	Name	Attached At	Status	Compliant hosts	Not Compliant hosts	
	Baselines applicable to Datacenter1					
	Baselines applicable to descendents of Datacenter1					
☑	Critical Host Updat...	10.17.216.1...	Unknown	0	0	1

14 of 14 updates will be remediated

6 Select the baselines to remediate.

To exclude individual updates from the remediation process, click **Updates**.

The Updates page of the Remediate wizard appears.



Remediate

Baseline and Updates

Select the specific baselines or updates that you want to apply.

All updates in the selected baselines will be remediated by default. You may uncheck any updates you do not want to remediate at this time.

Update Name or Severity contains: ▾ Clear

☑	Update Name	Severity	Release Date	Compliance	Vendor ID	Patch Ava.
☑	Security bugs fixed in vmkernel m...	Critical	10/5/2007 11:55...		ESX350-...	Yes
☑	Bugs fixed in network drivers.	Critical	10/5/2007 11:55...		ESX350-...	Yes
☑	Several bugs fixed in vmx module...	Critical	10/5/2007 11:56...		ESX350-...	Yes
☑	Provided new PBM for SUSE 11 U2.	Critical	10/5/2007 11:56...		ESX350-...	Yes
□	COS fix for Ooops.	Critical	10/5/2007 11:56...		ESX350-...	Yes
☑	More fixes in scsi drivers.	Critical	10/5/2007 11:56...		ESX350-...	Yes
☑	New feature: Dynamic Tracing...	Critical	10/5/2007 11:57...		ESX350-...	Yes
☑	Fixes a stack overflow in tools.	Critical	10/5/2007 11:57...		ESX350-...	Yes
□	This is a roll-up bundle.	Critical	9/15/2007 7:24:...		ESX350-...	Yes
☑	This is a roll-up security bundle.	Critical	9/15/2007 7:24:...		ESX350-...	Yes
□	This is a non-security roll-up bundl...	Critical	9/15/2007 7:24:...		ESX350-...	Yes
☑	This is to fix bugs in ESXi image.	Critical	9/17/2007 7:24:...		ESXi350-...	Yes
☑	To fix some bugs in tools compon...	Critical	9/17/2007 7:24:...		ESXi350-...	Yes
☑	Bugs fixed for VI Client.	Critical	9/17/2007 7:24:...		ESXi350-...	Yes

11 of 14 updates will be remediated

7 Select which updates to include or exclude from the remediation and click **Next**.

8 Review the list of updates that will be excluded and click **Next**.

9 Select remediation options including when the remediation will take place and how remediation failures will be handled and click **Next**.

10 Review the summary information for the task to be completed and click **Finish**.

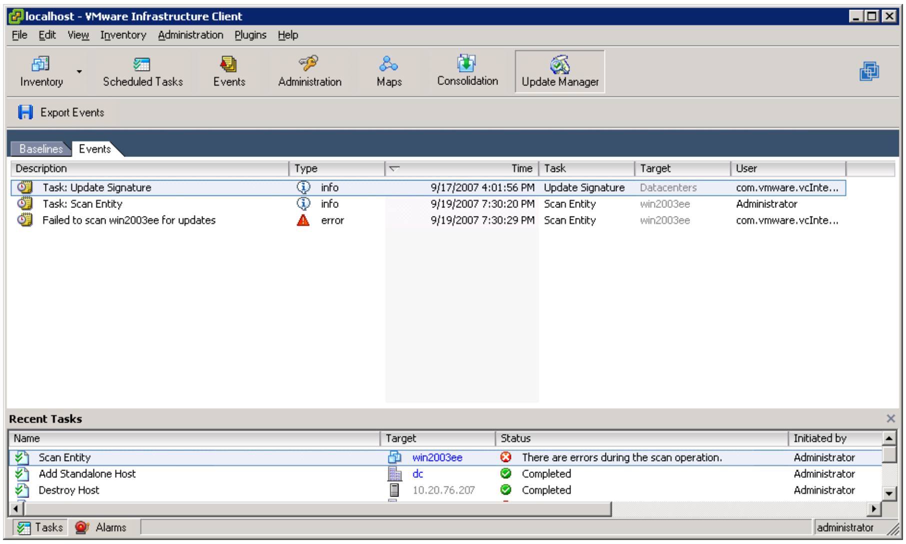
Working with Update Manager Events

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 33.

To review events

Connect the VI Client to a VirtualCenter server on which Update Manager is installed and click **Update Manager**.

Information about recent events appears.



Description	Type	Time	Task	Target	User
Task: Update Signature	info	9/17/2007 4:01:56 PM	Update Signature	Datacenters	com.vmware.vcInte...
Task: Scan Entity	info	9/19/2007 7:30:20 PM	Scan Entity	win2003ee	Administrator
Failed to scan win2003ee for updates	error	9/19/2007 7:30:29 PM	Scan Entity	win2003ee	com.vmware.vcInte...

Name	Target	Status	Initiated by
Scan Entity	win2003ee	There are errors during the scan operation.	Administrator
Add Standalone Host	dc	Completed	Administrator
Destroy Host	10.20.76.207	Completed	Administrator

To export events

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

2 Click the **Events** tab and click **Export Events**.

3 Provide information about how to export the events and click **Save**.

   a Provide a name for the file in which to save the events.

   b Select a format in which to save the events. Available formats include Excel Spreadsheet, HTML with or without CSS, comma delimited files, or XML.

Review the exported events using a viewer of your choice.

Operations Reference 3

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 31.

“Events” on page 33.

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** > **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 websites. Shavlik provides metadata for virtual machines and applications and VMware provides metadata for ESX Server hosts. A common cause of having no updates available for baselines is that Update Manager cannot contact the Shavlik servers. The connection between Update Manager and the website includes several links, the failure of any of which might cause updates in baselines to be unavailable. For example, some possible causes and solutions include:

- Shavlik being unavailable. Check the Shavlik Web site to determine whether the website is available. The URL for the Shavlik website is http://www.shavlik.com.
- VMware update service being unavailable to provide information about ESX Server updates.

- Web server proxy misconfiguration. See "Configuring Update Manager to Use with an Internet Proxy" on page 15.
- Poor network connectivity. Check to determine 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 Not Applicable. Such a condition typically indicates an error in scanning. Examine the server logs for ScanTasks that are marked as Failed.

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.

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 31.

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 NonCompliant

For Windows virtual machines, check the registry to ensure 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 presents 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 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 of a patch installation and the completion 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 as 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 tab 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 only apply 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 ensure that the account being used to do the scanning has sufficient permissions and that your SSL connections are properly configured.

Events

Update Manager produces events during normal functioning. You can use these events to understand the processes that the system is completing.

Table 3-1. Update Manager Events

Type	Message Text	Information
Info	Successfully downloaded guest update metadata. New updates: *`number of updates`*	
Error	Failed to download guest update metadata	Check your network connections to ensure 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 ensure 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 ensure that your metadata source is reachable.
Info	Successfully downloaded guest update packages. New packages: *`number of guest update packages`*	
Error	Failed to download guest update packages	Check your network connections to ensure that your update source is reachable.
Info	Successfully downloaded guest update packages for UNIX. New packages: *`number of guest update packages`*	
Error	Failed to download guest update packages for UNIX	Check your network connections to ensure that your update source is reachable.
Info	Successfully downloaded host update packages. New packages: *`number of guest update packages`*	
Error	Failed to download host update packages	Check your network connections to ensure that your update source is reachable.
Info	Successfully scanned *`data.Updates`* for updates	

Table 3-1. Update Manager Events (Continued)

Type	Message Text	Information
Error	Failed to scan *virtual machine or ESX_Server name* for updates	
Warning	Warning during scanning *virtual machine or ESX Server 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 virtual machine's state. Consider rebooting the virtual machine to facilitate scanning.
Error	Failed to scan *ESX Sever name* for updates because of an invalid state: *ESX Server state*	Check the state of the ESX. Consider rebooting the host to facilitate scanning.
Info	Remediation succeeded for *virtual machine or ESX Server name*	
Error	Remediation failed for *virtual machine or ESX Server name* with *error message*	Check the target's state. Consider restarting the target to facilitate remediation.
Error	Failed to remediate *virtual machine name* for updates because of an invalid state: *data.state.@enum.VirtualMachine.ConnectionState*	Check the virtual machine's state. Consider restarting the virtual machine to facilitate remediation.
Error	Failed to remediate *ESX Server Nmae* for updates because of an invalid state: *data.state.@enum.HostSystem.ConnectionState*	Check the state of the ESX Server. Consider restarting the host to facilitate remediation.
Error	Failed to scan or remediate *virtual machine name* because of unsupported or unknown OS: *data.os*	
Error	Can't remediate *virtual machine name*: Remediation of Linux virtual machines is not supported	
Info	Update Manager download alert (critical/total): ESX *data.esxCritical*/*data.esxTotal*; Windows *data.windowsCritical*/*data.windowsTotal*; Linux *data.linuxCritical*/*data.linuxTotal*	Provides information about the number of updates downloaded.
Error	Failed to scan *vm.name* for updates because host *host.name* is of unsupported version *data.version*	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Failed to remediate *vm.name* for updates because host *host.name* is of unsupported version *data.version*	For the latest information on which hosts can be scanned, see the release notes.
Error	Failed to scan *host.name* for updates because it is of unsupported version *data.version*	Hosts beginning with 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 *host.name* for updates because it is of unsupported version *data.version*	Hosts beginning with 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	Update Manager Guest Agent successfully installed on *vm.name*	
Error	Failed to install Update Manager Guest Agent on *vm.name*	Update Manager Guest Agent is required for remediating virtual machines. For more information on installing Update Manager Guest Agent, see the Update Manager Administrative Guide.

Table 3-1. Update Manager Events (Continued)

Type	Message Text	Information
Error	Failed to install Update Manager Guest Agent on *vm.name* because VMware Tools is not installed or is of an incompatible VMware Tools version. The required version is *data.requiredVersion* and the installed version is *data.installedVersion*.	
Error	There is no Update Manager license for *data.name* for the required operation.	Consider obtaining the required licenses to complete the desired task.
Error	Update Manager is running out of storage space. Location: *data.Volume*. Available space: *data.FreeSpace*	Consider adding more storage.
Error	Update Manager is critically low on storage space! Location: *data.Volume*. Available space: *data.FreeSpace*	Consider adding more storage.
Error	Update Manager Guest Agent failed to respond in time on *vm.name*. Please check if the VM is powered on and Guest Agent is running.	
Error	An internal error occurred in communication with Update Manager Guest Agent on *vm.name*. Please check if the VM is powered on and retry the operation.	
Error	An unknown internal error occurred during the required operation on *vm.name*. Please check the logs for more details and retry the operation.	
Error	Failed to install update *data.updateId* on *data.entityName*	
Info	Install of update *data.updateId* on *data.entityName* *data.message*	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Failed to scan orphaned VM *vm.name*	
Info	Failed to remediate orphaned VM *vm.name*	
Error	Failure in downloading patches for following updates: *data.message*	Check your network connections to ensure that your patch source is reachable.

Index

Updates for the Administration Guide

Last Updated: July 09, 2009

This document provides updates to the Update Manager 1.0 *Administration Guide*. Updated descriptions and procedures 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 *Administration Guide*:

- Updates for the Installing, Upgrading, and Uninstalling Update Manager Section on Page 11
- Updates for the Installing the Update Manager Download Service Section on Page 13
- Updates for the To manually modify proxy configuration Procedure on Page 16
- Updates for the To create a baseline by using the Baseline Creation wizard Procedure on Page 18
- Updates for the To edit an existing baseline Procedure on Page 20
- Updates for Removing Baselines Section on Page 20

Updates for the Installing, Upgrading, and Uninstalling Update Manager Section on Page 11

Information about SQL Server 2005 Express is missing from Table 2-1. The following updated table now contains new patch and driver requirements for Oracle 10g Release 2.

Database Type	Patch and Driver Requirements
SQL Server 2000	Use SQL Server driver for the client.
SQL Server 2005	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 (10.1.0.3.0)	None
Oracle 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.

The preparation of the Update Manager database is omitted in the Installing, Upgrading, and Uninstalling Update Manager section.

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."

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.

Updates for the Installing the Update Manager Download Service Section on Page 13

The Installing the Update Manager Download Service section contains an example that states the required amount of space incorrectly. Instead, the example should be the following.

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 will be patching, as well as the number of years you will be gathering patches on this system. Expect to need 50GB for each year of ESX Server patching and 11GB 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 100GB for the hosts and 44GB for the virtual machines for a total of 144GB. Therefore, to install in such an environment, install it to a server with at least 144GB of available space for patch storage.

Updates for the To manually modify proxy configuration Procedure on Page 16

In the To manually modify proxy configuration procedure the steps for manually modifying the proxy configuration are incorrect. The correct procedure is the following:

To manually modify proxy configuration

1 Find the `vci-integrity.xml` file in the Update Manager installation directory.

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

2 Create a backup copy of this file in case you need to revert to the previous configuration.

3 Edit the file by changing the values within the following tags:

```
<proxyPort>3128</proxyPort>

<proxyServer>yournewproxy.companydomain.com</proxyServer>

<useProxyServer>true</useProxyServer>
```

4 Save and close the file.

Updates for the To create a baseline by using the Baseline Creation wizard Procedure on Page 18

The To create a baseline by using the Baseline Creation wizard procedure does not describe the steps to create a dynamic baseline. Instead, the procedure is the following.

To create a baseline by using the Baseline Creation wizard

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

2 On the **Baselines** tab, click **Add**.

3 Provide a name and a description of this baseline.

Update Manager does not support single baselines that apply to both target types. Baselines must apply to either ESX Server hosts or virtual machines.

4 Click **Next**.

5 Choose the type of the baseline.

The options are: **Fixed** and **Dynamic**.

Decide what updates to include in the dynamic baseline and whether to add or remove specific updates from it.

6 Click **Next**.

Depending on the choices you make, one of the following pages appears:

- The Updates page, if you chose to create a fixed baseline
- The Ready to Complete page, if you chose to create a dynamic baseline
- The Exclusions page, if you chose to create a dynamic baseline and to add or remove specific updates from it

7 Customize the baseline.

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

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

8 Enter search criteria and click **Find**.

- **Name/Vendor ID contains** – Enter text to restrict the updates displayed. Text entered in this field searches update names and ID numbers. Standard wildcard logic is used in assessing these names. Enter multiple names by using commas to separate each item. This field is assessed cumulatively, so as more strings are entered, more updates are likely to be included in the baseline.
- **Severity** – Select the severity of updates to be included in this update.
- **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.
- **Language** – Select which language versions of patches to include.
- **Released Date** – Provide **Before** and **After** dates to specify a date range for updates. When the range is bounded by single criteria, all updates before or after the specified date are included.

9 Select any further updates.

10 Click **Next**.

If you select to create a dynamic baseline and add or remove updates from the list of all critical and noncritical updates, the **Inclusions** page appears.

11 Select individual updates to include in the baseline and click **Next**.

12 Review the Ready to Complete page and click **Finish**.

Updates for the To edit an existing baseline Procedure on Page 20

The To edit an existing baseline procedure states that to add or remove specific updates from the baseline you have to click **Updates**.

In addition, if the existing baseline is dynamic, click **Exclusions** or **Inclusions** to review and edit the updates.

Updates for Removing Baselines Section on Page 20

The Removing Baselines section does not indicate the difference between detaching and removing baselines.

To detach a baseline from an inventory object means that the baseline will be no more applied to the object, but the baseline is still present on the **Baselines** tab. To remove a baseline means to delete it from the VI Client.

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 Virtual Infrastructure object.

To remove a baseline

1 Connect the VI Client to a VirtualCenter Server on which Update Manager is installed.

2 Click **Update Manager**.

3 On the **Baselines** tab, select the baselines to remove.

4 Click **Remove**.

A message appears to confirm that you want to delete the selected baselines.

5 Click **Yes**.