VMware vCenter Update Manager Administration Guide

vCenter Update Manager 4.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000139-04

vmware®

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

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

The VMware Web site also provides the latest product updates.

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

docfeedback@vmware.com

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

Contents

Updated Information

This *VMware vCenter Update Manager Administration Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *VMware vCenter Update Manager Administration Guide*.

Table 1.

Revision	Description
EN-000139-04	Table "Update Manager Events," on page 84 now contains information that if you want to remediate a host running a virtual machine on which Update Manager or vCenter Server are installed, the machine must be manually migrated to another host.
EN-000139-03	■ "Configure a Microsoft SQL Server Database," on page 25 now includes a requirement for SQL Server databases to be in the default dbo schema. ■ "Create a New Data Source (ODBC)," on page 25 now contains updated information about database connection requirements. ■ "Installing Update Manager," on page 27 now contains updated information about system account and database connection requirements.
EN-000139-02	■ Table "Supported Database Formats," on page 22 now includes additional database formats supported by Update Manager. ■ "Installing and Uninstalling Update Manager," on page 27 and "Install Update Manager Server," on page 28 now reflect the support of Windows XP SP3. ■ Chapter 3, "Installing, Setting Up, and Using the Update Manager Download Service," on page 37 is updated to exclude shared folders as a valid mechanism for transferring patches to Update Manager. ■ "Use a Shared Repository as a Patch Download Source," on page 44 now reflects that Update Manager does not support the usage of folders located on a network share as a shared repository. ■ Minor revisions.
EN-000139-01	■ "Installing and Uninstalling Update Manager," on page 27 now reflects the support of Windows Server 2008. ■ Step 7 in the task "Install Update Manager Server," on page 28 now reflects that if the DSN uses Windows NT authentication, the fields for the user name and password can be left blank. ■ Changed the order of the topics in Chapter 3, "Installing, Setting Up, and Using the Update Manager Download Service," on page 37. ■ Updated "Export the Downloaded Updates," on page 40 to fix an incorrect command line and added a "What to do next" subsection. ■ Updated "Use a Shared Repository as a Patch Download Source," on page 44 with examples of the shared repository paths. ■ Minor revisions.
EN-000139-00	Initial release.

About This Book

The *VMware vCenter Update Manager Administration Guide* provides information on how to install, configure and use VMware® vCenter Update Manager to scan, patch, and upgrade (remediate) the objects in your vSphere environment. In addition, this book includes information on the most common user scenarios.

For scanning and remediation, Update Manager works with the following ESX/ESXi versions.

- For virtual machine patching operations, Update Manager works with ESX 3.5 and later and ESX 3i version 3.5 and later.
- For VMware Tools and virtual machine hardware upgrade operations, Update Manager works with ESX/ESXi version 4.0 and later.
- For ESX/ESXi host patching operations, Update Manager works with ESX 3.0.3 and later, ESX 3i version 3.5 and later.
- For ESX/ESXi host upgrade operations, Update Manager works with ESX 3.0.0 and later, ESX 3i version 3.5 and later.

Intended Audience

This book is intended for anyone who wants to install, upgrade, or use Update Manager. This book 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.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To 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

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

1 Understanding Update Manager

vCenter Update Manager enables centralized, automated patch and version management for VMware vSphere and offers support for VMware ESX/ESXi hosts, virtual machines, and virtual appliances.

Updates you specify can be applied to operating systems, as well as applications on scanned ESX/ESXi hosts, virtual machines, and virtual appliances. With Update Manager, you can:

- Scan for compliance and apply updates for guests, appliances, and hosts.
- Directly upgrade hosts, virtual machine hardware, VMware Tools, and virtual appliances.
- Update third-party software on hosts.

Update Manager requires network connectivity with VMware vCenter Server. Each installation of the Update Manager must be associated (registered) with a single vCenter Server instance. The Update Manager module consists of a plug-in that runs on the vSphere Client and a server component, which you can install on the same computer as the vCenter Server system or on a different computer.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode and you want to use Update Manager with each vCenter Server system, you must install and register Update Manager modules with each vCenter Server system. You can use Update Manager only with the vCenter Server system with which it is registered.

Update Manager can scan and remediate (update) powered on, suspended, and powered off virtual machines, and templates, in addition to scanning and remediating hosts. If the upgrade or patching fails, you can revert the virtual machines back to their prior condition without losing data. Update Manager can scan and remediate powered on, VMware Studio registered, Red Hat, Ubuntu, SUSE, and CentOS Linux virtual appliances.

You can deploy Update Manager in a secured network without Internet access. In such a case, you can use the VMware vCenter Update Manager Download Service to download patch metadata and patch binaries.

This chapter includes the following topics:

Security Best Practices

Maintaining current patching levels for operating systems and applications helps reduce the number of vulnerabilities in an environment and the range of issues requiring solutions.

All systems require ongoing patching and reconfiguration, or other solutions. Reducing the diversity of systems in an environment and keeping them in compliance are considered security best practices.

Advantages of Compliance

Many virus attacks take advantage of existing, well-known issues. Update Manager allows you to update virtual machines, appliances, and ESX/ESXi hosts to make your environment more secure.

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

To make your environment more secure:

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

In a typical large environment, many different machines run various operating systems. Adding virtual machines to an environment increases this diversity. Update Manager automates the process of determining the state of your environment and updates your VMware virtual machines and ESX/ESXi hosts.

Compliance and Security Best Practices

The goal of compliance is to increase the security of your deployment system.

To achieve the goal of compliance, and increase security and stability, regularly evaluate the following.

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

It is also important to determine who is responsible for making these evaluations, when these evaluations are to be made, and which tactics to use to implement the plan.

Update Manager Client Overview

The Update Manager Client has two main views, Administrator's view and Compliance view.

You can use the **Update Manager** icon under Solutions and Applications in the vSphere Client Home page or click **Admin view** from the Update Manager tab to access the Administrator's view. In the Update Manager Client Administrator's view you can perform the following tasks:

- Configure the Update Manager settings
- Create and manage baselines and baseline groups
- View Update Manager events
- Review the patch repository and add or remove patches from a baseline

Compliance view information for a selected inventory object is displayed on the Update Manager tab in the Hosts and Clusters or VMs and Templates inventory view of the vSphere Client. In the Update Manager Client Compliance view you can perform these tasks:

- View compliance and scan results for each selected inventory object
- Attach and detach baselines and baseline groups from a selected inventory object
- Scan a selected inventory object
- Stage patches for hosts
- Remediate a selected inventory object

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have installed and registered more than one Update Manager instance, you can configure the settings for each Update Manager instance. Configuration properties that you modify are applied only to the Update Manager instance that you specify and are not propagated to the other instances in the group. You can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered from the navigation bar.

If your vCenter Server is a part of a connected group in vCenter Linked Mode, you can manage baselines and baseline groups as well as scan and remediate only the inventory objects managed by the vCenter Server system with which Update Manager is registered.

About the Update Manager Process

Upgrading and applying patches with the Update Manager is a multistage process in which procedures must be performed in a particular order. Following the suggested process helps ensure a smooth update with a minimum of system downtime.

The Update Manager process begins by downloading information about a set of security patches. One or more of these patches are aggregated to form a baseline. Multiple baselines can be added to a baseline group. A baseline group is a composite object that consists of a set of nonconflicting baselines. You can use baseline groups to combine different types of baselines and then scan and remediate an inventory object against all of them as a whole. If a baseline group contains both upgrade and patch baselines, the upgrade executes first.

A collection of virtual machines, virtual appliances, and ESX/ESXi hosts or individual inventory objects can be scanned for compliance with a baseline or a baseline group and later remediated (updated). You can initiate these processes manually or through scheduled tasks.

The following list provides a high-level overview of the Update Manager process in your vSphere environment.

- Configuring the Update Manager Patch Download Source on page 14

  You can configure the Update Manager server to download patches either from the Internet or from a shared repository.

- Downloading Patches and Patch Metadata on page 14

  Downloading patches and patch metadata is an automatic process. At regular configurable intervals, Update Manager contacts Shavlik and VMware to gather the latest information (metadata) about available patches.

- Creating Baselines and Baseline Groups on page 15

  Creating baselines and baseline groups is an optional step. Baselines can be upgrade or patch baselines. Baselines contain a collection of one or more patches, service packs and bug fixes, or upgrades. Baseline groups are assembled from existing baselines and might contain one upgrade baseline per type and one or more patch baselines or a combination of multiple patch baselines.

- Attaching Baselines and Baseline Groups to vSphere Objects on page 15

  To use baselines and baseline groups, you must attach them to selected inventory objects such as virtual machines, virtual appliances, or hosts.

- Scanning Selected vSphere Objects on page 15

  Scanning is the process in which attributes of a set of hosts, virtual machines, or virtual appliances are evaluated against all patches and upgrades in the repository depending on the type of scan you select.

- Reviewing Scan Results on page 16

  Update Manager scans objects to determine how they comply with baselines and baseline groups that you attach.

- Staging Patches for Hosts on page 16

  If you want to apply patches to the hosts in your environment, you can stage the patches before remediation. Staging patches is an optional step.

- Remediating Selected vSphere Objects on page 17

  Remediation is the process in which Update Manager applies patches and upgrades to ESX/ESXi hosts, virtual machines, or virtual appliances after a scan is complete. Remediation helps ensure that machines and appliances are secured against known potential attacks and have greater reliability resulting from the latest fixes.

Configuring the Update Manager Patch Download Source

You can configure the Update Manager server to download patches either from the Internet or from a shared repository.

Configuring the Update Manager patch download source is an optional step.

If your deployment system is connected to the Internet, you can use it as a source for downloading patches to the vCenter Update Manager server. You can use the default settings and links for downloading patches. You can also add URL addresses to download third-party patches that are applicable only to ESX 4.x hosts.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the patches using the Update Manager Download Service. For more information, see Chapter 3, "Installing, Setting Up, and Using the Update Manager Download Service," on page 37.

For detailed descriptions of the procedures, see "Configuring Update Manager Patch Download Sources," on page 43.

Downloading Patches and Patch Metadata

Downloading patches and patch metadata is an automatic process. At regular configurable intervals, Update Manager contacts Shavlik and VMware to gather the latest information (metadata) about available patches.

VMware provides information about patches to ESX/ESXi, and Shavlik provides information for all major applications and operating systems. Information about all virtual machines and ESX/ESXi 4.0 patches is downloaded, regardless of whether the application or operating system to which the patch applies is currently in use in your environment. Patches for ESX/ESXi 3.5 and ESX 3.0.3 hosts are downloaded after you add an ESX 3.5, ESXi 3.5 or ESX 3.0.3 host to your environment.

With Update Manager 4.0, you can download information about ESX/ESXi 4.x patches from third-party vendor URL addresses.

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.

The first time a virtual machine is to be remediated, the applicable patches are downloaded to the Update Manager server and the patches are applied. The details of how a patch is applied, such as whether it is applied immediately or at a later time, are determined by the combination of what is possible under the conditions and what the user requests.

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

If Update Manager cannot conveniently download patches – for example, if it is deployed on an internal network segment that does not have reliable Internet access – VMware vCenter Update Manager Download Service downloads and stores patches on the machine on which it is installed so that Update Manager servers can use the patches later.

You can configure Update Manager to use an Internet proxy to download patch information and patches.

You can change the time interval in which Update Manager downloads patches, or you can download patches immediately. For a detailed description of the procedure, see "Configure Checking for Patches," on page 46.

Creating Baselines and Baseline Groups

Creating baselines and baseline groups is an optional step. Baselines can be upgrade or patch baselines. Baselines contain a collection of one or more patches, service packs and bug fixes, or upgrades. Baseline groups are assembled from existing baselines and might contain one upgrade baseline per type and one or more patch baselines or a combination of multiple patch baselines.

When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines and baseline groups to determine their level of compliance.

Update Manager includes four default patch baselines and four upgrade baselines. You cannot edit or delete the default baselines. You can use the default baselines, unless you want to create patch and upgrade baselines that meet the criteria you want. Baselines you create, as well as default baselines, can be combined in baseline groups. For more information about baselines and baseline groups, see "Using Baselines and Baseline Groups," on page 17 and Chapter 5, "Working with Baselines and Baseline Groups," on page 51.

Attaching Baselines and Baseline Groups to vSphere Objects

To use baselines and baseline groups, you must attach them to selected inventory objects such as virtual machines, virtual appliances, or hosts.

Although you can attach baselines and baseline groups to individual objects, it is more efficient to attach them to container objects, such as folders, hosts, clusters, and datacenters. Attaching a baseline to a container object transitively attaches the baseline to all objects in the container.

For a detailed description of the procedure, see "Attach Baselines and Baseline Groups to Objects," on page 61.

Scanning Selected vSphere Objects

Scanning is the process in which attributes of a set of hosts, virtual machines, or virtual appliances are evaluated against all patches and upgrades in the repository depending on the type of scan you select.

You can scan a host installation to determine whether the latest patches are applied, or you can scan a virtual machine to determine whether the latest patches are applied to its operating system.

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

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

Update Manager supports the following types of scan:

- Patch scan – You can perform patch scans on ESX 3.0.3 and later, ESX 3i version 3.5 and later, as well as virtual machines running Windows or Linux. You can scan for patches online as well as offline virtual machines and templates.
- Host upgrade scan – You can scan ESX 3.0.0 and later and ESX 3i version 3.5 and later for upgrading to ESX/ESXi 4.0.
- VMware Tools scan – You can scan virtual machines running Windows or Linux for the latest VMware Tools version. You can perform VMware Tools scans on online as well as offline virtual machines and templates. VMware recommends that you power on the virtual machine at least once before performing a VMware Tools scan.
- Virtual machine hardware upgrade scan – You can scan virtual machines running Windows or Linux for the latest virtual hardware supported on the host. You can perform virtual machine hardware upgrade scans on online as well as offline virtual machines and templates.
- Virtual appliance upgrade scan – You can scan powered on, VMware Studio registered Red Hat, Ubuntu, SUSE, and CentOS Linux virtual appliances.

You can initiate scans on container objects, such as datacenters, clusters, or folders, to scan all the ESX/ESXi hosts or virtual machines and appliances contained in the container object.

You can configure Update Manager to scan virtual machines, virtual appliances, and ESX/ESXi hosts against baselines and baseline groups by manually initiating or scheduling scans to generate compliance information. VMware recommends that you schedule scan tasks at a datacenter or vCenter Server system level to make sure that scans are up to date. For manual and scheduled scanning procedures, see Chapter 6, “Scanning vSphere Objects and Viewing Scan Results,” on page 67.

Reviewing Scan Results

Update Manager scans objects to determine how they comply with baselines and baseline groups that you attach.

You can review compliance by examining results for a single virtual machine, virtual appliance, template, or ESX/ESXi host or for a group of virtual machines and appliances or hosts.

The compliance information is displayed on the Update Manager tab. For more information about viewing compliance information, see “Viewing Scan Results and Compliance States for vSphere Objects,” on page 69.

Staging Patches for Hosts

If you want to apply patches to the hosts in your environment, you can stage the patches before remediation. Staging patches is an optional step.

Staging patches for ESX/ESXi 4.0 hosts allows you to download the patches from the Update Manager server to the ESX/ESXi hosts without applying the patches immediately. Staging patches speeds up the remediation process because the patches and updates are already available locally on the hosts. See “Stage Patches for ESX/ESXi Hosts,” on page 76.

Remediating Selected vSphere Objects

Remediation is the process in which Update Manager applies patches and upgrades to ESX/ESXi hosts, virtual machines, or virtual appliances after a scan is complete. Remediation helps ensure that machines and appliances are secured against known potential attacks and have greater reliability resulting from the latest fixes.

Update Manager allows you to upgrade ESX/ESXi hosts, virtual appliances, VMware Tools, and the virtual hardware of virtual machines to the latest version, with the option of rolling back the upgrade if it fails. You can also set up custom preupgrade and postupgrade scripts to run before and after an upgrade. Upgrades for ESX and ESXi hosts, virtual machines, and virtual appliances are managed through baselines and baseline groups.

You can remediate machines and appliances in much the same way that you can scan them. As with scanning, you cannot only remediate a single virtual machine or virtual appliance, but you can also initiate remediation on a folder of virtual machines and virtual appliances, vApp, a cluster, or a datacenter, or all objects in your virtual infrastructure. As with scanning, resource pools are the only vSphere object type that can never be remediated.

With Update Manager 4.0, you can perform orchestrated upgrades of hosts and virtual machines. Orchestrated upgrades allow you to upgrade all hosts in the inventory by using host upgrade baselines. You can use orchestrated upgrades to upgrade the virtual hardware and VMware Tools of virtual machines in the inventory at the same time, using baseline groups containing the following baselines:

- VM Hardware Upgrade to Match Host
- VMware Tools Upgrade to Match Host

Orchestrated upgrades can be performed at a cluster, folder or datacenter level.

Update Manager supports remediation for the following inventory objects:

- Powered on, suspended, or powered off virtual machines and templates for VMware Tools and virtual machine hardware upgrade, as well as patch installation.
- Powered on, VMware Studio registered Red Hat, Ubuntu, SUSE, and CentOS Linux virtual appliances for virtual appliance upgrade.
- ESX/ESXi hosts for patch and upgrade remediation.

Hosts are put into maintenance mode before remediation if the update requires it. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates the virtual machines to other hosts within a cluster before the host is put in maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for VMotion. For other containers or individual hosts that are not in a cluster, migration cannot be performed.

You can remediate the objects in your vSphere inventory by using either manual remediation or regularly scheduled remediation. For more information about manual and scheduled remediation, see Chapter 7, “Remediating vSphere Objects,” on page 73.

Using Baselines and Baseline Groups

Baselines contain a collection of one or more updates such as service packs, patches, upgrades, or bug fixes. Baseline groups are assembled from existing baselines. When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines to determine their level of compliance.

Administrators can create, edit, delete, attach, or detach baselines and baseline groups. For large organizations with different groups or divisions, each group can define its 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.

Baseline Types

Update Manager supports different types of baselines that you can use and apply when scanning and remediating the different objects in your inventory.

Update Manager provides upgrade or patch baselines.

Upgrade Baseline Defines which version a particular host, virtual hardware, VMware Tools, or virtual appliance should be.

Patch Baseline Defines a minimum level of updates that must be applied to a given host or virtual machine.

At regular intervals, Update Manager queries update repositories that vendors provide to find available patches. The server for the 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.

A patch baseline can be either dynamic or fixed.

Dynamic The contents of a dynamic baseline are 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.

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 known worm.

Update Manager Default Baselines

Update Manager includes default baselines that you can use to scan any virtual machine, virtual appliance, or host to determine whether they have all patches applied for the different categories or are upgraded to the latest version. The default baselines cannot be modified or deleted.

Critical VM Patches Checks virtual machines for compliance with all important Linux patches and all critical Windows patches.

Non-Critical VM Patches Checks virtual machines for compliance with all optional Linux patches and Windows patches.

Critical Host Patches Checks ESX/ESXi hosts for compliance with all critical patches.

Non-Critical Host Patches Checks ESX/ESXi hosts for compliance with all optional patches.

VMware Tools Upgrade to Match Host Checks virtual machines for compliance with the latest VMware Tools version on the host. Update Manager supports upgrading of VMware Tools for virtual machines on ESX/ESXi 4.0 hosts.

VM Hardware Upgrade to Match Host Checks the virtual hardware of a virtual machine for compliance with the latest version supported by the host. Update Manager supports upgrading to virtual hardware version 7.0 on ESX/ESXi 4.0 hosts.

VA Upgrade to Latest	Checks virtual appliance compliance with the latest virtual appliance version.
VA Upgrade to Latest Critical	Checks virtual appliance compliance with the latest critical virtual appliance version.

Baseline Groups

You can create baseline groups that contain both patch and upgrade baselines.

The set of baselines in a baseline group must be non-conflicting. A baseline group is also limited to a certain combination of patches and upgrades.

- Multiple patch baselines.
- One upgrade and multiple patch baselines.

  For example, one ESX/ESXi upgrade baseline and multiple ESX/ESXi patch baselines.
- Multiple upgrade baselines, but only one upgrade baseline per upgrade type (like VMware Tools, virtual machine hardware, virtual appliance, or host).

  For example, one VMware Tools Upgrade to Match Host baseline and one VA Upgrade to Latest baseline.
- Multiple upgrade baselines, but only one upgrade baseline per upgrade type and multiple patch baselines.

  For example, one VM Hardware Upgrade to Match Host baseline, one VA Upgrade to Latest Critical baseline, and one or more, patch baselines.

Baseline Attributes

Baselines have baseline attributes that you can use to identify the baseline type, what patches or upgrades are included in the baseline, and so on.

Table 1-1. Baseline Attributes

Attribute	Description
Baseline Name	Identifies the baseline. The name is established when a baseline is created and can be modified.
Content	For patch baselines, the content specifies the number of updates included in the baseline. Some updates, such as service packs, include many smaller patches that might have been previously distributed individually. The number of updates could indicate how long a scan and remediation might take to complete, but does not indicate the extent of the updates included in the baseline. For upgrade baselines, the content specifies the upgrade baseline details.
Component	Displays the type of baseline. Possible values are: Host Patches, VM Patches, VMware Tools, VM Hardware, and Host Upgrade.
Last Modified	Specifies the last time patches were added to or removed from the 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 ascertain whether expected changes were made to baselines.
Baseline Type	Identifies the type of baseline. Possible values include Dynamic and Fixed.

Update Manager Settings

You can configure Update Manager settings, such as scheduling updates and scans.

You can configure the following Update Manager settings:

- When to check for updated patch information.
- When to scan or remediate virtual machines, virtual appliances, and 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.
- How to handle failures to put hosts in maintenance mode.
- How to handle rebooting virtual appliances after remediation.

Setting Up, Installing, and Upgrading Update Manager 2

Before you install VMware vCenter Update Manager, you must set up an Oracle or Microsoft SQL Server database. If your deployment system is relatively small one containing up to 5 hosts and 50 virtual machines, you can use a SQL Server 2005 Express database, which you can install during the Update Manager installation.

You can install the Update Manager server component on the same computer as vCenter Server or on a different computer. After you install the Update Manager server component, to use Update Manager, you must install the Update Manager Client plug-in and enable it on the vSphere Client.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, you can install and register Update Manager instances with each vCenter Server system. You cannot use Update Manager for the vCenter Server systems in the vCenter Linked Mode with which no Update Manager instance is registered.

This chapter includes the following topics:

Update Manager Hardware Requirements

You can run Update Manager on any system that meets the minimum hardware requirements.

Minimum hardware requirements for Update Manager vary depending on how Update Manager is deployed. If the database is installed on the same machine as Update Manager, requirements for memory size and processor speed are higher. To ensure acceptable performance, make sure that you have the minimum requirements listed in Table 2-1.

Table 2-1. Minimum Hardware Requirements

Hardware	Requirements
Processor	Intel or AMD x86 processor with two or more logical cores, each with a speed of 2GHz
Network	10/100 Mbps
	For best performance, use a Gigabit connection between Update Manager and the ESX/ESXi hosts

Table 2-1. Minimum Hardware Requirements (Continued)

Hardware	Requirements
Memory	2GB RAM if Update Manager and vCenter Server are on different machines
	4GB RAM if Update Manager and vCenter Server are on the same machine

Update Manager uses a SQL Server or Oracle database. VMware recommends that you use a dedicated database for Update Manager, not a database shared with vCenter Server, and to back up the database periodically. Best practice is to have the database on the same computer as Update Manager or on a computer in the local network.

Depending on the size of your deployment system, Update Manager requires a minimum amount of free space per month for database usage. For more information about space requirements, see the *VMware vCenter Update Manager Sizing Estimator*.

Preparing the Update Manager Database

The Update Manager server and Update Manager Download Service require a database to store and organize server data. Update Manager supports Oracle, Microsoft SQL Server, and Microsoft SQL Server 2005 Express.

Before installing Update Manager, you must create a database instance and configure it to ensure that all Update Manager database tables are placed in it. If you are using Microsoft SQL Server 2005 Express, you install and configure the database when you install Update Manager. Microsoft SQL Server 2005 Express is used for small deployments of up to 5 hosts and 50 virtual machines.

To use a Microsoft SQL Server and Oracle databases, you must configure a system DSN and test it with ODBC.

The Update Manager database you use can be the same as the vCenter Server database, a separate database, or you can leverage existing database clusters. For best results in a large scale environment VMware recommends that you use a dedicated Update Manager database which is located on a different computer than the vCenter System database.

The VMware vCenter Update Manager server requires administrative credentials to connect to the database.

Before you begin the database setup, review the required database patches. If you do not prepare your database correctly, the Update Manager installer might display error or warning messages.

Supported Database Formats

Update Manager works with specific databases and requires certain drivers and patches.

Update Manager supports the database formats listed in Table 2-2. Database versions are 32-bit unless stated otherwise.

Table 2-2. Supported Database Formats

Database Type	Patch and Driver Requirements
SQL Server 2005 Standard Edition (SP1)	Use SQL Native Client driver for the client.
SQL Server 2005 Standard Edition (SP2 required)	Use SQL Native Client driver for the client.
SQL Server 2005 Standard Edition (SP3 required)	Use SQL Native Client driver for the client.
SQL Server 2008 Standard Edition	Use SQL Native Client driver for the client.
SQL Server 2005 Enterprise Edition (SP1)	Use SQL Native Client driver for the client.
SQL Server 2005 Enterprise Edition (SP2)	Use SQL Native Client driver for the client.
SQL Server 2005 Enterprise Edition (SP3)	Use SQL Native Client driver for the client.
SQL Server 2008 Enterprise Edition	Use SQL Native Client driver for the client.

Table 2-2. Supported Database Formats (Continued)

Database Type	Patch and Driver Requirements
SQL Server 2005 Enterprise Edition 64-bit (SP2)	Use SQL Native Client driver for the client.
SQL Server 2005 Enterprise Edition 64-bit (SP3)	Use SQL Native Client driver for the client.
SQL Server 2008 Enterprise Edition 64-bit	Use SQL Native Client driver for the client.
SQL Server 2005 Standard Edition 64-bit (SP2 required)	Use SQL Native Client driver for the client.
SQL Server 2005 Standard Edition 64-bit (SP3 required)	Use SQL Native Client driver for the client.
SQL Server 2008 Standard Edition 64-bit	Use SQL Native Client driver for the client.
SQL Server 2005 Express	Use SQL Native Client driver for the client.
Oracle 10g Standard Edition, Release 1 [10.1.0.3.0]	
Oracle 10g Enterprise Edition, Release 1 [10.1.0.3.0]	
Oracle 10g Standard Edition, Release 2 [10.2.0.3.0]	Supported with version 10.2.0.3.0 or later.
Oracle 10g Enterprise Edition, Release 2 [10.2.0.3.0]	Supported with version 10.2.0.3.0 or later.
Oracle 10g Enterprise Edition, Release 2 [10.2.0.3.0] 64-bit	Supported with version 10.2.0.3.0 or later.
Oracle 11g Standard Edition	
Oracle 11g Enterprise Edition	

Configure an Oracle Database

To use an Oracle database for Update Manager, you must first set up the database.

Procedure

1 Download Oracle 10g or Oracle 11g from the Oracle Web site, install it, and create a database (for example, `VUM`).

Make sure that the TNS Listener is up and running, and test the database service to be sure it is working.

2 Download Oracle ODBC from the Oracle Web site.

3 Install the corresponding Oracle ODBC driver through the Oracle Universal Installer.

IMPORTANT Oracle 10g requires Oracle 10.2.0.3 or later drivers.

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.

In this example, *ORACLE_BASE* is the root of the Oracle directory tree.

Configure an Oracle Connection to Work Locally

You can configure an Oracle connection to work locally with Update Manager.

Prerequisites

The ODBC Data Source you use must be a system DSN.

Procedure

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;
```

In this example, *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 these specific permissions to the user.

```
grant connect to user
grant resource to user
grant create any job to user
grant create view to user
grant create any sequence to user
grant create any table to user
grant lock any table to user
grant create procedure to user
grant create type to user
grant unlimited tablespace to user
# To ensure space limitation is not an issue
```

4 Create an ODBC connection to the database.

These are example settings.

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

Configure an Oracle Database to Work Remotely

You can configure your Oracle database to work with Update Manager remotely.

Before configuring a remote connection, first set up the database as described in “Configure an Oracle Database,” on page 23.

Prerequisites

The ODBC Data Source you use must be a system DSN.

Procedure

1 Install the Oracle client on the Update Manager server machine.

2 Use the Net Configuration Assistant tool to add the entry to connect to the managed host.

```
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 to which the client needs to connect.

3 (Optional) Edit the `tnsnames.ora` file located in *ORACLE_HOME*`\network\admin\`, as appropriate.

Here, *ORACLE_HOME* is located under `C:\`*ORACLE_BASE*, and it contains subdirectories for Oracle software executable and network files.

4 Create an ODBC connection to the database.

These are example settings.

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

Configure a Microsoft SQL Server Database

When you install Update Manager, you can establish an ODBC connection with a SQL Server database. Before using a Microsoft SQL Server database with Update Manager, you must create a new data source.

If you use SQL Server for Update Manager, do not use the master database.

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

Procedure

1 Create a SQL Server database by using Enterprise Manager on SQL Server.

You can define the default database for the database operator (DBO) user. The Update Manager SQL Server database that you create should be in the default dbo schema.

2 Create a SQL Server database user with DBO rights.

Make sure that 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.

Create a New Data Source (ODBC)

To prepare a Microsoft SQL Server database to work with Update Manager, you have to create a new data source (ODBC).

Procedure

1 On your Update Manager server system, select **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.

2 Click the **System DSN** tab.

3 Create or modify an ODBC system data source.

Option	Action
Create an ODBC system data source	a Click **Add**. b For SQL Server 2005 or SQL Server 2008, select **SQL Native Client**, and click **Finish**.
Modify an existing ODBC system data source	Double-click the ODBC system data source to modify.

4 In the Microsoft SQL Server DSN Configuration window, enter the necessary information and click **Next**.

Type the SQL Server machine name in the text field if you cannot find it in the drop-down menu.

a Type an ODBC DSN in the **Name** text field.

For example, type `VUM`.

b (Optional) Type an ODBC DSN description in the **Description** text field.

c Select the SQL Server name from the **Server** drop-down menu.

5 Configure the SQL Server Authentication page, and click **Next**.

- If you are using a local SQL Server, select **Integrated Windows authentication**.
- If you are using a remote SQL Server, select the appropriate SQL Server authentication method.

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

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

IMPORTANT Update Manager does not support Windows authentication of the database when the database is located on a different machine, because of local system account issues. Make sure that if the Update Manager database is located on a remote machine, the database and the system DSN use SQL Server authentication.

---

6 Select a database from the **Change the default database to** drop-down menu, specify the ANSI settings, and click **Next**.

7 Specify the language and translation settings, select a location for the log files, and click **Finish**.

What to do next

To test the data source, in the ODBC Microsoft SQL Server Setup window, click **Test Data Source**, and click **OK**. Ensure that the SQL Agent is running on your database server by double-clicking the SQL Server icon in the system tray.

This applies to SQL Server 2005 and SQL Server 2008 editions.

Identify the SQL Server Authentication Type

You can identify whether SQL Server is using Windows NT or SQL Server authentication.

Procedure

1 Open SQL Server Enterprise Manager.

2 Click the **Properties** tab.

3 Check the connection type.

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 vCenter Update Manager installation or upgrade.

No additional configuration is required.

Maintaining Your Update Manager Database

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

Maintaining your Update Manager database involves several tasks:

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

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

Installing and Uninstalling Update Manager

Update Manager can be installed on machines running Windows XP SP2, Windows XP SP3, Windows Server 2003, and Windows Server 2008.

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

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

Installing Update Manager

You can install the Update Manager server component on the same computer as vCenter Server or on a different computer. After you install the Update Manager server component, to use Update Manager, you must install the Update Manager Client plug-in and enable it on the vSphere Client.

To improve performance, especially in large scale environments, VMware recommends that you install the Update Manager server component on a different computer than the vCenter Server system.

During the Update Manager installation, you have to register the Update Manager server with the vCenter Server system and set it up to work correctly. Update Manager, vCenter Server and vSphere Client must be of compatible version. For more information about compatibility, see Table 2-3.

Create an Update Manager database unless you want to use SQL Server 2005 Express. For large scale environments, VMware recommends that you set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database.

To run and use Update Manager, you must use a local system account for the machine on which Update Manager is installed.

IMPORTANT Update Manager does not support Windows authentication of the database when the database is located on a different machine, because of local system account issues. Make sure that if the Update Manager database is located on a remote machine, the database and the system DSN use SQL Server authentication.

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 vCenter Server system that Update Manager will work with. Defaults are provided in some cases, but ensure that you have the correct information for networking:
  - IP address.
  - User name and password for the vCenter Server system.
  - Port numbers. In most cases, the default Web service ports (80 and 443) are used.
- Administrative credentials required to complete the installation:
  - User name for an account with sufficient privileges. This is often Administrator.
  - Password for the account used for the installation.
  - System DNS name, user name, and password for the database with which Update Manager will work.

VMware uses designated ports for communication. Additionally, Update Manager server connects to vCenter Server, ESX/ESXi hosts and Update Manager Client plug-in on designated ports. If a firewall exists between any of these elements and Windows firewall service is in use, the installer opens the ports during the installation. For custom firewalls, you must manually open the required ports.

VMware recommends that you provide a minimum of 20GB free space for Update Manager to store patch data.

Install Update Manager Server

The Update Manager installation requires a connection with a single vCenter Server instance. You can install Update Manager on the same computer on which vCenter Server is installed or on a different computer.

You can install Update Manager on machines running Windows XP SP2, Windows XP SP3, Windows Server 2003, or Windows Server 2008.

Before installing Update Manager, install vCenter Server. For more information about installing vCenter Server see the *vSphere Installation Guide*.

Prerequisites

Before installation, you must create and set up an Update Manager database, unless you are using SQL Server 2005 Express.

Make sure that 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. Although the **db_owner** role is required for upgrading, no SQL jobs are created as part of the Update Manager installation.

Procedure

1 Insert the Installer CD into the CD-ROM drive of the Windows server that is hosting the Update Manager server and select **vCenter Update Manager**.

  If you cannot launch the `autorun.exe` file, browse to locate the `UpdateManager` folder on the CD and run `VMware-UpdateManager.exe`.

2 Choose the language for the installer and click **OK**.

3 Review the Welcome page and click **Next**.

4 Accept the terms in the license agreement and click **Next**.

5 Enter information about vCenter Server and the administrative account that Update Manager server will use to connect to the vCenter Server and click **Next**.

6 Select the database options and click **Next**.

- If you do not have an existing database, select **Install a Microsoft SQL Server 2005 Express instance**. This database is suitable for small deployments of up to 5 hosts and 50 virtual machines.
- If you have a supported database, select **Use an existing supported database** and select a DSN from the drop-down menu.

7 (Optional) Enter the database user name and password for the system DSN and click **Next**.

If the DSN uses Windows NT authentication, leave the user name and password fields blank.

8 (Optional) If the system DSN you enter points to an existing Update Manager database with the same schema, select to leave your existing database or replace it with an empty one.

9 Specify how to identify your Update Manager instance on the network by selecting an IP or host name from the drop-down menu.

If the computer on which you install Update Manager has one NIC card, the Update Manager installer automatically detects the IP address. If the computer has multiple NIC cards, select the correct IP address or use a DNS name. The DNS name must be resolved from all hosts that this Update Manager will manage.

10 Enter the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

Configuring the proxy settings is optional.

11 (Optional) Provide information about the proxy server and port and whether the proxy should be authenticated and click **Next**.

12 Select the Update Manager installation and patch download directories and click **Next**.

If you do not want to use the default locations, click **Change** to browse to a different directory.

13 Click **Next**.

14 Click **Install** to begin the installation.

The Update Manager server component is installed.

What to do next

Install the vCenter Update Manager Client plug-in and enable it on a vSphere Client.

Install Update Manager Client

Update Manager functionality is an integral part of vCenter Server. To use Update Manager, you must install the Update Manager Client (the Update Manager user interface component), which is delivered as a plug-in for the vSphere Client.

You must install the Update Manager Client plug-in on any vSphere Client that you will use to manage Update Manager.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered.

2 Select **Plug-ins > Manage Plug-ins**.

3 In the Extension Manager window, click **Download and install** for the VMware vCenter Update Manager extension.

4 Complete the Update Manager Client installation, and click **Finish**.

5 Click **Close** to close the Extension Manager window after the Update Manager extension has a status of Enabled.

The plug-in icon is displayed on the vSphere Client Home page under Solutions and Applications.

Installing the Guest Agent

The VMware vCenter Update Manager Guest Agent facilitates Update Manager processes. For Linux and Windows operating systems, the Guest Agent is automatically installed the first time a patch remediation is scheduled or when a patch scan is initiated on a powered on virtual machine.

For best results, ensure that the latest version of the Guest Agent is installed in a virtual machine.

For Linux virtual machines, Update Manager checks for the presence of the Guest Agent whenever a Linux virtual machine in the vSphere inventory is powered on. Update Manager displays the discovery task as a `Detect Linux GuestAgent` task. If other Linux virtual machines are powered on, Update Manager starts the discovery again and the `Detect Linux GuestAgent` task is displayed in the Tasks pane. The task involves sending messages to each guest operating system and waiting for a response from the vCenter Update Manager Guest Agent. A timeout in the response means that no Guest Agent is installed. The process does not install the Guest Agent in the guest operating system.

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

The Guest Agent installation packages for Windows and Linux guests are located in the `\docroot\vci\guestAgent\` subfolder of the Update Manager installation directory. For example, if Update Manager is installed in `C:\Program Files\VMware\Infrastructure\Update Manager`, the Guest Agent installers are in `C:\Program Files\VMware\Infrastructure\Update Manager\docroot\vci\guestAgent\`.

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

Uninstalling Update Manager

Update Manager has a relatively small impact on computing resources such as disk space. Unless you are certain that you want to remove Update Manager, leave an existing installation in place for later use and disable the Update Manager Client plug-in.

The Update Manager server and plug-in can be uninstalled separately.

Uninstall Update Manager Server

You can uninstall the Update Manager server component.

Procedure

1 From the Windows Start menu, select **Settings > Control Panel > Add or Remove Programs**.

2 Select VMware vCenter Update Manager and click **Remove**.

The Update Manager server component is uninstalled from your system.

Uninstall Update Manager Client

If you uninstall Update Manager, you might also want to uninstall the Update Manager Client plug-in from the vSphere Client.

Procedure

1 From the Windows Start menu, select **Settings > Control Panel > Add or Remove Programs**.

2 Select VMware vCenter Update Manager Client and click **Remove**.

After you uninstall the Update Manager plug-in, the **Update Manager** icon is no longer available in the vSphere Client. Patch binaries and log data remain on the server where Update Manager was installed.

Upgrading Update Manager

You can upgrade Update Manager 1.0 and later to Update Manager 4.0.

During the Update Manager upgrade the `vci-integrity.xml` is overwritten. The following parameters that you modified in the `vci-integrity.xml` file are not lost during the upgrade.

- vCenter Server host and port settings – The IP of the computer on which vCenter Server is installed and the port which Update Manager server uses to connect to vCenter Server. These settings can be configured using the `<vpxdLocation>` tag.
- Patch store – The patch download location (the directory in which Update Manager stores patch metadata and patch binaries) that can be configured using the `<patchStore>` tag.
- Patch depot URL – The URL and port that Update Manager Client uses to contact the Update Manager server and to download patch data. The URL contains either the name or the IP of the computer on which Update Manager server is installed. These settings can be configured using the `<PatchDepotUrl>` tag. If there is no such setting, the ESX/ESXi hosts use the Update Manager server and Web Server port as a URL address to download host patches from the Update Manager server.
- Patch depot proxy URL – The proxy URL that the Update Manager server uses to download ESX host patches. If there is no value, Update Manager uses the proxy server in the proxy settings to download host patches. This setting can be configured using the `<PatchDepotProxyUrl>` tag.
- Proxy settings – The Update Manager proxy settings. These settings include the proxy port (`<proxyPort>`), proxy server (`<proxyServer>`), and usage of a proxy server (`<useProxyServer>`).
- Soap port – The SOAP port on which the Update Manager Client connects to the Update Manager server. This setting can be configured using the `<soapPort>` tag.
- Web Server port – The Web port on which ESX/ESXi hosts connect to the Update Manager server for host patch downloads. This setting can be configured using the `<webServerPort>` tag
- Patch metadata download URL – The URL from which Update Manager downloads patch metadata for hosts. This variable can be configured using the `<PatchMetadataDownloadUrl>` tag. During the upgrade to Update Manager 4.0, the value in the `<PatchMetadataDownloadUrl>` tag is moved to the `<ESX3xUpdateUrl>` tag.

For information on which versions are compatible, refer to Table 2-3. In this table U stands for Update. The compatible versions marked with an asterisk (*) passed preliminary tests for compatibility. This compatibility is experimental and not fully supported. The Update Manager server and Update Manager Client plug-in must be the same version.

Table 2-3. Compatibility Matrix

	VirtualCenter Server					vCenter Server	VI Client					vSphere Client
Update Manager	**2.5**	**2.5 U 1**	**2.5 U 2**	**2.5 U 3**	**2.5 U 4**	**4.0**	**2.5**	**2.5 U 1**	**2.5 U 2**	**2.5 U 3**	**2.5 U 4**	**4.0**
1.0	**Yes**	No	No	No	No	No	**Yes**	No	No	No	No	No
1.0 U 1	No	**Yes**	No	No	No	No	No	**Yes**	No	No	**Yes***	No
1.0 U 2	No	No	**Yes**	No	No	No	No	No	**Yes**	No	**Yes***	No
1.0 U 3	No	No	No	**Yes**	No	No	No	No	No	**Yes**	**Yes***	No
1.0 U 4	No	No	No	No	**Yes**	No	No	No	No	No	**Yes**	No
4.0	No	No	No	No	No	**Yes**	No	No	No	No	No	**Yes**

When you upgrade Update Manager, you cannot change the installation path and patch download location. To change these parameters, you must install a new version of Update Manager rather than upgrade.

You must upgrade the Update Manager database either before or during the Update Manager upgrade. You can select whether to keep your existing data in the database or to replace it during the upgrade of Update Manager.

Upgrade Update Manager Server

Upgrading Update Manager involves upgrading VirtualCenter Server to a compatible version.

Prerequisites

Before upgrading Update Manager, stop the Update Manager and vCenter Server services and back up the Update Manager database manually. The installer upgrades the database schema, making the database irreversibly incompatible with previous Update Manager versions.

Make sure that 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. Although the **db_owner** role is required for the upgrade, SQL jobs are not created as part of the Update Manager installation.

Procedure

1 Upgrade VirtualCenter Server to vCenter Server 4.0.

NOTE The vCenter Server installation wizard warns you that Update Manager is not compatible when vCenter Server is upgraded.

2 Insert the installer CD in the CD-ROM drive of the server on which Update Manager is installed.

3 Select a language and click **OK**.

4 In the upgrade warning message, click **OK**.

5 Review the Welcome page and click **Next**.

6 Accept the terms in the license agreement and click **Next**.

7 Enter the vCenter Server system credentials and click **Next**.

To keep the Update Manager's registration with the original vCenter Server system valid, keep the vCenter Server system IP and enter the credentials from the original installation.

8 Enter the database password for the VMware vCenter Update Manager database and click **Next**.

The database password is required only if the DSN does not use Windows authentication.

9 On the Database Upgrade page, select **Yes, I want to upgrade my Update Manager database**, and **I have taken a backup of the existing Update Manager database**, and click **Next**.

VMware recommends that you create a backup copy of the existing database before proceeding with the upgrade.

10 (Optional) If you upgrade the database to the latest schema before upgrading Update Manager, on the Database re-initialization warning page select to keep your existing database.

If you select to replace your existing database with an empty one, you lose all of your existing data.

11 Enter the Update Manager port settings, select whether you want to configure the proxy settings, and click **Next**.

Configure the proxy settings if you install Update Manager on a computer that has access to Internet.

12 (Optional) Provide information about the proxy server and port and whether the proxy should be authenticated and click **Next**.

13 Click **Install** to begin the upgrade.

What to do next

Upgrade the Update Manager Client plug-in.

Upgrade Update Manager Client

After you upgrade the Update Manager server, you must upgrade the Update Manager Client plug-in to the same version.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered.

2 Select **Plug-ins > Manage Plug-ins**.

3 In the Extension Manager window, click **Download and install** for the VMware vCenter Update Manager extension.

4 Complete the Update Manager Client installation, and click **Finish**.

5 Click **Close** to close the Extension Manager window after the Update Manager extension has a status of Enabled.

The plug-in icon is displayed on the vSphere Client Home page.

Update Manager Best Practices and Recommendations

You can install Update Manager on the same computer as the vCenter Server system or on a different computer. You can install the Update Manager Client plug-in on one computer or on different computers, depending on where the vSphere Client is installed.

The Update Manager server and plug-in must be the same version. Update Manager, vCenter Server, and vSphere Client must be of a compatible version. For more information about compatibility, see Table 2-3.

Update Manager has two deployment models:

- Internet-connected model - The Update Manager server has connectivity to the VMware patch repository and Shavlik and third-party patch repositories (for ESX 4.x hosts). Update Manager works with vCenter Server to scan and remediate the virtual machines, appliances, hosts, and templates.
- Air gap or semi-air gap model - Update Manager has no direct connection to the Internet and cannot download patch metadata. In this model, use the Update Manager Download Service (UMDS) to download patch metadata and patch binaries. You can configure the Update Manager server to use a shared repository as a patch datastore to scan and remediate the objects that you select from the inventory. For more information about using UMDS, see Chapter 3, “Installing, Setting Up, and Using the Update Manager Download Service,” on page 37.

It is not recommended to install Update Manager and vCenter Server on a virtual machine that is managed by the same vCenter Server system. Upon scanning and remediating, the virtual machine on which Update Manager and vCenter Server are installed can reboot and the whole deployment system will shut down.

Update Manager Deployment Configurations

You can install Update Manager on the same computer on which vCenter Server is installed or on a different computer.

The different configurations are listed in Table 2-4.

Table 2-4. Update Manager Deployment Configurations

Configuration	Virtual Machine 1	Virtual Machine 2	Virtual Machine 3	Virtual Machine 4	Virtual Machine 5
I	vCenter Server				
	vCenter Server database				
	Update Manager server				
	Update Manager database				
	vSphere Client				
	Update Manager Client plug-in				
II	vCenter Server	Update Manager server			
	vCenter Server database				
	Update Manager database				
	vSphere Client				
	Update Manager Client plug-in				
III	vCenter Server	vCenter Server database			
	Update Manager server				
	vSphere Client				
	Update Manager Client plug-in	Update Manager database			
IV	vCenter Server	Update Manager server	vSphere Client		
	vCenter Server database	Update Manager database	Update Manager Client plug-in		
V	vCenter Server	vCenter Server database	vSphere Client		
	Update Manager server	Update Manager database	Update Manager Client plug-in		
VI	vCenter Server	Update Manager server	vCenter Server database	Update Manager database	vSphere Client
					Update Manager Client plug-in

Update Manager Deployment Models and Their Usage

You can use the different Update Manager deployment models in different cases, depending on the size of your system.

There are several common Update Manager server host deployment models:

- vCenter Server and Update Manager server are installed on one host and their database instances are on the same host.

  This is the so called all-in-one system. It is most reliable when your system is relatively small (up to 20 hosts or 200 virtual machines).

- vCenter Server and Update Manager server are installed on one host and their database instances are on two separate hosts.

  This model is recommended for medium deployments, with more than 300 virtual machines or 30 hosts.

- vCenter Server and Update Manager server run on different hosts, each with its own database instance.

  This model is recommended for large deployments when the datacenters contain more than 1,000 virtual machines or 100 hosts.

Installing, Setting Up, and Using the Update Manager Download Service

3

VMware vCenter Update Manager Download Service (UMDS) is an optional module of Update Manager. UMDS downloads patch metadata and patch binaries that would not otherwise be available to the Update Manager server. To use UMDS, you must install it on a separate computer that has access to the Internet.

For security reasons and deployment restrictions, vSphere, including Update Manager, might be installed in an air-gap network. An air-gap network is a secured network that is disconnected from other local networks and the Internet. Update Manager requires access to patch information to function properly. Install UMDS on a computer that has Internet access to download patch binaries and patch metadata, and then export the downloads to a portable media drive so that they become accessible to the Update Manager server.

In an environment where Update Manager has access to the UMDS system, you can automate the export process and transfer files from UMDS to the Update Manager server by using a Web server. The Web server must be set up on the machine on which UMDS is installed.

UMDS can download patches for a variety of systems and versions:

- ESX 3i or higher, and ESX 3.5 or higher
- All Update Manager-supported versions of Windows virtual machines
- All Update Manager-supported versions of Linux virtual machines (patch metadata only)

You can also set up UMDS to download ESX/ESXi 4.x patches from third-party portals.

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

This chapter includes the following topics:

Installing the Update Manager Download Service

If Update Manager does not have access to the Internet, install the Update Manager Download Service to download patches.

The UMDS installer requires a database. Before installing UMDS, you must create a database instance and configure it to ensure that all tables are placed in it. You must configure a DSN and test the DSN from ODBC. If you are using Microsoft SQL Server 2005 Express, you install and configure the database when you install UMDS.

The amount of space required to store the patches on the server on which UMDS is installed varies based on the number of different operating systems and applications you intend to patch, as well as the number of years you intend to gather patches on this system. Allocate 50GB for each year of ESX patching, and 11GB for each virtual machine operating system and locale combination.

UMDS must be the same version as Update Manager. You can check whether the latest version of UMDS is installed from **Add or Remove Programs** in the Control Panel.

To use the latest UMDS version, you have to uninstall the older UMDS version before installing the new version. If you upgrade Update Manager, clean up the Download Service database and re-download the patch data in UMDS 4.0. If Update Manager is not upgraded yet, import the patches to the machine on which Update Manager is installed using the corresponding version of UMDS. You can import the patches using the `vmware-updateDownloadCli.exe` which is no longer supported in UMDS 4.0. Then upgrade Update Manager and reinstall UMDS to use its latest version.

Install the Update Manager Download Service

You can install the Update Manager Download Service if Update Manager does not have access to the Internet.

Prerequisites

Uninstall any previous version of the Update Manager Download Service. If a previous version of UMDS is already installed, the installation wizard displays an error message and the installation cannot proceed.

Procedure

1 Insert the VMware vCenter Update Manager installation CD into the CD-ROM drive of the Windows server that will host UMDS.

2 Browse to the `umds` folder on the CD and run `VMware-UMDS.exe`.

3 Select the language for the installation and click **OK**.

4 Review the Welcome page and click **Next**.

5 Accept the terms in the license agreement and click **Next**.

6 Select the database options and click **Next**.

- If you do not have an existing database, select **Install a Microsoft SQL Server 2005 Express instance (for small scale deployments)**. This database is suitable for deployments of up to 5 hosts and 50 virtual machines.
- If you have an existing database, select **Use an existing supported database** and select a system DSN.

7 Enter the Update Manager Download Service proxy settings and click **Next**.

8 Select the Update Manager Download Service installation and patch download directories and click **Next**.

If you do not want to use the default locations, click **Change** to browse to a different directory.

9 Click **Install** to begin the installation.

Set Up the Update Manager Download Service

You can specify which patches and updates to download with UMDS.

Procedure

1 Log in to the machine where the UMDS is installed, and open a Command Prompt window.

2 Change to the directory where the UMDS is installed.

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

3 Specify the updates to download.

- To set up a download of all ESX host updates, enter
  `vmware-umds --set-config --enable-host 1 --enable-win 0 --enable-lin 0`
- To set up a download of all Windows updates, enter
  `vmware-umds --set-config --enable-host 0 --enable-win 1 --enable-lin 0`
- To set up a download of all Linux updates, enter
  `vmware-umds --set-config --enable-host 0 --enable-win 0 --enable-lin 1`
- To set up a download of all available updates, enter
  `vmware-umds --set-config --enable-host 1 --enable-win 1 --enable-lin 1`

What to do next

Download the selected patches.

Download Patches Using the Update Manager Download Service

After you set up the UMDS, you can download the selected patches to the machine on which UMDS is installed.

Procedure

1 Log in to the machine where the UMDS is installed, and open a Command Prompt window.

2 Change to the directory where the UMDS is installed.

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

3 Download the selected patches using the command `vmware-umds --download`.

If you have already downloaded patches and want to download them again, include the start and end times to restrict the patches to download.

For example, if you want to re-download the patches downloaded in May 2008, enter:

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

The patches previously downloaded for the specified period are removed and downloaded again.

Download Third-Party Patches for ESX/ESXi Hosts

You can configure the Update Manager Download Service to connect to the Web sites of third-party vendors to download ESX/ESXi 4.x host patches.

Procedure

1 Log in to the machine on which the UMDS is installed.

2 Navigate to the UMDS installation directory and locate the file `downloadConfig.xml`.

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

3 Edit the file by adding the third-party URL addresses between the <HostConfig> and </HostConfig> tags.

```
<HostConfig>
<ESXThirdPartyUpdateUrl id="url2">http://third_party_URL</ESXThirdPartyUpdateUrl>
</HostConfig>
```

NOTE You can add a third-party URL address only for ESX/ESXi 4.x hosts.

You can add multiple third-party URL addresses by adding multiple third-party elements of the type <ESXThirdPartyUpdateUrl id="url2"> with different *id* attribute values.

4 Save and close the file.

5 Download the patches using the UMDS.

Export the Downloaded Updates

You can export downloaded patches to a specific location that serves as a shared repository for Update Manager. You can configure Update Manager to use the shared repository as a patch download source. The shared repository can also be hosted on a Web server.

Procedure

1 Log in to the machine where UMDS is installed and open a Command Prompt window.

2 Change to the directory where UMDS is installed.

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

3 Specify the export parameters.

```
vmware-umds -E --export-store repository_path
```

This command specifies the full path of the export directory.

If you are working in a semi-air-gap deployment, *repository_path* is the path to the folder on the Web server that serves as a shared repository. For example, if you are running an IIS Web server, the default path is C:\Inetpub\wwwroot\UMDS. For the Apache Web server, the default path is C:\Apache2\htdocs\UMDS.

If Update Manager is installed in an air-gap deployment, *repository_path* can be the path to a portable media drive. Export the downloads to the portable media drive to physically transfer the patches to the machine on which Update Manager is installed.

What to do next

Configure Update Manager to use a shared repository as a patch download source. The shared repository can be a folder on the machine on which Update Manager is installed, or on a Web server. For more information, see "Use a Shared Repository as a Patch Download Source," on page 44.

Configuring Update Manager 4

Update Manager runs with the default configuration properties if you have not modified them during the installation. You can modify the Update Manager settings later from the Update Manager Administrator's view.

You can modify the Update Manager settings only if you have the permissions to configure the Update Manager settings and service. These permissions must be assigned on the vCenter Server system with which Update Manager is registered. For more information about managing users, groups, roles and permissions, see the *vSphere Basic System Administration*.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have installed and registered more than one Update Manager instance, you can configure the settings for each Update Manager instance. Configuration properties you modify are applied only to the Update Manager instance you specify and are not propagated to the other instances in the group. You can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered from the navigation bar.

This chapter includes the following topics:

Configure Update Manager Network Connectivity Settings

After you install Update Manager and if you keep the default settings during the installation, the Update Manager Web server listens on 9084 TCP and 9087 TCP. The Update Manager SOAP server listens on 8084 TCP. You can modify the network settings to avoid conflicts with other programs installed on the same machine.

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

The network connectivity settings do not depend on where the Update Manager and vCenter Server are installed.

- Update Manager connects to vCenter Server on port 80.
- ESX/ESXi hosts connect to the Update Manager Web server listening on HTTP port 9084 for host patch downloads.
- Update Manager connects to ESX/ESXi hosts on port 902 for pushing the virtual machine patches and host upgrade files.
- The Update Manager Client plug-in connects to the Update Manager SOAP server listening on port 8084. It also connects to the Update Manager Web server on HTTP port 9087 for uploading the host upgrade files

The Update Manager network settings include the IP address or DNS name which the update utility on hosts use to retrieve the patch metadata and binaries from the Update Manager server (through HTTP). The IP is configured during the installation, but it can be later changed from the **IP address or host name for the patch store** drop-down menu on the Network Connectivity page.

IMPORTANT Use an IP address whenever possible to avoid any potential DNS resolution problems. If you must use a DNS name, instead of IP, ensure that the DNS name you specify can be resolved from all hosts managed by the Update Manager.

Update Manager 4.0 supports Internet Protocol version 6 (IPv6) environment for scanning and remediating ESX/ESXi 4.0 hosts. For virtual machine scanning and remediation IPv6 is not supported.

If you have ESX 3.x hosts in your inventory and the Update Manager is installed on a computer with IPv6, the scan and remediation operations on the hosts fail, because the hosts are not able to connect to the Update Manager server. VMware recommends that you install Update Manager on a computer with IPv4 enabled to scan and remediate ESX 3.x hosts.

Prerequisites

Before changing the network connectivity settings, check for conflicts with other port settings. Cancel or wait until any running remediation or scan tasks complete.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

   If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings click **Network Connectivity**.

4 Edit the network port settings.

Option	Description
SOAP port	Update Manager client uses this port to communicate with the Update Manager server. There are no limitations to the range of ports used, as long as there are no conflicts.
Server port (range: 9000–9100)	Listening port for the Web server that provides access to the plug-in client installer, and provides access to the patch depot for ESX/ESXi hosts. Update Manager automatically opens ESX/ESXi firewall ports in this range to allow outbound HTTP traffic to the patch store.
IP address or host name for the patch store	The IP address or name of the host in which patches are downloaded and stored. IMPORTANT Use an IP address whenever possible to avoid any potential DNS resolution problems. If you must use a DNS name, instead of IP, ensure that the DNS name you specify can be resolved from all hosts managed by the Update Manager.

5 Click **Apply**.

What to do next

Restart the Update Manager service for network changes to take effect.

Configuring Update Manager Patch Download Sources

You can configure the Update Manager server to download patches either from the Internet or from a shared repository.

If your deployment system is connected to the Internet, you can use it as a source for downloading patches to the vCenter Update Manager server. You can use the default settings and links for downloading patches. You can also add URL addresses to download third-party patches that are applicable only to ESX 4.x hosts.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the patches using the Update Manager Download Service. For more information, see Chapter 3, "Installing, Setting Up, and Using the Update Manager Download Service," on page 37.

Changing the patch download source from a shared repository to Internet, and the reverse, is a configurational change. Both options are mutually exclusive. You cannot download patches from the Internet and a shared repository at the same time. To download the new data, you must run the VMware vCenter Update Manager Update Download task by clicking the **Download Now** button.

If the VMware vCenter Update Manager Update Download task is running when you apply the new configurational settings, the task continues to use the old settings.

Configure Update Manager to Use the Internet as a Patch Download Source

If your deployment system is connected to the Internet, you can directly download Windows, Linux, and VMware ESX/ESXi patches.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings click **Patch Download Settings**.

4 In the Patch Download Sources pane, select **Direct connection to Internet**.

5 Select the patch type that you want to download.

You can select to download Windows, Linux and VMware (ESX 4.x and ESX 3.x) patches. You cannot specify the location of the default patches. You can only enable or disable downloading.

6 (Optional) Add an additional third-party patch download source for ESX 4.x hosts.

7 Click **Apply**.

8 Click **Download Now** to run the VMware vCenter Update Manager Update Download task and download patches immediately.

Add a Third-Party Patch Download Source for ESX 4.x Hosts

If you are using the Internet as a download source for patches, you can add a third-party URL address to download ESX 4.x patches.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings click **Patch Download Settings**.

4 In the Patch Download Sources pane, select **Direct connection to Internet**.

5 Click **Add Patch Source**.

6 In the Add Patch Source window, enter the URL and, optionally, a description.

Update Manager does not support authenticated URL addresses.

7 Click **Validate URL** to verify that the URL is accessible.

8 Click **OK**.

9 Click **Download Now** to run the VMware vCenter Update Manager Update Download task and to download the patches immediately.

The location is added to the list of Internet patch sources.

Use a Shared Repository as a Patch Download Source

You can configure Update Manager to use a shared repository as a patch download source.

Prerequisites

You must create the shared repository by using the Update Manager Download Service and host it on a Web server or a local disk.

For more information, see "Export the Downloaded Updates," on page 40.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings click **Patch Download Settings**.

4 In the Patch Download Sources pane, select **Use a shared repository**.

5 Enter the path or the URL to the shared repository.

For example: `C:\`*`repository_path`*`\`, `https://`*`hostname`*`/`*`repository_path`*`/`, or `http://`*`hostname`*`/`*`repository_path`*`/`

In these examples, *hostname* and *repository_path* are the path to the folder to which you have exported the patches. In a semi-air-gap environment, the folder can be on the machine on which Update Manager is installed, or on a Web server.

You can enter an HTTP or HTTPS address, or a location on the disk on which Update Manager is installed. HTTPS addresses are supported without any authentication.

IMPORTANT You cannot use folders located on a network drive as a shared repository. Update Manager does not download patch binaries and patch metadata from folders on a network share either in the Microsoft Windows Uniform Naming Convention form (such as `\\Computer_Name_or_Computer_IP\Shared`), or on a mapped network drive (for example, `Z:\`).

---

6 Click **Validate URL** to validate the path.

7 Click **Apply**.

8 Click **Download Now** to run the VMware vCenter Update Manager Update Download task and to download the patches immediately.

The shared repository is used as a patch download source.

Configure Update Manager Proxy Settings

You can configure Update Manager to download patches from the Internet using a proxy server.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 In the Proxy Settings pane, change the proxy information.

If the proxy requires authentication, select **Proxy requires authentication** and provide a user name and password.

4 (Optional) Click **Test Connection** at any time to test that you can connect to the Internet through the proxy.

5 Click **Apply**.

Configure Checking for Patches

Update Manager checks for patches at regular intervals. Generally, the default schedule settings are sufficient, but you can change the schedule if your environment requires more or less frequent checks.

If you have applications that receive frequent patches or must get patches as soon as they are released, you can decrease the duration between checks for patches. If you are not concerned about the latest patches and want to reduce network traffic, or if you cannot access the patch servers, you can increase the duration between checks for patches.

The default task to download patch metadata and patch binaries is the VMware vCenter Update Manager Update Download task. By modifying this task you configure checking for patches. You can modify the VMware vCenter Update Manager Update Download task from either the Scheduled Tasks window of the vSphere Client or the Configuration tab of the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

   If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings, click **Patch Download Schedule**.

4 Click **Edit Patch Downloads** on the upper-right.

   The Schedule Update Download wizard appears.

5 Specify a task name and, optionally, a description.

6 Specify the **Frequency**, **Interval** and **Start Time** of the update download, and click **Next**.

7 (Optional) Specify one or more email addresses where results of the update download process are sent when the new patches are downloaded, and click **Next**.

   You must configure mail settings for the vCenter Server system to enable this option.

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

The task runs according to the time you specified.

Take Snapshots Before Remediation

You can configure Update Manager to take snapshots of virtual machines before applying patches and upgrades. If the remediation fails, you can use the snapshot to return the virtual machine to the state before the remediation.

You can choose to keep these snapshots indefinitely or for a fixed period of time. Use the following guidelines when managing snapshots:

- Keeping snapshots indefinitely might consume a large amount of disk space and degrade virtual machine performance.
- Keeping no snapshots saves space, ensures best virtual machine performance, and might reduce the amount of time it takes to complete remediation, but limits the availability of a rollback.
- Keeping snapshots for a set period of time uses less disk space and offers a backup for a short time.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings, select **Virtual Machine Settings**.

4 To take snapshots of the virtual machines before remediating them, select **Snapshot the virtual machines before remediation to enable rollback**.

5 Configure snapshots to be kept indefinitely or for a fixed period of time.

6 Click **Apply**.

These settings become the default rollback option settings for virtual machines. You can specify different settings when you configure individual remediation tasks.

Configure How Update Manager Responds to Failure to Put Hosts in Maintenance Mode

Some ESX/ESXi host patches require that the host enters maintenance mode before they can be applied. Update Manager puts the ESX/ESXi hosts in maintenance mode before applying these patches. You can configure how Update Manager responds if entering maintenance mode fails.

Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates virtual machines to other ESX/ESXi hosts within a cluster before the host is put in maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for VMotion. For other containers or individual hosts that are not in a cluster, migration cannot be performed.

If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

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

If you do not have a VMware High Availability, VMware Distributed Resource Scheduler, or VMware VMotion setup, select **Power Off and Retry**.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings, click **ESX Host Settings**.

4 Select an option from the **Failure response** drop-down menu to determine how Update Manager responds if a host cannot be put in maintenance mode.

Option	Description
Fail Task	Log this failure in the Update Manager logs and take no further action.
Retry	Wait for the retry delay period and retry putting the host into maintenance mode as many times as you indicate in **Number of retries**.
Power Off Virtual Machines and Retry	Power off all virtual machines and retry putting the host into maintenance mode as many times as you indicate in **Number of retries** field. Virtual machines are shut down as though their power off button is used.
Suspend Virtual Machines and Retry	Suspend all running virtual machines and retry putting the host into maintenance mode as many times as indicated in **Number of retries** field.

5 If applicable, specify the retry delay and the number of retries.

6 Click **Apply**.

These settings become the default failure response settings. You can specify different settings when you configure individual remediation tasks.

Configure Smart Rebooting

Smart rebooting selectively reboots the virtual appliances and virtual machines in the vApp to maintain startup dependencies and possibly reboots the appliances that are not remediated. You can enable and disable smart rebooting of virtual appliances after remediation.

Smart rebooting is enabled by default. If you disable smart rebooting, the virtual appliances are restarted according to their individual remediation requirements and disregard any startup dependencies.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Configuration** tab.

3 Under Settings, click **vApp Settings**.

4 Deselect **Enable smart reboot after remediation** to disable smart rebooting.

Configure Update Manager Patch Download Location

When you install Update Manager, you can select the location for downloading patches. To change the location after installation, you must manually edit the `vci-integrity.xml` file.

Procedure

1 Log in to the Update Manager server as an administrator.

2 Stop the Update Manager service.

a Right-click **My Computer** and click **Manage**.

b In the left pane, expand **Services and Applications** and click **Services**.

c In the right pane, right-click the **VMware Update Manager Service** and click **Stop**.

3 Navigate to the Update Manager installation directory and locate the `vci-integrity.xml` file.

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

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

5 Edit the file by changing the following fields:

`<patchStore>`*`your_new_location`*`</patchStore>`

The default patch download location is: `C:\Documents and Settings\All Users\Application Data\VMware \VMware Update Manager\Data\`

The directory path must end with \.

6 Save the file in UTF-8 format, replacing the existing file.

7 Copy the contents from the old patchstore directory to the new folder.

What to do next

Restart the Update Manager service.

Configure Mail Sender Settings

You must configure the email address of the sender account to enable vCenter Server operations, such as sending email notifications as alarm actions.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered.

2 Select **Home > Administration > vCenter Server Settings** to display the vCenter Server Settings dialog box.

3 In the navigation pane, select **Mail**.

4 Enter the SMTP server information.

The SMTP server is the DNS name or IP address of the SMTP gateway to use for sending email messages.

5 Enter the sender account information.

The sender account is the email message address of the sender.

For example, **`mail_server@datacenter.com`**

6 Click **OK**.

Restart the Update Manager Service

In some cases, such as when you change the network connectivity settings, you must restart the Update Manager service.

Procedure

1 Log in as the administrator to the machine on which the Update Manager server component is installed.

2 Right-click **My Computer** and click **Manage**.

3 In the left pane of the Computer Management window, expand **Services and Applications** and click **Services**.

4 In the right pane, right-click **VMware Update Manager Service** and select **Restart**.

Wait until the service restarts on the local computer.

Run the VMware vCenter Update Manager Update Download Task

If you change the patch download source settings, you must run the VMware vCenter Update Manager Update Download task to download any new patches.

Procedure

1 In the vSphere Client, select **Home > Management > Scheduled Tasks** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to configure, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Right-click the **VMware vCenter Update Manager Update Download** task.

3 Select **Run**.

You can see the running task listed in the **Tasks** pane.

Working with Baselines and Baseline Groups

5

Baselines might be upgrade or patch baselines. Baselines contain a collection of one or more patches, service packs and bug fixes, or upgrades. Baseline groups are assembled from existing baselines and might contain one upgrade baseline per type and one or more patch baselines or a combination of multiple patch baselines. When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines and baseline groups to determine their level of compliance.

You must have baseline permissions to manage baselines and baseline groups. Permissions must be assigned on the vCenter Server system with which Update Manager is registered. For more information about managing users, groups, roles, and permissions, see *vSphere Basic System Administration*.

Update Manager includes four default dynamic patch baselines and four upgrade baselines. You cannot edit or delete default baselines.

Critical VM Patches	Checks virtual machines for compliance with all important Linux patches and all critical Windows patches.
Non-Critical VM Patches	Checks virtual machines for compliance with all optional Linux patches and Windows patches.
Critical Host Patches	Checks ESX/ESXi hosts for compliance with all critical patches.
Non-Critical Host Patches	Checks ESX/ESXi hosts for compliance with all optional patches.
VMware Tools Upgrade to Match Host	Checks virtual machines for compliance with the latest VMware Tools version on the host. Update Manager supports upgrading of VMware Tools for virtual machines on ESX/ESXi 4.0 hosts.
VM Hardware Upgrade to Match Host	Checks virtual hardware of a virtual machine for compliance with the latest version supported by the host. Update Manager supports upgrade to virtual machine hardware version 7.0 on ESX/ESXi 4.0 hosts.
VA Upgrade to Latest	Checks virtual appliance compliance with the latest virtual appliance version.
VA Upgrade to Latest Critical	Checks virtual appliance compliance with the latest critical virtual appliance version.

In the vSphere Client, default baselines are displayed on the Baselines and Groups tab of the Update Manager Client Administrator's view.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode and you have an Update Manager instance for each vCenter Server system in the group, the baselines and baseline groups you create and manage are applicable only to the inventory object managed by the vCenter Server system with which the selected Update Manager instance is registered. You cannot use an Update Manager instance with a vCenter Server system, with which the instance is not registered.

This chapter includes the following topics:

Creating Baselines

You can create patch and upgrade baselines to meet the needs of your specific deployment by using the New Baseline wizard. Creating additional, customized baselines allows patches to be grouped into logical sets.

You create baselines in the Update Manager Client Administrator's view.

Create a Patch Baseline

Patch baselines can be applied to either hosts or virtual machines. Depending on the patch criteria you select, patch baselines can be either dynamic or fixed.

Patch data in dynamic baselines change depending on the criteria you specify each time Update Manager downloads new patches. Fixed baselines contain only patches you select, regardless of new patch downloads.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have more than one Update Manager instance, patch baselines you create are not applicable to all inventory objects managed by other vCenter Server systems in the group. Baselines are specific for the Update Manager instance you select.

Create a Dynamic Patch Baseline

Dynamic baselines consist of a set of patches that meet certain criteria. The contents of a dynamic baseline varies as the available patches change. You can also exclude or add specific patches. This does not change with new patch downloads.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

   If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click **Create** in the upper-right corner.

   The New Baseline wizard opens.

3 Provide a name and description for the baseline.

4 Under Baseline Type, select either **Host Patch** or **VM Patch**, and click **Next**.

5 Select **Dynamic** as the type of baseline, and click **Next**.

6 On the Criteria page, enter criteria to define the patches to include, and then click **Next**.

Option	Description
Text contains	Restricts the patches displayed to those containing the text that you enter.
Product	Restricts the set of patches to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches to include.
Released Date	Specifies the range for the release dates of the patches.
Patch Vendor	Specifies which patch vendor to use.
Add or remove specific patches to/ from this baseline	Specifies whether to include or exclude patches from the patch set that results from the dynamic baseline criteria. You can select which patches to include or exclude later in the wizard.

The relationship between these fields is defined by the Boolean operator AND.

For example, when you enter text in the **Text contains** text box and select a product and severity option, the patches are restricted to the patches for the selected product containing the specified text and are of the specified severity level.

7 (Optional) On the Dynamic Patches to Exclude page, select one or more patches in the list and click the down arrow to exclude them from the baseline.

The Dynamic Patches to Exclude page appears only when you select **Add or remove specific patches to/ from this baseline** on the Criteria page.

8 (Optional) Click the **Filter** button to select specific patches to exclude from the baseline.

9 Click **Next**.

10 (Optional) On the Other Patches to Add page, select individual patches to include in the baseline and click the down arrow to move them into the Patches to Add list.

The Other Patches to Add page appears only when you select **Add or remove specific patches to/from this baseline** on the Criteria page. The patches you add to the dynamic baseline stay in the baseline regardless of the new downloaded patches.

11 (Optional) Click the **Filter** button to select specific patches to exclude from the baseline.

12 Click **Next**.

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

The dynamic patch baseline is displayed in the list of patch baselines.

Create a Fixed Patch Baseline

Fixed baselines consist of a specific set of patches that do not change as patch availability changes.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click **Create** in the upper-right corner.

The New Baseline wizard opens.

3 Provide a name and description for the baseline.

4 Under Baseline Type, select either **Host Patch** or **VM Patch**, and click **Next**.

5 Select **Fixed** for the type of baseline and click **Next**.

6 Select individual patches to include, and click the down arrow to add them to the Included Patches list.

7 (Optional) Filter the patches to find specific patches to include in the baseline.

8 Click **Next**.

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

The fixed patch baseline is displayed in the list of patch baselines.

Filter the Patches in the New Baseline Wizard

When you create a patch baseline, you can filter the patches to find specific patches to exclude or include in the baseline.

Procedure

1 If you are creating a fixed patch baseline, on Patches page of the New Baseline wizard, click **Filter**.

If you are creating a dynamic patch baseline, on the Patches to Exclude or Patches to Add page of the New Baseline wizard, click **Filter**.

2 On the Filter Patches page, enter the criteria to define the patches to include or exclude.

Option	Description
Text contains	Restricts the patches displayed to those containing the text that you enter.
Product	Restricts the set of patches to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches to include.
Released Date	Specifies the range for the release dates of the patches.
Patch Vendor	Specifies which patch vendor to use.

The relationship between these fields is defined by the Boolean operator AND.

3 Click **Find**.

The patches in the New Baseline wizard are filtered with the criteria you entered.

Create a Host Upgrade Baseline

You can create an ESX/ESXi host upgrade baseline by using the New Baseline wizard. Create a baseline with already uploaded ESX/ESXi upgrade files unless or use a specific ISO or ZIP file, which you can upload.

The files for ESX host upgrade are ISO files and the files for ESXi host upgrade are ZIP files.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have more than one Update Manager instance, host upgrade baselines you create are not applicable to the hosts managed by other vCenter Server systems in the group. Baselines are specific for the Update Manager instance you select.

Create a Host Upgrade Baseline Using Upgrade Files

You can create a host upgrade baseline with specific ESX/ESXi upgrade files that you upload.

IMPORTANT The COS VMDK Location and Post-Upgrade Options pages of the wizard appear only when you create an ESX or ESX/ESXi host upgrade baseline. When you create only an ESXi upgrade baseline, the pages are not available.

Prerequisites

Before creating a host upgrade baseline, obtain the upgrade files from the ESX/ESXi distribution at http://vmware.com/download/ or http://vmware.com/download/vi/.

For ESX 4.0, the upgrade file is named `esx-DVD-4.0.0-`*`build_number`*`.iso`. For ESXi, the upgrade file is named `ESXi-4.0.0-`*`build_number`*`-upgrade-release.zip`. Here *build_number* is the build number of the host version.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

   If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click **Create** in the upper-right corner.

   The New Baseline wizard opens.

3 Provide a name and description for the baseline.

4 Under Baseline Type, select **Host Upgrade** and click **Next**.

5 (Optional) On the Upgrade Version page, select **Upload Upgrade Files** from the drop-down menu.

   If you create a host upgrade baseline for the first time, the Upgrade Version page is not available and you have to browse for the ISO and ZIP files.

6 On the Select Upgrade Files page, browse to locate the `.iso` and `.zip` upgrade files from your file system and click **Next**.

   IMPORTANT The `.iso` and `.zip` files that you upload must be the same version if you want to upgrade ESX and ESXi hosts together using the same baseline. You can upload only one of the file types and remediate the respective hosts against this baseline.

   The upload process can take several minutes and must not be interrupted.

7 On the COS VMDK Location page, specify the location of the VMDK (virtual disk) to which to migrate the COS (console operating system) of the ESX host and then click **Next**.

Option	Description
(Recommended) Automatically select a datastore on the local host. The operation will fail if there is no local datastore with sufficient free space.	Selects a datastore attached directly to the host. Because the host requires the COS to boot, it must reside in a location that does not depend on the network so that you can reboot if the network goes down.
Select a specific datastore. The operation will fail if the specified datastore is not connected to the host or does not have sufficient free space.	Allows you to select the local or network datastore and to browse for the folder in which to place the COS VMDK. If Update Manager cannot access the datastore, the upgrade fails.

IMPORTANT The datastores cannot be shared between hosts.

Supported datastore drivers are SCSI, SAS, SAN, hardware iSCSI, drivers fronted by a RAID controller, IDE, and SATA.

8 (Optional) To not roll back the host, on the Post-Upgrade Options page, deselect **Try to reboot the host and roll back the upgrade in case of failure**.

9 (Optional) Specify a script to run after the upgrade completes and when the post-upgrade script times out, and then click **Next**.

Use the post-upgrade script to configure the ESX/ESXi host after the upgrade.

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

The host upgrade baseline is displayed in the list of upgrade baselines.

Create a Host Upgrade Baseline Using an Available Upgrade Version

You can create a host upgrade baseline by using an available upgrade version.

IMPORTANT The COS VMDK Location and Post-Upgrade Options pages of the wizard appear only when you create an ESX or ESX/ESXi host upgrade baseline. When you create only an ESXi upgrade baseline, the pages are not available.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click **Create** in the upper-right corner.

The New Baseline wizard opens.

3 Provide a name and description for the baseline.

4 Under Baseline Type, select **Host Upgrade** and click **Next**.

5 On the Upgrade Version page, specify the host upgrade version from the drop-down menu, and click **Next**.

Upgrades apply to ESX/ESXi hosts, unless the upgrade indicates ESX only or ESXi only. If the upgrade applies to ESX only or ESXi only, after you select the upgrade version, you can upload the missing file.

6 (Optional) Upload the missing upgrade file and click **Next**.

7 On the COS VMDK Location page, specify the location of the VMDK (virtual disk) to which to migrate the COS (console operating system) of the ESX host and then click **Next**.

Option	Description
(Recommended) Automatically select a datastore on the local host. The operation will fail if there is no local datastore with sufficient free space.	Selects a datastore attached directly to the host. Because the host requires the COS to boot, it must reside in a location that does not depend on the network so that you can reboot if the network goes down.
Select a specific datastore. The operation will fail if the specified datastore is not connected to the host or does not have sufficient free space.	Allows you to select the local or network datastore and to browse for the folder in which to place the COS VMDK. If Update Manager cannot access the datastore, the upgrade fails.

IMPORTANT The datastores cannot be shared between hosts.

Supported datastore drivers are SCSI, SAS, SAN, hardware iSCSI, drivers fronted by a RAID controller, IDE, and SATA.

8 (Optional) To not roll back the host, on the Post-Upgrade Options page, deselect **Try to reboot the host and roll back the upgrade in case of failure**.

9 (Optional) Specify a script to run after the upgrade completes and when the post-upgrade script times out, and then click **Next**.

Use the post-upgrade script to configure the ESX/ESXi host after the upgrade.

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

The host upgrade baseline is displayed in the list of upgrade baselines.

Create a Virtual Appliance Upgrade Baseline

A virtual appliance upgrade baseline consists of a set of user-defined rules.

If you add rules that conflict, the Update Manager displays an Upgrade Rule Conflict window so that you can resolve the conflicts.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click **Create** in the upper-right corner.

The New Baseline wizard opens.

3 Provide a name and description for the baseline.

4 Under Baseline Type, select **Virtual Appliance Upgrade**, and click **Next**.

5 Select **Vendor**, **Appliance**, and **Upgrade To** options from the respective drop-down menus, and click **Add Rule**.

6 (Optional) Add multiple rules.

   a On the Upgrade Options page of the New Baseline wizard, click **Add Multiple Rules**.

   b Select one or more vendors.

   c Select one or more appliances.

   d Select one **Upgrade To** option to apply to the selected appliances, and click **OK**.

   If you create multiple rules to apply to the same virtual appliance, only the first applicable rule in the list is applied.

7 (Optional) Resolve the conflicts within the rules you apply, if any.

   a In the Upgrade Rule Conflict window select to disregard or use the newly created rules, or to manually resolve the problem.

   b Click **OK**.

8 Click **Next**.

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

The virtual appliance upgrade baseline is displayed in the list of upgrade baselines.

Creating Baseline Groups

A baseline group consists of a set of nonconflicting baselines. Baseline groups allow you to scan and remediate objects against multiple baselines at once.

You can perform an orchestrated upgrade of the virtual machines by remediating the same folder or datacenter against a baseline group containing these baselines:

- VMware Tools Upgrade to Match Host
- VM Hardware Upgrade to Match Host

You create baseline groups using the New Baseline Group wizard. When creating a baseline group, use the following guidelines:

- You can include all patch baselines in one baseline group.
- You can have only one upgrade baseline per upgrade type (VMware Tools, virtual machine hardware, virtual appliance, or host) in a baseline group.

For example, you cannot have two different ESX host upgrade baselines or two different virtual appliance upgrade baselines.

You can create two types of baseline groups depending on the object type to which you want to apply them:

- Baseline groups for hosts
- Baseline groups for virtual machines and virtual appliances

Baseline groups you create are displayed on the **Baselines and Groups** tab of the Update Manager Client Administrator's view.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have more than one Update Manager instance, baseline groups you create are not applicable to all inventory objects managed by other vCenter Server systems in the group. Baseline groups are specific for the Update Manager instance that you select.

Create a Host Baseline Group

You can combine one upgrade baseline and multiple patch baselines or combine multiple patch baselines in a baseline group.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Baselines and Groups** tab.

3 Click **Create** above the Baseline Groups pane.

4 Enter a unique name for the baseline group.

5 Under Baseline Group Type, select **Host Baseline Group** and click **Next**.

6 Select a host upgrade baseline to include it in the baseline group.

7 (Optional) Create a new host upgrade baseline by clicking **Create new Host Upgrade Baseline** at the bottom of the Upgrades page and complete the New Baseline wizard.

8 Click **Next**.

9 Select the patch baselines that you want to include in the baseline group.

10 (Optional) Create a new patch baseline by clicking **Create new Host Patch Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

11 Click **Next**.

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

The host baseline group is displayed in the Baseline Groups pane.

Create a Virtual Machine and Virtual Appliance Baseline Group

You can combine upgrade and patch baselines in a virtual machine and virtual appliance baseline group. Upgrade baselines you include must be non-conflicting.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Baselines and Groups** tab.

3 Click **Create** above the Baseline Groups pane.

4 Enter a unique name for the baseline group.

5 Under Baseline Group Type, select **Virtual Machines and Virtual Appliances Baseline Group** and click **Next**.

6 For each type of upgrade (virtual appliance, virtual hardware, and VMware Tools), select one of the available upgrade baselines to include in the baseline group.

NOTE If only virtual appliances are remediated, the patches and upgrades for virtual machines are ignored. If only virtual machines are remediated, the upgrades for virtual appliances are ignored. If a folder contains both virtual machines and virtual appliances, only appropriate patches and upgrades are applied to each type of object.

7 (Optional) Create a new Virtual Appliance upgrade baseline, by clicking **Create New Virtual Appliance Upgrade Baseline** at the bottom of the Upgrades page, and complete the New Baseline wizard.

8 Click **Next**.

9 Select the patch baselines that you want to include in the baseline group.

10 (Optional) Create a new patch baseline, by clicking **Create New Virtual Machine Patch Baseline** at the bottom of the Patches page, and complete the New Baseline wizard.

11 Click **Next**.

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

The baseline group is displayed in the Baseline Groups pane.

Add Baselines to a Baseline Group

You can add a patch or upgrade baseline to an existing baseline group.

You add baselines to baseline groups from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click the **Hosts** or **VMs/VAs** button, depending on the type of baseline that you want to add.

3 From the Baseline Groups pane, select a baseline group.

4 In the upper Baselines pane, click the **Patch Baselines** or **Upgrade Baselines** tab.

5 Select a baseline from the list and click the down arrow.

The baseline is added to the selected baseline group.

Remove Baselines from a Baseline Group

You can remove a patch or upgrade baseline from an existing baseline group.

You remove baselines from baseline groups from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click the **Hosts** or **VMs/VAs** button, depending on the type of baseline that you want to remove.

3 From the Baseline Groups pane, select a baseline group.

4 Select a baseline from the list on the right and click the up arrow.

The baseline is removed from the selected baseline group.

Attach Baselines and Baseline Groups to Objects

To view compliance information and remediate objects in the inventory against specific baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects.

You attach baselines and baseline group to objects from the Update Manager Client Compliance view.

Although you can attach baselines and baseline groups to individual objects, it is more efficient to attach them to container objects, such as folders, hosts, clusters, and datacenters. Attaching a baseline to a container object transitively attaches the baseline to all objects in the container.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, you can attach baselines and baseline groups to objects managed by the vCenter Server system with which Update Manager is registered. Baselines and baseline groups you select to attach are specific for the Update Manager instance that is registered with the vCenter Server system.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object that you want to attach the baseline to.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select the object in the inventory, and click the **Update Manager** tab.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, the Update Manager tab is available only for the vCenter Server systems with which an Update Manager instance is registered.

4 Click **Attach** in the upper-right corner.

The Attach Baseline or Group window appears.

5 Select one or more baselines or baseline groups to attach to the object.

If you select one or more baseline groups, all baselines in the groups are selected. You cannot deselect individual baselines in a group.

6 (Optional) Click the **Create Baseline Group** or **Create Baseline** links to create a baseline group or a baseline and finish the respective wizard.

7 Click **Attach**.

The baselines and baseline groups that you selected to attach are displayed in the Attached Baselines and Attached Baseline Groups panes of the **Update Manager** tab.

Filter the Baselines and Baseline Groups Attached to an Object

You can filter the baselines and baseline groups attached to a specific inventory object and perform a search within the baselines and baseline groups.

You filter baselines and baseline groups attached to an object from the Update Manager Client Compliance view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory**.

2 Select the type of object that you want to view.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object from the inventory.

This object can be a single virtual machine, appliance, or host or a container object.

4 Click the **Update Manager** tab.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, the Update Manager tab is available only for the vCenter Server systems with which an Update Manager instance is registered.

5 Enter text in the **Name contains** text box above the Attached Baselines pane.

The baselines and baseline groups containing the text that you entered are listed in the respective panes. If the inventory object you select is a container object, the virtual machines, appliances or hosts in the Virtual Machines and Virtual Appliances or Hosts pane at the bottom of the tab are also filtered.

Detach Baselines and Baseline Groups from Objects

You can detach baselines and baseline groups from objects to which the baselines or baseline groups were directly attached. Because vSphere objects can have inherited properties, you might have to select the parent object where the baseline or baseline group is attached and remove it from the parent object.

You detach baselines and baseline group from objects from the Update Manager Client Compliance view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory**.

2 Select the type of object that you want to detach the baseline from.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select the object in the inventory, and click the **Update Manager** tab.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, the Update Manager tab is available only for the vCenter Server systems with which an Update Manager instance is registered.

4 Right-click the baseline or baseline group to remove and select **Detach Baseline** or **Detach Baseline Group**.

5 Select the inventory objects from which you want to detach the baseline or baseline group and click **Detach**.

The baseline or baseline group you detach is no longer listed in the Attached Baselines or Attached Baseline Groups pane.

Edit a Patch Baseline

You can edit an existing host or virtual machine patch baseline, but you cannot modify the default patch baselines.

You edit patch baselines from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, select the type of baseline to edit by clicking either the **Hosts** or **VMs/VAs** button and click the **Patch Baselines** tab.

3 Select a patch baseline and click **Edit** in the upper-right corner of the Baselines pane.

4 Edit the name and description of the baseline.

5 Change the patch options, criteria, and patches to include or exclude.

6 Click **OK** to save the changes.

Edit a Host Upgrade Baseline

You can change the name, description, and upgrade options of an existing host upgrade baseline. You cannot upload a different upgrade file.

You edit upgrade baselines from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, click the **Hosts** button, and click the **Upgrade Baselines** sub-tab.

3 Select an existing upgrade baseline and click **Edit** in the upper-right corner of the Baselines pane.

4 Edit the name and description of the baseline, and the appropriate options.

Option	Description
Upgrade Version	Click to change the upgrade version.
COS VMDK Location	Click to edit the specified location of the VMDK to which to migrate the COS of the ESX host.
Post-Upgrade Options	Click to edit the settings to reboot the host in case of failure and the post-upgrade usage settings.

5 Click **OK** to save the changes.

Edit a Virtual Appliance Upgrade Baseline

You can change the name, description and upgrade options of an existing upgrade baseline.

You edit upgrade baselines from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Baselines and Groups** tab, click the **VMs/VAs** button, and click the **Upgrade Baselines** sub-tab.

3 Select an existing upgrade baseline and click **Edit** in the upper-right corner of the Baselines pane.

4 Edit the appropriate options.

Option	Description
Baseline Name	Edit the baseline name and description.
Upgrade Options	Edit the existing rules or create new rules to apply.

5 Click **OK** to save the changes.

Edit a Baseline Group

You can change the name and type of an existing baseline group, as well as add or remove the included upgrade and patch baselines of a baseline group.

You edit baseline groups from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Select a baseline group from the Baseline Groups pane and click **Edit** above the pane.

3 Edit the name of the baseline group.

4 Change the included upgrade baselines (if any).

5 Change the included patch baselines (if any).

6 Review the Ready to Complete page and click **OK**.

Delete Baselines

You can delete baselines that you no longer need from Update Manager. Deleting a baseline detaches it from all the objects to which the baseline is attached.

You delete baselines from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, select the baselines to remove, and click **Delete**.

3 In the confirmation dialog box, click **Yes**.

The baseline is deleted.

Delete Baseline Groups

You can delete baseline groups that you no longer need from Update Manager. Deleting a baseline group detaches it from all the objects to which the baseline group is attached.

You delete baseline groups from the Update Manager Client Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 On the **Baselines and Groups** tab, select the baseline groups to remove, and click **Delete**.

3 In the confirmation dialog box, click **Yes**.

The baseline group is deleted.

Scanning vSphere Objects and Viewing Scan Results

6

Scanning is the process in which attributes of a set of hosts, virtual machines, or virtual appliances are evaluated against all patches and upgrades in the repository depending on the type of scan.

To generate compliance information and view scan results you must attach baselines and baseline groups to the objects you scan.

You can configure Update Manager to scan virtual machines, virtual appliances, and ESX/ESXi hosts by manually initiating or scheduling scans to generate compliance information.

You scan vSphere objects from the Update Manager Client Compliance view.

This chapter includes the following topics:

Manually Initiate a Scan of ESX/ESXi Hosts

You can manually initiate a scan of hosts in the vSphere inventory to execute the scan immediately. VMware recommends that you scan the vSphere objects against attached baselines and baseline groups.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.

2 Right-click a host, datacenter, or any container object and select **Scan for Updates**.

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

3 Select the types of updates to scan for.

The options are **Patches** and **Upgrades**.

4 Click **Scan**.

The selected inventory object is scanned against all patches in the Update Manager repository and available upgrades, depending on the option that you selected.

Manually Initiate a Scan of Virtual Machines and Virtual Appliances

To scan virtual machines and virtual appliances in the vSphere inventory immediately, you can manually initiate a scan against attached baselines and baseline groups.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > VMs and Templates** in the navigation bar.

2 Right-click a virtual machine, virtual appliance, a folder of virtual machines and appliances, or a datacenter, and select **Scan for Updates**.

All child objects of the object are also scanned. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes and the more accurate the compliance view is.

3 Select the types of updates to scan for.

The options are **Patches**, **Virtual Appliance upgrades**, **VM Hardware upgrades**, and **VMware Tools upgrades**.

4 Click **Scan**.

The virtual machines and appliances that you select are scanned against all patches in the Update Manager patch repository and available upgrades, depending on the options you select.

Schedule a Scan

You can configure the vSphere Client to run scans of objects in the inventory at specific times or at intervals that are convenient for you.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Management > Scheduled Tasks** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager to use to schedule a scan task by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click **New** in the toolbar to open the Select a Task to Schedule dialog box.

3 Select **Scan for Updates** and click **OK**.

4 Select the type of vSphere infrastructure object to scan, and click **Next**.

You can select to scan virtual machines and virtual appliances or ESX/ESXi hosts.

5 Using the inventory tree, select the inventory object to be scanned and click **Next**.

All child objects of the object that you select are also scanned.

6 Select the types of updates to scan for.

7 Enter a unique name and, optionally, a description for the scan.

8 Set the frequency of the task, time to start, and click **Next**.

9 (Optional) Specify one or more email addresses to send the results to and click **Next**.

You must configure mail settings for the vCenter Server system to enable this option.

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

The scan task is listed in the Scheduled Tasks window of the vSphere Client.

Viewing Scan Results and Compliance States for vSphere Objects

Update Manager scans objects to determine how they comply with baselines and baseline groups you attach. You can review compliance by examining results for a single virtual machine, virtual appliance, template, or ESX/ESXi host or for a group of virtual machines or hosts.

Supported groupings of virtual machines or ESX/ESXi hosts include virtual infrastructure container objects such as folders, clusters, and datacenters.

Baselines interact with virtual machines, virtual appliances, templates, and hosts in the following ways:

- If a user does not have permission to view an object, its contents, or a virtual machine, the results of those scans are not displayed. For more information about managing users, groups, roles and permissions, see *vSphere Basic System Administration*.
- Compliance with baselines and baseline groups is assessed at the time of viewing, so a brief pause might occur while information is gathered to make sure that all information is current.
- Objects must have an attached baseline or baseline group to be examined for compliance information.
- Only relevant compliance information is provided. For example, if a container has Windows XP and Windows Vista virtual machines, and patch baselines for Windows XP and Windows Vista patches are attached to this container, the relevant baselines are applied to each type of machine. Windows Vista virtual machines are assessed for compliance with Windows Vista baselines and the results are displayed. The same Windows Vista virtual machines are not assessed for compliance with Windows XP patches, and as a result, the status of their compliance is displayed as not applicable.
- Compliance status is displayed based on permissions. Users with permission to view a container, but not all the contents of the container are shown the aggregate compliance of all entities in the container. Individual accounts for compliance only appear as the user's permissions permit. To view the compliance status, the user must also have permission to view the baseline or software update compliance status for an object in the inventory. Users that have privileges to remediate patches and upgrades and to stage patches on a particular inventory entity, can view the compliance status of the same entity even if they do not have the view compliance permission. For more information about managing users, groups, roles and permissions, see *vSphere Basic System Administration*.
- When you scan a host against a fixed baseline that contains only patches that are made obsolete by newer ones, and the newer patches are already installed on the host, the compliance status of the old patches is not applicable. If the newer patches are not installed, the compliance status of the new patches is not compliant. You can install the noncompliant patches after you start a remediation process.

  When you scan a host against a fixed baseline that contains both obsolete and newer patches, the old patches are displayed as not compliant. Only the newer patches are installed after starting a remediation process.

View Compliance Information for vSphere Objects

You can review how virtual machines, virtual appliances, and hosts comply with baselines and baseline groups. You can view results for a single object or for a group of virtual machines, virtual appliances, or hosts.

Procedure

1. Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.
2. Select the type of object for which you want to view compliance information.

   For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object or a parent object from the inventory.

4 Click the **Update Manager** tab to view the scan results and compliance states.

Compliance View

Information about the compliance states of selected vSphere inventory objects is displayed in the Update Manager Client Compliance view.

The information is displayed in four panes.

Table 6-1. Update Manager Tab Panes

Pane	Description
Attached Baseline Groups	Displays the baseline groups attached to the selected object. If you select **All Groups and Independent Baselines** all attached baselines in the Attached Baselines pane are displayed. If you select an individual baseline group, only the baselines in that group are displayed in the Attached Baselines pane.
Attached Baselines	Displays the baselines attached to the selected object and included in the selected baseline group.
Compliance	Contains a compliance graph that changes dynamically depending on the inventory object, baseline groups and baselines that you select. The graph represents the percentage distribution of the virtual machines, appliances or hosts in a selected container object that are in a particular compliance state against selected baselines. If you select an individual host, virtual machine or appliance, the color of the graph is solid and represents a single compliance state. Above the graph, the following compliance states are displayed: ■ All Applicable – Total number of inventory objects for which compliance is being calculated. This number is the total of objects in the selected container inventory object minus the objects for which the selected baselines do not apply. The applicability of a baseline is determined depending on whether the baseline is directly attached to the virtual machine, appliance or host or is attached to a container object. Applicability also depends on whether the baseline contains patches or upgrades that can be applied to the selected object. ■ Non-Compliant – Number of virtual machines, appliances, or hosts in the selected container object that are not compliant with at least one patch or upgrade in the selected baseline. ■ Incompatible – Number of virtual machines, appliances or hosts in the selected container object that cannot be remediated against the selected baselines and baseline groups. Incompatible state requires more attention and investigation for determining the reason for incompatibility. To obtain more information about the incompatibility, view patch or upgrade details. ■ Unknown – Number of virtual machines, appliances, or hosts in the selected container object that are not scanned against at least one of the patches or upgrades in the selected baselines and baseline groups. ■ Compliant – Number of compliant virtual machines, appliances, or hosts in the selected container object.
Virtual Machines and Virtual Appliances or Hosts	Displays a table of the virtual machines and virtual appliances or hosts that meet the selections from the Attached Baseline Groups, Attached Baselines and Compliance panes.

Review Baseline or Baseline Group Compliance with vSphere Objects

Scan results provide information on the degree of compliance with attached baselines and baseline groups. You can view information on individual vSphere objects or all objects in a container and receive detailed information about the patches and upgrades included in a baseline or a baseline group.

The following information is included:

- When the last scan was completed at this level.
- The total number of compliant and noncompliant patches.
- For each baseline or baseline group, the number of virtual machines, appliances, or hosts that are applicable, noncompliant, incompatible, unknown, or compliant.
- For each baseline or baseline group, the number of patches that are applicable to particular virtual machines or hosts.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of object for which you want to view scan results.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object from the inventory.

This object can be a single virtual machine, virtual appliance, host, or a container object.

4 Click the **Update Manager** tab.

5 Select a baseline group or baseline or select **All Groups and Independent Baselines**.

6 In the Compliance pane, select a compliance status from the list (All Applicable, Non-Compliant, Incompatible, Unknown and Compliant).

The virtual machine, virtual appliance, or host in the compliance state that you select appear in the Virtual Machines and Virtual Appliances or Hosts pane at the bottom of the **Update Manager** tab.

7 Click the link indicating the number of patches that are in compliance, are not in compliance, or are in an unknown state in the Patches column.

The Patch Details window appears.

8 Click the link in the Upgrades column in the Virtual Machines and Virtual Appliances or Hosts pane at the bottom of the **Update Manager** tab. The link indicates the number of upgrades in the selected compliance state.

The Upgrade Details window appears.

Viewing Patch Details

The Patch Details window displays a table of the patches ordered according to their compliance status with the selected virtual machine or host.

The compliance summary above the table represents the number of the applicable patches, missing patches (noncompliant), compliant patches, staged patches, and so on. If there are patches in incompatible state, the compliance summary displays a detailed view of the incompatible patches. Incompatibility might be a result of a conflict, missing update packages, and so on.

You can obtain complete information about a patch by double clicking a selected patch in the Patch Details window.

The columns in the patch details window table and their descriptions are listed in Table 6-2.

Table 6-2. Patch Details Window

Option	Description
Update Name	Name of the update.
Compliance	Compliance state of the update. The state might be Missing (Non-compliant), Not Applicable, Unknown, Installed (compliant), and so on.
Severity	Severity of the update. For hosts the severity status might be Critical, General, Security, and so on. For virtual machines the severity might be Critical, Important, Moderate, and so on.
Impact	What is the action you must take to apply the update. This action might include a reboot of the system or entering maintenance mode (for hosts).

Viewing Upgrade Details

The Upgrade Details window presents information about a specific upgrade you select.

The information represented in the Upgrade Details window is displayed in Table 6-3.

Table 6-3. Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	Type of the baseline. The type can be host upgrade, virtual machine upgrade, or virtual appliance upgrade.
Baseline Description	The description of the baseline, if any. If the baseline has no description, it is not displayed.
Compliance State	The compliance state is displayed for host upgrades only and represents the compliance state of the host against the upgrade baseline.
Details	Details specific to the type of baseline. For example, for the VM Hardware Upgrade to Match Host baseline, the details include the current hardware version and the target hardware version of the virtual machine.

Remediating vSphere Objects 7

You can remediate virtual machines, virtual appliances, and hosts using either user-initiated remediation or regularly scheduled remediation.

You can remediate virtual machines and appliances together.

If your vCenter Server is a part of a connected group in vCenter Linked Mode, you can remediate only the inventory objects managed by the vCenter Server system with which Update Manager is registered.

This chapter includes the following topics:

Orchestrated Upgrades of Hosts and Virtual Machines

You can perform orchestrated upgrades of the hosts or virtual machines in your vSphere inventory.

Orchestrated upgrades allow you to upgrade all hosts in the inventory using a single host upgrade baseline that is attached to a container object in the vSphere inventory. You can use orchestrated upgrade to upgrade the virtual machine hardware and VMware Tools of the virtual machines in the vSphere inventory at the same time, using baseline groups containing these baselines:

- VM Hardware Upgrade to Match Host
- VMware Tools Upgrade to Match Host

You can perform an orchestrated upgrade at the cluster, folder, datacenter, or individual entity level.

Upgrading the virtual hardware of the virtual machines exposes new devices and capabilities to the guest operating systems. You must upgrade VMware Tools before upgrading the virtual hardware version so that all required drivers are updated in the guest. Upgrading the virtual hardware of the virtual machines is not possible if VMware Tools is not installed, out of date, or managed by third-party vendors.

When you upgrade virtual machines against a baseline group containing the VM Hardware Upgrade to Match Host baseline and the VMware Tools Upgrade to Match Host baseline, Update Manager sequences the upgrade operations in the correct order and VMware Tools is upgraded first.

During the upgrade of VMware Tools, the virtual machines must be powered on. If a virtual machine is in a powered off or suspended state before remediation, Update Manager powers on the machine. After the upgrade completes, Update Manager reboots the machine and restores the original power state of the virtual machine.

During the virtual hardware upgrade, the virtual machines must be shut down. After the remediation completes, Update Manager restores the original power state of the virtual machines. If a virtual machine is powered on, Update Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

Remediation of Hosts

Host remediation is executed in different ways depending on the types of baselines you attach and whether the host is in a cluster or not.

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

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

When you remediate hosts against baseline groups containing upgrade and patch baselines, the upgrade is performed first. Host upgrade in a high-latency network in which Update Manager and the hosts are at different locations might take a few hours because the upgrade file is copied from the Update Manager server repository to the host before the upgrade. During this time, the host stays in maintenance mode.

The host upgrade remediation of ESX/ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

NOTE When you upgrade a host, no third-party management agents or software applications are migrated to the ESX 4.0/ESXi 4.0 host.

Update Manager handles host patches in the following ways:

- If a patch in a baseline requires the installation of another patch, Update Manager detects the prerequisite in the depot and installs it together with the selected patch.
- If a patch is in conflict with other patches that are installed on the host, the conflicting patch might not be installed or staged. However, if another patch in the baseline resolves the conflicts, the conflicting patch is installed. For example, if a baseline contains patch A and patch C, and patch A conflicts with patch B, which is already installed on the host, but patch C obsoletes patch B, and patch C is not in conflict with patch A, the remediation process installs patches A and C.
- When multiple versions of the same patch are selected, Update Manager installs the newest version and skips the older versions.

Remediation Specifics of ESX Hosts

When remediating ESX hosts, Update Manager handles patches in different ways depending on the ESX host version.

In the ESX 3.5 patch remediation process, cumulative rollups and updates are considered patches. If a rollup contains two patches installed on the host, the state of the host is noncompliant against the rollup until the rollup itself is installed on the host.

In the ESX 4.0 patch remediation process, Update Manager operates with vSphere Installation Bundles (`*.vib` files). A bundle is the smallest installable unit on an ESX 4.x host. A bulletin defines a specific fix for a host, a rollup that aggregates previous fixes, or an update release. When a host is compliant with all bundles in a bulletin, it is compliant with the vSphere bulletin that contains the bundles.

If a bundle depends on other bundles, Update Manager installs the necessary prerequisite bundles during the remediation process. As a result, the number of patches after staging and remediation might be greater than the number of patches that you selected for staging or remediation. For example, when you stage or remediate a host against a baseline consisting of a bulletin that contains bundle A, and bundle A requires bundle B (bundle B is not part of the bulletin), both bundles get staged or installed. In such a case, the patch count for staged or installed patches is two, not one.

Before the ESX host upgrade remediation, Update Manager runs a script on the host to check whether the host can be upgraded. If the host can be upgraded, Update Manager copies the ISO file to the host. The ISO file contains the bits that are to be installed as well as a Linux `kernel` and `ramdisk`, which serve as the installer environment. The host reboots into the installer, and the installer creates a service console virtual disk (VMDK) to install the packages into the console VMDK. The host is rebooted, upgraded to ESX 4.0, and reconnected to the vCenter Server system. If the upgrade fails, you can roll back to the previous version.

Remediation Specifics of ESXi Hosts

For ESXi hosts, updates are all-inclusive. The most recent update contains the patches from all previous releases.

The ESXi image on the host maintains two copies. The first copy is in the active boot and the second one is the standby boot. When you patch an ESXi host, Update Manager creates a new image based on the content of the active boot and the content of the patch. The new ESXi image is then located in the standby boot and Update Manager designates the active boot as the standby boot and reboots the host. When the ESXi host reboots, the active boot contains the patched image and the standby boot contains the previous version of the ESXi host image.

Using Update Manager you can apply third-party patches to ESXi hosts only if the third-party software is already installed on the ESXi host.

When you upgrade an ESXi host, Update Manager replaces the backup image of the host with the new image and replaces the active boot and the standby boot. During the upgrade the layout of the disk hosting the boots changes. The total disk space for an ESXi host remains 1GB, but the disk partition layout within that 1GB disk space changes to accommodate the new size of the boots where the ESXi 4.0 images will be stored.

For purposes of rollback, the term update refers to all ESXi patches, updates, and upgrades. Each time you update an ESXi host, a copy of the previous ESXi build is saved on your host.

If an update fails and the ESXi 4.0 host cannot boot from the new build, the host reverts to booting from the original boot build. ESXi permits only one level of rollback. Only one previous build can be saved at a time. In effect, each ESXi 4.0 host stores up to two builds, one boot build and one standby build.

Remediation of Templates

Templates are a type of virtual machine, so they can be remediated.

Take snapshots of templates before remediation, especially if the templates are sealed. A template that is sealed is stopped before the 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 to allow 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 an error occurs, a template might not be returned to its sealed state. For example, if Update Manager loses its connection with the vCenter Server system during remediation, the template cannot be returned to its sealed state. Creating a snapshot before remediation provides an easy recovery from such issues.

Rolling Back to a Previous Version

If remediation fails, you can roll back virtual machines and appliances to their previous state.

You can configure Update Manager to take snapshots of virtual machines and appliances and keep them indefinitely or for a specific period of time. After the remediation completes, you can validate the remediation and delete the snapshots if they are not needed.

By default, when you remediate a host against an upgrade baseline, the host rolls back if the upgrade fails.

Rebooting Virtual Machines After Patch Remediation

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

Users can postpone the shutdown for up to 60 minutes. After the specified time elapses, a final timer before shutdown appears.

Stage Patches for ESX/ESXi Hosts

Staging patches for ESX/ESXi hosts allows you to download the patches from the Update Manager server to the ESX/ESXi hosts, without applying the patches immediately. Staging patches speeds up the remediation process because the patches are already available locally on the hosts.

Staging patches does not require that the hosts enter maintenance mode. Staging patches whose installation requires that a host enters maintenance mode, can significantly reduce the downtime during remediation.

Patches cannot be staged if they are obsoleted by patches in the baselines or baseline groups for the same stage operation. Update Manager stages only patches that it can install in a subsequent remediation process, based on the present scan results of the host. If a patch is obsoleted by patches in the same selected patch set, the obsoleted patch is not staged.

If a patch is in conflict with the patches in the Update Manager server repository and is not in conflict with the host, after a scan, Update Manager reports this patch as a conflicting one. You can stage the patch to the host and after the stage operation, Update Manager reports this patch as staged.

During the stage operation, Update Manager performs pre- and post-scan operations, and the compliance state of the baseline is updated.

IMPORTANT Staging patches is supported for ESX/ESXi 4.0 hosts.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.

2 Right click a datacenter, cluster, or host, and select **Stage Patches**.

3 Select the patch baselines to stage.

4 Select the hosts where patches will be applied and click **Next**.

If you select to stage patches to a single host, it is selected by default.

5 (Optional) Deselect the patches to exclude from the stage operation.

6 (Optional) To search within the list of patches, enter text in the text box in the upper-right corner.

7 Click **Next**.

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

The number of the staged patches for the specific host is displayed in the Patches column in the Virtual Machines and Virtual Appliances or Hosts pane of the Update Manager tab.

All staged patches, whether installed or not during a remediation, are deleted from the host after remediation completes.

Manually Remediating Hosts, Virtual Machines and Virtual Appliances

You can manually remediate ESX/ESXi hosts, virtual machines and virtual appliances at any time.

By remediating a container object from the inventory, you can perform an orchestrated upgrade of all the hosts or virtual machines in the selected container object.

You can perform an orchestrated upgrade of hosts by remediating a cluster or a datacenter against a single baseline. You can perform an orchestrated upgrade of virtual machines by remediating the same datacenter against a baseline group containing these baselines:

- VMware Tools Upgrade to Match Host
- VM Hardware Upgrade to Match Host

Manually Remediate Hosts Against Upgrade and Patch Baselines

You can remediate hosts against attached upgrade and patch baselines, or baseline groups that contain multiple patch baselines or an upgrade baseline and multiple patch baselines.

Prerequisites

To remediate a host against a baseline group containing both upgrade and patch baselines, attach the baseline group to the host.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory > Hosts and Clusters** in the navigation bar.

2 Right-click the object you want to remediate, and select **Remediate**.

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

By selecting to upgrade a container object against an upgrade baseline, or a baseline group containing an upgrade baseline, you perform an orchestrated upgrade of the hosts in the container object.

3 Select the baselines and baseline group to apply.

4 (Optional) Select the hosts that you want to remediate and click **Next**.

If you remediate a single host, it is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

6 (Optional) On the ESX 4.0 Upgrade page, click the links of the settings that you want to edit.

Option	Description
COS VMDK location (Classic ESX only)	In the ESX 4.0 COS VMDK Location window, specify the datastore location for the VMDK to migrate the COS of the ESX host. IMPORTANT The datastores cannot be shared between hosts.
Rollback on failure (Classic ESX only)	In the ESX 4.0 Post Upgrade Options window, specify whether to disable rollback in case of failure.
Post-Upgrade script (Classic ESX only)	In the ESX 4.0 Post Upgrade Options window, specify a post-upgrade script usage after the upgrade completes and when the post-upgrade script times out.

The ESX 4.0 Upgrade page appears in the Remediate wizard only when you remediate against an ESX upgrade baseline or your baseline group contains an ESX upgrade baseline.

7 Click **Next**.

8 (Optional) Deselect specific patches to exclude them from the remediation process and click **Next**.

9 (Optional) Review the list of patches to be excluded and click **Next**.

10 On the Host Remediation Options page, enter a unique name for the task and optionally a description.

11 Select **Immediately** to begin the process right after you complete the wizard.

12 Specify the failure response for the remediation process from the **Failure response** drop-down menu, the delay in the retry and the number of retries, if applicable, and click **Next**.

Option	Description
Fail Task	Log this failure in the Update Manager logs and take no further action.
Retry	Wait for the retry delay period and retry putting the host into maintenance mode as many times as you indicate in **Number of retries**.
Power Off Virtual Machines and Retry	Power off all virtual machines and retry putting the host into maintenance mode as many times as you indicate in **Number of retries** field. Virtual machines are shut down as though their power off button is used.
Suspend Virtual Machines and Retry	Suspend all running virtual machines and retry putting the host into maintenance mode as many times as indicated in **Number of retries** field.

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

Manually Remediate Virtual Machines and Virtual Appliances

You can manually remediate virtual machines and virtual appliances at the same time.

To remediate virtual machines and virtual appliances together, they must be in one container, such as a folder, vApp, or a datacenter. You must then attach a baseline group or a set of individual virtual appliance or virtual machine baselines to the container. If you attach a baseline group, it can contain both virtual machine and virtual appliance baselines. The virtual machine baselines apply to virtual machines only, and the virtual appliance baselines apply to virtual appliances only.

NOTE You can remediate powered on Red Hat, Ubuntu, SUSE, and CentOS Linux virtual appliances only.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** and select **VMs and Templates**.

2 Right-click the object you want to remediate, and select **Remediate**.

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

By selecting to upgrade a container object against an upgrade baseline group containing the VMware Tools Upgrade to Match Host baseline and the VM Hardware Upgrade to Match Host baseline, you perform an orchestrated upgrade of the virtual machines in the container object.

3 Select the baselines and baseline group to apply.

4 Select the virtual machines and appliances to remediate and click **Next**.

5 (Optional) In the Patches page, deselect the check boxes for patches that you want to exclude from the remediation process and click **Next**.

The Patches page appears only if you remediate against patch baselines or a baseline group containing patch baselines.

6 (Optional) Review the list of excluded patches and click **Next**.

7 In the Schedule page, enter a name and optionally a description for the task.

8 Select **Immediately** to begin the process after you complete the wizard.

9 (Optional) Specify the rollback options and click **Next**.

a In the Rollback Options page of the Remediate wizard, select **Snapshot the virtual machines before remediation to enable rollback**.

A snapshot of the virtual machine (virtual appliance) is taken before remediation. If the virtual machine (virtual appliance) needs to roll back, you can revert to this snapshot.

b Specify when the snapshot should be deleted or select **Don't delete snapshots**.

c Enter a name and optionally a description for the snapshot.

d (Optional) Select the **Snapshot the memory for the virtual machine** check box.

10 Review the Ready to Complete page, and click **Finish**.

Scheduling Remediation for Hosts, Virtual Machines and Virtual Appliances

You can schedule the remediation process of hosts, virtual machines and virtual appliances using the Remediate wizard.

You can schedule remediation for all hosts or all virtual machines in a container object from the vSphere inventory and thus perform scheduled orchestrated upgrades of the hosts or virtual machines in the selected container object.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have installed and registered more than one Update Manager instance, you can create scheduled tasks for each Update Manager instance. Scheduled tasks you create are specific only to the Update Manager instance you specify and are not propagated to the other instances in the group. You can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered from the navigation bar.

Schedule Host Remediation Against Upgrade and Patch Baselines

You can schedule remediation for hosts at a time that is convenient for you.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Management > Scheduled Tasks** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager to use to schedule a remediation task by selecting the name of the corresponding vCenter Server system in the navigation bar.

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

3 Select **Remediate** and click **OK**.

4 In the Remediate wizard, select **ESX/ESXi hosts** and click **Next**.

5 Select the parent object to remediate and click **Next**.

All hosts under the selected object are also remediated. By selecting to upgrade a container object against an upgrade baseline or a baseline group containing an upgrade baseline, you perform an orchestrated upgrade of the hosts in the container object.

6 Select the baselines or baseline groups to apply.

7 (Optional) Select the hosts that you want to remediate and click **Next**.

If you remediate a single host, it is selected by default.

8 On the End User License Agreement page, accept the terms and click **Next**.

9 (Optional) On the ESX 4.0 Upgrade page, click the links of the settings that you want to edit.

Option	Description
COS VMDK location (Classic ESX only)	In the ESX 4.0 COS VMDK Location window, specify the datastore location for the VMDK to migrate the COS of the ESX host. IMPORTANT The datastores cannot be shared between hosts.
Rollback on failure (Classic ESX only)	In the ESX 4.0 Post Upgrade Options window, specify whether to disable rollback in case of failure.
Post-Upgrade script (Classic ESX only)	In the ESX 4.0 Post Upgrade Options window, specify a post-upgrade script usage after the upgrade completes and when the post-upgrade script times out.

The ESX 4.0 Upgrade page appears in the Remediate wizard only when you remediate against an ESX upgrade baseline or your baseline group contains an ESX upgrade baseline.

10 Click **Next**.

11 (Optional) Deselect specific patches to exclude them from the remediation process and click **Next**.

12 (Optional) Review the list of patches to be excluded and click **Next**.

13 On the Host Remediation Options page, enter a unique name for the task and optionally a description.

14 Specify a time for the remediation process to begin.

15 Specify the failure response for the remediation process and click **Next**.

Option	Description
Fail Task	Log this failure in the Update Manager logs and take no further action.
Retry	Wait for the retry delay period and retry putting the host into maintenance mode as many times as you indicate in **Number of retries**.
Power Off Virtual Machines and Retry	Power off all virtual machines and retry putting the host into maintenance mode as many times as you indicate in **Number of retries** field. Virtual machines are shut down as though their power off button is used.
Suspend Virtual Machines and Retry	Suspend all running virtual machines and retry putting the host into maintenance mode as many times as indicated in **Number of retries** field.

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

Schedule Virtual Machine and Virtual Appliance Remediation

You can schedule remediation for virtual machines and virtual appliances at a time that is convenient for you. You can remediate virtual machines and virtual appliances together.

IMPORTANT You can remediate powered on VMware Studio registered Red Hat, Ubuntu, SUSE, and CentOS Linux virtual appliances only.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Management > Scheduled Tasks** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager to use to schedule a remediation task by selecting the name of the corresponding vCenter Server system in the navigation bar.

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

3 Select **Remediate** and click **OK**.

4 In the Remediate wizard select **Virtual machines and virtual appliances** and click **Next**.

5 Select the object to remediate and click **Next**.

By selecting to upgrade a container object against an upgrade baseline group containing the VMware Tools Upgrade to Match Host baseline and the VM Hardware Upgrade to Match Host baseline, you perform an orchestrated upgrade of the virtual machines in the container object.

6 Select the baselines or baseline groups to apply.

7 Select the machines and appliances to remediate and click **Next**.

8 (Optional) On the Patches page deselect the check boxes for patches that you want to exclude from the remediation process and click **Next**.

The Patches page appears only if you remediate against patch baselines or a baseline group containing patch baselines.

9 (Optional) Review the list of excluded patches and click **Next**.

10 Enter the name and, optionally, a description for the task.

11 Select the time to initiate the remediation process for each virtual machine state (powered on, powered off, or suspended), and click **Next**.

12 (Optional) Specify the rollback options and click **Next**.

   a On the Rollback Options page of the Remediate wizard, select **Snapshot the virtual machines before remediation to enable rollback**.

      A snapshot of the virtual machine (virtual appliance) is taken before remediation. If the virtual machine (virtual appliance) requires a rollback, you can revert to this snapshot.

   b Specify when the snapshot should be deleted or select **Don't delete snapshots**.

   c Enter a name and optionally a description for the snapshot.

   d (Optional) Select the **Snapshot the memory for the virtual machine** check box.

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

The scheduled remediation task is displayed in the Scheduled Tasks window.

8 View Update Manager Events

Update Manager stores data about events. You can review this event data to gather information about operations that are in progress or that have finished.

You can view events in the Update Manager Administrator's view.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

2 Click the **Events** tab to get information about recent events.

This chapter includes the following topics:

View Tasks and Events for a Selected Object

You can view tasks and events that are associated with a single object or all objects in the vSphere inventory.

By default, the tasks list for an object includes tasks performed on its child objects. You can filter the list by removing tasks performed on child objects and by using keywords to search for tasks.

If your vCenter Server system is a part of a connected group in Linked Mode, a column in the task list displays the name of the vCenter Server system on which the task was performed.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Inventory** in the navigation bar.

2 Select the type of objects to remediate.

For example, **Hosts and Clusters** or **VMs and Templates**.

3 Select an object in the inventory.

4 Click the **Task & Events** tab.

5 Switch between tasks and events by clicking the **Tasks** and **Events** buttons.

Update Manager Events

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

Table 8-1. Update Manager Events

Type	Message Text	Action
Info	Successfully downloaded guest patch definitions. New patches: *number_of_patches*.	
Error	Failed to download guest patch definitions.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded guest patch definitions for UNIX. New patches: *number_of_patches*.	
Error	Failed to download guest patch definitions for UNIX.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded host patch definitions. New patches: *number_of_patches*.	
Error	Failed to download host patch definitions.	Check your network connections to make sure that your metadata source is reachable.
Info	Successfully downloaded guest patch packages. New packages: *number_of_packages*.	
Error	Failed to download guest patch packages.	Check your network connections to make sure that your patch source is reachable.
Info	Successfully downloaded guest patch packages for UNIX. New packages: *number_of_packages*.	
Error	Failed to download guest patch packages for UNIX.	Check your network connections to make sure that your patch source is reachable.
Info	Successfully downloaded host patch packages. New packages: *number_of_packages*.	
Error	Failed to download host patch packages.	Check your network connections to make sure that your patch source is reachable.
Info	Successfully scanned *virtual_machine_or_ESX_host_name* for patches.	
Error	Scanning *virtual_machine_or_ESX_host_name* has been cancelled by a user.	
Error	Failed to scan *virtual_machine_or_ESX_host_name* for patches.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for scan errors.
Warning	Found a missing patch: *patch_name* while scanning *virtual_machine_or_ESX_host_name*. Re-downloading patch definitions may resolve this problem.	
Info	Successfully scanned *virtual_appliance_name* for VA upgrades.	
Error	Failed to scan *virtual_appliance_name* for VA upgrades.	
Info	Successfully scanned *virtual_machine_name* for VMware Tools upgrades.	

Table 8-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Failed to scan *virtual_machine_name* for VMware Tools upgrades.	
Warning	VMware Tools is not installed on *virtual_machine_name*. VMware vCenter Update Manager only supports upgrading existing Tools installation.	
Warning	VMware Tools upgrade skipped for *virtual_machine_name*. It is supported only for VMs on ESX 4.0 host onwards.	
Error	Failed to scan *virtual_machine_name* because of an invalid state: *virtual_machine_state*.	Check the state of the virtual machine. Reboot the virtual machine to facilitate scanning.
Error	Failed to scan *ESX_host_name* for patches because of an invalid state: *ESX_host_state*	Check the state of the host. Reboot the host to facilitate scanning.
Info	Remediation succeeded for *virtual_machine_or_ESX_host_name*.	
Error	Remediation failed for *virtual_machine_or_ESX_host_name* with *error_message*.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for remediation errors.
Info	VMware Tools upgrade succeeded for *virtual_machine_name*.	
Error	VMware Tools upgrade failed for *virtual_machine_name*.	
Error	Failed to remediate *virtual_machine_name* because of an invalid state: *virtual_machine_state*.	Check the virtual machine's state. Restart the virtual machine to facilitate remediation.
Error	Failed to remediate *ESX_host_name* because of an invalid state: *ESX_host_state*.	Check the state of the host. Restart the host to facilitate remediation.
Info	Staging succeeded for *ESX_host_name*.	
Error	Staging failed for *ESX_host_name*.	
Error	Failed to stage patches on *ESX_host_name* because of invalid state: *ESX_host_connection_state*.	
Error	Failed to scan or remediate *virtual_machine_name* because of unsupported or unknown OS: *operating_system_name*.	
Error	Can't remediate *virtual_machine_name* for patches: Remediation of Linux VMs is not supported.	
Info	VMware vCenter 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 patches downloaded.
Error	Failed to scan *virtual_machine_name* because host *ESX_host_name* is of unsupported version *ESX_host_version*.	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Failed to remediate *virtual_machine_name* because host *ESX_host_name* is of unsupported version *ESX_host_version*.	For the latest information on which hosts can be scanned, see the release notes.
Error	Failed to scan *ESX_host_name* because it is of unsupported version *ESX_host_version*.	Hosts of versions later than ESX 3.0.3 and ESX 3i can be scanned. For the latest information on which ESX/ESXi hosts can be scanned, see the release notes.

Table 8-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Failed to stage patches on *ESX_host_name* because it is of unsupported version *ESX_host_version*.	Hosts of versions later than ESX/ESXi 4.0 can be staged. For the latest information on which ESX/ESXi host can be staged, see the release notes.
Error	Failed to remediate *ESX_host_name* for patches because it is of unsupported version *ESX_host_version*.	Hosts of versions later than ESX 3.0.3 and ESX- 3i can be scanned. For the latest information on which ESX/ESXi hosts can be scanned, see the release notes.
Info	VMware vCenter Update Manager Guest Agent successfully installed on *virtual_machine_name*.	
Error	Failed to install VMware vCenter Update Manager Guest Agent on *virtual_machine_name*.	Update Manager Guest Agent is required for remediating virtual machines.
Error	Failed to install VMware vCenter Update Manager Guest Agent on *virtual_machine_name* because VMware Tools is not installed or is of an incompatible VMware Tools version. The required version is *required_version_number* and the installed version is *installed_version_number*.	
Error	There is no VMware vCenter Update Manager license for *virtual_machine_or_ESX_host_name* for the required operation.	Obtain the required licenses to complete the desired task.
Warning	VMware vCenter Update Manager is running out of storage space. Location: *path_location*. Available space: *free_space*.	Add more storage.
Warning	VMware vCenter Update Manager is critically low on storage space! Location: *path_location*. Available space: *free_space*.	Add more storage.
Error	VMware vCenter Update Manager Guest Agent failed to respond in time on *virtual_machine_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 *virtual_machine_name*. Please check if the VM is powered on and retry the operation.	
Error	VMware vCenter Update Manager Guest Agent failed to access DVD drive on *virtual_machine_name*. Please check if a DVD drive is available and retry the operation.	
Error	An unknown internal error occurred during the required operation on *virtual_machine_name*. Please check the logs for more details and retry the operation.	
Error	Failed to install patches on *virtual_infrastructure_entity_name*.	
Info	Installing patches on *virtual_infrastructure_entity_name message*.	
Info	Install of patch on *virtual_infrastructure_entity_name* Succeeded.	
Info	Start rebooting host: *ESX_host_name*.	
Info	Waiting for host: *ESX_host_name* to reboot.	
Info	Host: *ESX_host_name* is successfully rebooted.	
Error	Host: *ESX_host_name* reboot failed. Please take a look at the host.	
Error	Failed to stage patch: *patch_name* on *ESX_host_name*.	

Table 8-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Stage of patch *patch_name* on *ESX_host_name* Succeeded.	
Error	Failed to reboot host *ESX_host_name*.	
Error	Failed to stage patches on *ESX_host_name*.	
Info	Start staging of patch *patch_name* on *ESX_host_name*.	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Failed to scan orphaned VM *virtual_machine_name*.	
Info	Failed to remediate orphaned VM *virtual_machine_name*.	
Error	Failure in downloading patch packages for following patches: *message*.	Check your network connections to make sure that your patch source is reachable.
Warning	*virtual_machine_name* contains an unsupported volume *volume_label*. Scan results for this virtual machine may be incomplete.	
Info	Initiating the task cancellation on *virtual_machine_or_ESX_host_name*	
Warning	There are running tasks for the entity *virtual_infrastructure_entity_name* that cannot finish within a specific time. The operation will be aborted.	
Warning	Action is not supported for offline or suspended virtual appliance *virtual_appliance_name*.	A scan or remediation process is not supported for offline virtual appliance.
Warning	Action is not supported for Linux VM/VA *virtual_machine_or_virtual_appliance_name*, tools not installed or boot up failure.	
Info	Successfully discovered virtual appliance *virtual_appliance_name*.	
Info	Failed to discover virtual appliance *virtual_appliance_name*.	An error occurred during the discovery of the virtual appliance.
Error	Auto update is set to ON for virtual appliance *virtual_appliance_name*.	If auto-update is set to ON in the virtual appliance, Update Manager cannot perform remediation.
Error	Repository address not set for virtual appliance *virtual_appliance_name*, it doesn't support patches by vCenter.	
Info	Open *virtual_machine_or_ESX_host_name* firewall ports.	
Info	Close *virtual_machine_or_ESX_host_name* firewall ports.	
Info	Patch definitions for *virtual_machine_or_ESX_host_name* missing. Please download patch definitions first.	
Info	Patch definitions for *virtual_machine_or_ESX_host_name* corrupted. Please check the logs for more details. Re-downloading patch definitions may resolve this problem.	
Info	Host upgrade in progress: Clearing partitions.	
Info	Host upgrade in progress: Partitioning physical hard drives.	
Info	Host upgrade in progress: Partitioning virtual hard drives.	
Info	Host upgrade in progress: Mounting file systems.	
Info	Host upgrade in progress: Installing packages.	

Table 8-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Host upgrade in progress: Migrating ESX v3 configuration to ESX v4.	
Info	Host upgrade in progress: Installing network configuration.	
Info	Host upgrade in progress: Setting timezone.	
Info	Host upgrade in progress: Setting keyboard.	
Info	Host upgrade in progress: Setting language.	
Info	Host upgrade in progress: Configuring authentication.	
Info	Host upgrade in progress: Setting root password.	
Info	Host upgrade in progress: Boot setup.	
Info	Host upgrade in progress: Running post-install script.	
Info	Host upgrade installer completed.	
Error	Host upgrade installer aborted.	
Info	Host upgrade in progress.	
Error	Host CPU not supported. A 64bit CPU is required.	
Error	The root partition does not have enough space for the installer: *disk_size*MB required, *disk_size*MB found.	
Warning	The root partition needs to be on the same disk as the `/boot` partition.	
Error	Error in ESX configuration file *ESX.conf*.	
Error	Error in inventory file.	
Error	Boot partition does not have enough space: *disk_size*MB required, *disk_size*MB found.	
Error	Boot partition is on an unsupported disk type.	
Warning	Unsupported agents found on the host.	
Warning	Unsupported services found on the host.	
Warning	Unsupported configuration found on the host, this configuration will not be migrated.	
Warning	Unsupported devices found on the host.	
Warning	Insufficient memory found on the host: *memory_size* MB required, *memory_size*MB found.	
Warning	Unsupported boot disk found on the host.	
Error	Upgrade pre-check script error.	
Info	Successfully scanned *virtual_machine_name* for Virtual Hardware upgrades.	
Error	Failed to scan *virtual_machine_name* for Virtual Hardware upgrades.	
Error	Virtual Hardware upgrade failed for *virtual_machine_name*, since VMware Tools is not the latest version. Presence of latest VMware Tools is a prerequisite for upgrading Virtual Hardware.	
Warning	Virtual Hardware upgrade skipped for *virtual_machine_name*. It is supported only for VMs on ESX 4.0 host onwards.	

Table 8-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Virtual Hardware upgrade succeeded for *virtual_machine_name*.	
Error	Virtual Hardware upgrade failed for *virtual_machine_name*.	
Error	VM *virtual_machine_name* is a VM that has either VMware vCenter Update Manager or VMware vCenter installed. This VM would be ignored for scan/remediation.	Virtual machines on which Update Manager or vCenter Server is installed are not scanned or remediated.
Error	The host *ESX_host_name* has a VM *virtual_machine_name* with VMware vCenter Update Manager or VMware vCenter installed. The VM needs to be moved to another host for the remediation to proceed.	Update Manager does not remediate hosts running virtual machines on which Update Manager or vCenter Server is installed. You must manually migrate such virtual machines to another host before you start the remediation process.
Error	Error while waiting for VMware Tools to respond. Please check whether VMware Tools is running in VM *virtual_machine_name*.	
Error	The version of VMware Tools installed in *virtual_machine_name* does not support automatic upgrade. Please upgrade VMware Tools manually.	
Info	Suspended VM *virtual_machine_name* has been skipped.	
Error	Cannot deploy upgrade agent on host.	
Error	Cannot run upgrade script on host.	

Patch Repository 9

Patch metadata is kept in a repository. You can use the patch repository to manage patches, check on new patches that have been downloaded, view patch details, and view in which baselines a patch is included.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have at least one Update Manager instance, you can select which Update Manager patch repository to view.

Patch repository is displayed in the Update Manager Administrator's view.

This chapter includes the following topics:

View Available Patches

The Patch Repository provides a convenient way to view the available downloaded patches and to include available patches in a baseline you select.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

   If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have at least one Update Manager instance, you can select which Update Manager patch repository to view by selecting the name of the respective vCenter Server system from the navigation bar.

2 Click the **Patch Repository** tab to view all the available patches.

The most recent downloaded patches are displayed in bold.

Add and Remove Patches from a Baseline

From the Patch Repository you can include available, recently downloaded patches in a baseline you select.

Procedure

1 Connect the vSphere Client to a vCenter Server system with which Update Manager is registered and select **Home > Solutions and Applications > Update Manager** in the navigation bar.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have at least one Update Manager instance, you can select which Update Manager patch repository to view by selecting the name of the respective vCenter Server system from the navigation bar.

2 Click the **Patch Repository** tab to view all the available patches.

3 Click the **Add to baseline** link in the Baselines column for a selected patch.

4 In the Edit containing baselines window, select or deselect the baselines in which you want to include, or from which you want to exclude this patch and click **OK**.

If your vCenter Server system is a part of a connected group in vCenter Linked Mode, and you have at least one Update Manager instance, you can add or exclude the patches from baselines specific to the selected Update Manager instance.

Search for Patches in the Patch Repository

You can search for specific patches in the patch repository using various criteria. An advanced search provides a way to filter the list of patches to display only those patches that match the criteria you specify.

Procedure

1 To locate a patch based on a keyword or phrase, enter text in the text box in the upper-right corner, and press Enter.

2 To search for patches using more specific criteria, click **Advanced** next to the text field.

3 In the Filter Patches window, enter search criteria.

Option	Description
Text contains	Restricts the patches displayed to those containing the text that you enter.
Product	Restricts the set of patches to the selected products or operating systems. The asterisk at the end of a product name is a wildcard character for any version number.
Severity	Specifies the severity of patches to include.
Released Date	Specifies the range for the release dates of the patches.
Patch Vendor	Specifies which patch vendor to use.

4 Click **Find**.

The contents of the Patch Repository are filtered according to the criteria you entered.

Common User Scenarios 10

With Update Manager, you can scan and remediate the objects in your vSphere inventory to keep them up to date with the latest patches, rollups, upgrades, and so on.

The common user scenarios provide task flows that you can perform with Update Manager to upgrade and patch your vSphere inventory objects and make them compliant against baselines and baseline groups that you attach.

This chapter includes the following topics:

Orchestrated Datacenter Upgrades Scenarios

Orchestrated upgrades allow you to upgrade the objects in your vSphere inventory in a two-step process: host upgrades followed by virtual machine upgrades. You can configure the process at the cluster level for higher automation or at the individual host or virtual machine level for granular control.

You can upgrade clusters with the virtual machine powered on as long as VMware Distributed Resource Scheduler (DRS) is available for the cluster. To perform an orchestrated upgrade, first remediate a cluster against a host upgrade baseline. Then remediate the same cluster against a virtual machine upgrade baseline group containing the VM Hardware Upgrade to Match Host baseline and the VMware Tools Upgrade to Match Host baseline.

- Orchestrated Upgrade of Hosts Scenario on page 94

  Update Manager allows you to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory using a single upgrade baseline.

- Orchestrated Upgrade of Virtual Machines Scenario on page 94

  An orchestrated upgrade allows you to upgrade VMware Tools and the virtual hardware of the virtual machines in your vSphere inventory at the same time. You can perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

Orchestrated Upgrade of Hosts Scenario

Update Manager allows you to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory using a single upgrade baseline.

You can perform orchestrated upgrades of hosts at the folder, cluster, or datacenter level.

This scenario describes how to perform an orchestrated upgrade of the hosts in your vSphere inventory.

Procedure

1 "Create a Host Upgrade Baseline," on page 55

2 "Attach Baselines and Baseline Groups to Objects," on page 61

To remediate hosts, you must attach the host upgrade baseline to a container object containing the hosts that you want to upgrade.

3 Scan the container object and review the scan results.

After you attach the host upgrade baseline to the selected container object, you must scan it to view the compliance state of the hosts in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of ESX/ESXi Hosts," on page 67
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

4 Remediate the container object against the attached baseline.

If hosts are in a noncompliant state, remediate the container object of the hosts to make it compliant with the attached baseline. You can start the remediation process manually or schedule a remediation task.

- "Manually Remediate Hosts Against Upgrade and Patch Baselines," on page 77
- "Schedule Host Remediation Against Upgrade and Patch Baselines," on page 80

Hosts that are upgraded reboot and disconnect for a period of time during the remediation.

The hosts in the remediated container object are upgraded and become compliant with the attached host upgrade baseline.

Orchestrated Upgrade of Virtual Machines Scenario

An orchestrated upgrade allows you to upgrade VMware Tools and the virtual hardware of the virtual machines in your vSphere inventory at the same time. You can perform an orchestrated upgrade of virtual machines at the folder or datacenter level.

Update Manager makes the process of upgrading the virtual machines convenient by providing baseline groups. When you remediate a virtual machine against a baseline group containing the VMware Tools Upgrade to Match Host baseline and the VM Hardware Upgrade to Match Host baseline, Update Manager sequences the upgrade operations in the correct order. As a result, the guest operating system is in a consistent state at the end of the upgrade.

This scenario describes how to perform an orchestrated upgrade of the virtual machines in your vSphere inventory.

Procedure

1 "Create a Virtual Machine and Virtual Appliance Baseline Group," on page 59

To upgrade virtual machines, you must create a virtual machine baseline group containing the VMware Tools Upgrade to Match Host baseline and the VM Hardware Upgrade to Match Host baseline.

2 "Attach Baselines and Baseline Groups to Objects," on page 61

To remediate the virtual machines, attach the baseline group to a container object that contains the virtual machines that you want to upgrade. The container object can be a folder or a datacenter.

3 Scan the container object and view the scan results.

After you attach the baseline group to the selected container object, you must scan it to view the compliance state of the virtual machines in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 68
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

4 Remediate the virtual machine container object against the attached baseline group.

If virtual machines are in a noncompliant state, you can remediate the container object to make the virtual machines compliant with the baselines in the attached baseline group. You can start the remediation manually or schedule a remediation task.

- "Manually Remediate Virtual Machines and Virtual Appliances," on page 78
- "Schedule Virtual Machine and Virtual Appliance Remediation," on page 81

During the upgrade of VMware Tools, the virtual machines must be powered on. If a virtual machine is in a powered off or suspended state before remediation, Update Manager powers on the machine. After the upgrade completes, Update Manager reboots the machine and restores the original power state of the virtual machine.

During the virtual machine hardware upgrade, the virtual machines must be shut down. After the remediation completes, Update Manager restores the original power state of the virtual machines. If a virtual machine is powered on, Update Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

The virtual machines in the container object become compliant with the attached baseline group.

Upgrade and Apply Patches to Hosts Using Baseline Groups Scenario

Baseline groups allow you to apply upgrade and patch baselines together and upgrade and update hosts in a single remediation operation.

You can upgrade all ESX/ESXi hosts in your deployment system using a single upgrade baseline. You can apply patches to the hosts at the same time using a baseline group containing one upgrade baseline and multiple host patch baselines.

This scenario describes how to upgrade and patch the hosts in your vSphere inventory at the same time.

Procedure

1 "Create a Host Upgrade Baseline," on page 55

2 "Create a Patch Baseline," on page 52

Create host patch baselines. You can create either dynamic or fixed patch baselines.

3 "Create a Host Baseline Group," on page 59

A host baseline group can contain one upgrade and multiple patch baselines. You can create a host baseline group with the upgrade and patch baselines that you created.

4 "Attach Baselines and Baseline Groups to Objects," on page 61

To remediate hosts, attach the baseline group to a container object containing the hosts that you want to update. The container object can be a folder, cluster, or datacenter.

5 Scan the container object and view the scan results.

After you attach the baseline group to the selected container object, you must scan it to view the compliance state of the hosts in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of ESX/ESXi Hosts," on page 67
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

6 Remediate the container object of the hosts against the attached baseline group.

If hosts are in a noncompliant state, remediate the container object to make it compliant with the baselines in the attached baseline group. You can start the remediation process manually or schedule a remediation task.

- "Manually Remediate Hosts Against Upgrade and Patch Baselines," on page 77
- "Schedule Host Remediation Against Upgrade and Patch Baselines," on page 80

During the remediation, the upgrade is performed first. Hosts that need to be both upgraded and updated with patches are first upgraded and then patched. Hosts that are upgraded might reboot and disconnect for a period of time during the remediation.

Hosts that do not need to be upgraded are only patched.

The hosts in the container object become compliant with the attached baseline group.

Apply Patches to Hosts Scenario

Host patching is the process in which Update Manager applies VMware ESX/ESXi host patches or third-party patches, such as Cisco Distributed Virtual Switch, to the ESX/ESXi hosts in your vSphere inventory.

At regular configurable intervals, Update Manager contacts Shavlik and VMware to gather the latest metadata about available patches. For more information about downloading patches, see "Downloading Patches and Patch Metadata," on page 14.

During host patch operations (scanning, staging, and remediation), you can check Update Manager events for information about the operation's status. You can also see which host patches are available in the Update Manager repository.

This scenario describes how to apply patches to the hosts in your vSphere inventory.

Prerequisites

You must configure Update Manager network connectivity settings, patch download sources, proxy settings, and checking for updates so that Update Manager downloads the host patches, patch metadata, and patch binaries. For more information, see Chapter 4, "Configuring Update Manager," on page 41.

Procedure

1 "Create a Patch Baseline," on page 52

Create host patch baselines. Patch baselines that you create can be either dynamic or fixed.

2 "Attach Baselines and Baseline Groups to Objects," on page 61

To remediate hosts, attach the patch baseline to a container object containing the hosts to which you want to apply the patches. The container object can be a folder, cluster, or datacenter.

3 Scan the container object and view the scan results.

After you attach the baseline group to the selected container object, you must scan it to view the compliance state of the hosts in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of ESX/ESXi Hosts," on page 67
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

4 (Optional) "Stage Patches for ESX/ESXi Hosts," on page 76

You can stage the patches and copy them from the Update Manager server to the hosts before applying them. Staging patches speeds up the remediation process and helps minimize the downtime of the hosts during remediation.

5 Remediate the container object of the hosts against the attached baseline group.

If hosts are in a noncompliant state, remediate the container object to make it compliant with the attached baseline. You can start the remediation process manually or schedule a remediation task.

- "Manually Remediate Hosts Against Upgrade and Patch Baselines," on page 77
- "Schedule Host Remediation Against Upgrade and Patch Baselines," on page 80

During staging patches and patch remediation, Update Manager performs pre- and post-scan operations. After remediation completes, the compliance state of the hosts against the attached baseline is updated to compliant.

Apply Patches to Virtual Machines Scenario

Update Manager allows you to keep the virtual machines in your vSphere inventory up to date. You can include patches for updating the virtual machines in your vSphere inventory in dynamic or fixed baselines, which can later be combined in baseline groups.

If you want to update the virtual machines with all critical or all noncritical patches, you can use the default Update Manager Critical VM Patches and Non-Critical VM Patches baselines.

This scenario describes how to apply patches to the virtual machines in your vSphere inventory.

Procedure

1 "Create a Patch Baseline," on page 52

2 (Optional) "Create a Virtual Machine and Virtual Appliance Baseline Group," on page 59

You can create a patch baseline group for the virtual machines that you want to remediate.

3 "Attach Baselines and Baseline Groups to Objects," on page 61

To remediate virtual machines, attach the patch baseline or baseline group to a container object containing the virtual machines. The container object can be a folder or datacenter.

4 Scan the container object and view the scan results.

After you attach the baseline or baseline group to the selected container object, you must scan it to view the compliance state of the virtual machines in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 68
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

5 Remediate the container object of the virtual machines against the attached baseline or baseline group.

If virtual machines are in a noncompliant state, remediate the container object to make it compliant with the attached baseline or baseline groups. You can start the remediation process manually or schedule a remediation task.

- "Manually Remediate Virtual Machines and Virtual Appliances," on page 78
- "Schedule Virtual Machine and Virtual Appliance Remediation," on page 81

One or more patches might require the guest operating system to reboot. If there are no users logged in to the guest operating system, the virtual machine reboots immediately. Otherwise, a dialog box informs users that are logged in of the upcoming shutdown.

The remediated virtual machines become compliant with the attached patch baselines or baseline groups.

Upgrade Virtual Appliances Scenario

An upgrade remediation of a virtual appliance upgrades the entire software stack in the virtual appliance, including the operating system and applications. If you want to upgrade the virtual appliance to the latest critical version, you can use one of the Update Manager predefined upgrade baselines or create your own.

This scenario describes how to upgrade the virtual appliances in your vSphere inventory.

Prerequisites

Virtual appliances must be powered on for scan and remediation operations. Because virtual appliances download the new virtual appliance version information or the new software package from the Internet, they must have Internet access.

Procedure

1 "Create a Virtual Appliance Upgrade Baseline," on page 57

2 "Attach Baselines and Baseline Groups to Objects," on page 61

To upgrade virtual appliances, attach the virtual appliance upgrade baseline to a container object containing the virtual appliances that you want to upgrade. The container object can be a folder, vApp, or datacenter.

3 Scan the container object and view the scan results.

After you attach the virtual appliance upgrade baseline to the selected container object, you must scan it to view the compliance state of the virtual appliances in the container. You can scan selected objects manually or schedule a scan task.

- "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 68
- "Schedule a Scan," on page 68
- "View Compliance Information for vSphere Objects," on page 69

The scan results are displayed in the Update Manager Client Compliance view.

4 Remediate the container object against the attached baseline.

If virtual appliances are in a noncompliant state, remediate the container object of the virtual appliances to make it compliant with the attached baseline. You can start the remediation process manually or schedule a remediation task.

- "Manually Remediate Virtual Machines and Virtual Appliances," on page 78
- "Schedule Virtual Machine and Virtual Appliance Remediation," on page 81

After you upgrade the virtual appliances, the guest operating system might reboot.

The virtual appliances are compliant with the attached baseline.

Keep the vSphere Inventory Up to Date Scenario

Using the Update Manager features, you can keep your vSphere inventory system updated with the most recent patches.

By changing the frequency of the checks for updates and patches, creating dynamic patch baselines, attaching the baselines to the objects in the inventory, and performing regular scans and remediations, you can keep your vSphere inventory of hosts, virtual machines, and virtual appliances updated.

This scenario describes how to keep the hosts and virtual machines in your vSphere inventory updated with the most recent patches.

Procedure

1 (Optional) "Configure Checking for Patches," on page 46

Update Manager checks for patches at regular intervals. You can modify the schedule for checking and downloading patches.

2 "Create a Dynamic Patch Baseline," on page 52

3 "Attach Baselines and Baseline Groups to Objects," on page 61

After you create dynamic patch baselines for hosts and virtual machines, attach the baselines to selected objects in the inventory.

4 "Schedule a Scan," on page 68

Schedule scans for the hosts and virtual machines in your vSphere inventory.

5 Schedule remediation for hosts and virtual machines.

To keep your system updated with the most recent patches, schedule remediation tasks for the hosts and virtual machines in the vSphere inventory using the dynamic baselines that you created.

- "Schedule Host Remediation Against Upgrade and Patch Baselines," on page 80
- "Schedule Virtual Machine and Virtual Appliance Remediation," on page 81

The hosts and virtual machines are updated with patches and are compliant with the attached patch baselines.

Generating Common Database Reports

Update Manager uses Microsoft SQL Server and Oracle databases to store information. Update Manager does not provide a reporting capability, but you can use a third-party reporting tool to query the database views to generate reports.

IMPORTANT The Update Manager database does not contain information about the objects in the inventory, and it contains internal inventory entity IDs. To get the original IDs for virtual machines, virtual appliances, and hosts, you must have access to the vCenter Server system database. From the vCenter Server system database, retrieve the ID of the objects that you are interested in. To obtain the Update Manager database IDs of the objects, Update Manager adds the prefix `vm-` (for virtual machines), `va-` (for virtual appliances), or `host-` (for hosts).

Generate Common Reports Using Microsoft Office Excel 2003

Using Microsoft Excel, you can connect to the Update Manager database and query the database views to generate a common report.

Prerequisites

You must have an ODBC connection to the Update Manager database.

Procedure

1 Log in to the computer on which the Update Manager database is set up.

2 From the Windows Start menu, select **Programs > Microsoft Office > Microsoft Excel**.

3 Click **Data > Import External Data > New Database Query**.

4 In the Choose Data Source window, select **VMware Update Manager** and click **OK**.

If necessary, in the database query wizard, select the ODBC DSN name and enter the user name and password for the ODBC database connection.

5 In the Query Wizard - Choose Columns window, select the columns of data to include in your query and click **Next**.

Option	Description
Available tables and columns	Lists the available tables, views, and columns. Scroll down to select a database view beginning with VUMV_, and expand the view to select specific columns by double-clicking them.
Columns in your query	Lists the columns you select to include in your query.
Preview of data in selected column	Displays the data in a selected column when you click **Preview Now**.

For example, if you want to get the latest scan results for all objects in the inventory and all patches for an inventory object, select these database views and their corresponding columns from the Available tables and columns pane:

- VUMV_UPDATES
- VUMV_ENTITY_SCAN_RESULTS

6 Click **OK** in the warning message that the Query Wizard cannot join the tables in your query.

7 In the Microsoft Query window, drag a column name from the first view to the other to join them manually.

For example, join the META_UID column from the VUMV_UPDATES database view with the UPDATE_METAUID column from the VUMV_ENTITY_SCAN_RESULTS database view.

A line between the columns selected indicates that these columns are joined.

The data is automatically queried for all inventory objects in the Microsoft Query window.

Generate Common Reports Using Microsoft SQL Server Query

Using a Microsoft SQL Server query, you can generate a common report from the Update Manager database.

Procedure

- To generate a report containing the latest scan results for all objects in the inventory and for all patches for an inventory object, run the query in Microsoft SQL Client.

```
SELECT r.entity_uid,r.ENTITY_STATUS,
                u.meta_uid, u.title, u.description, u.type, u.severity,
                (case when u.SPECIAL_ATTRIBUTE is null then 'false'
                else 'true'
                end) as IS_SERVICE_PACK,
                r.scanh_id, r.scan_start_time, r.scan_end_time
FROM VUMV_UPDATES u JOIN VUMV_ENTITY_SCAN_RESULTS r ON (u.meta_uid = r.update_metauid)
ORDER BY r.entity_uid, u.meta_uid
```

The query displays all patches that applicable to the scanned objects in the inventory.

11 Troubleshooting

If you encounter problems when running and using Update Manager, you can use a troubleshooting topic to understand and solve the problem, if there is a workaround.

This chapter includes the following topics:

Connection Loss with Update Manager Server or vCenter Server

Because of network connectivity loss or the servers restarting, the connection with the Update Manager server or vCenter Server system might stop.

Table 11-1 shows the Update Manager plug-in behavior and the causes for connection loss when the Update Manager is registered with a single vCenter Server system.

Table 11-1. Update Manager Plug-In Behavior in a Single vCenter Server System

Problem	Cause	Solution
Update Manager Client plug-in displays a reconnection dialog, and after 15-20 seconds, a failure message appears. The plug-in is disabled.	The Update Manager server stops and is not available for more than 15-20 seconds.	Start the Update Manager service and re-enable the Update Manager Client plug-in.
Update Manager client plug-in displays a reconnection dialog. Within 15-20 seconds, the dialog disappears, and the plug-in can be used.	The Update Manager server restarts, and the service becomes available within 15-20 seconds.	
vSphere Client displays a reconnection dialog. After an interval, it displays the login form. To use Update Manager, the Update Manager plug-in must be enabled again.	vCenter Server stops.	Start the vCenter Server service and enable the Update Manager plug-in.

Table 11-2 displays the Update Manager plug-in behavior and the causes for connection loss in an environment in which the vCenter Server system is part of a connected group in vCenter Linked Mode and an Update Manager instance is registered with each vCenter Server system in the group.

Table 11-2. Update Manager Plug-In Behavior in a Connected Group in vCenter Linked Mode

Problem	Cause	Solution
Update Manager client plug-in displays a modal reconnection dialog, and after 15-20 seconds, a failure message appears. The plug-in for the Update Manager server in use disappears from the vSphere Client. **Note** Although the Update Manager plug-in is shown as enabled, you have to disable and enable the plug-in after the connection is restored. If you select to use another vCenter Server system from the connected group, and the Update Manager registered with this vCenter Server system is running, the Update Manager plug-in is available for the running Update Manager server.	The Update Manager server in use stops and is not available for more than 15-20 seconds.	Start the Update Manager service.
Update Manager client plug-in displays a modal reconnection dialog. Within 15-20 seconds, the dialog disappears, and the plug-in can be used.	The Update Manager server in use restarts, and the service becomes available within 15-20 seconds.	

Table 11-2. Update Manager Plug-In Behavior in a Connected Group in vCenter Linked Mode (Continued)

Problem	Cause	Solution
If you select to use a vCenter Server system with which a stopped Update Manager server is registered, the Update Manager plug-in shows a modal reconnection dialog and tries to reconnect to the newly selected Update Manager server for 15-20 seconds.	An Update Manager server that is not currently in use stops.	Start the Update Manager service.
vSphere Client disables all tabs for the vCenter Server system. The Update Manager plug-in is disabled. When the vCenter Server system is available again, the Update Manager plug-in is automatically enabled for it.	vCenter Server stops.	Start the vCenter Server service.

Gather Update Manager Log Files

You can gather information about recent events on the Update Manager server for diagnostic purposes.

Procedure

1 Log in to the machine on which Update Manager is installed.

   To obtain the complete set of the logs, VMware recommends that you log in with the user name and password of the user that installed Update Manager.

2 Select **Start > All Programs > VMware > Generate Update Manager log bundle**.

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

Gather Update Manager and vCenter Server Log Files

When Update Manager server and vCenter Server are installed on the same computer, you can gather information about recent events on the Update Manager server and vCenter Server system for diagnostic purposes.

Procedure

1 Log in to the computer on which vCenter Server and Update Manager are installed.

2 Select **Start > All Programs > VMware > Generate vCenter Server log bundle**.

Log files for vCenter Server and the Update Manager server are generated as a ZIP package, which is stored on the current user's desktop.

Log Files Are Not Generated

Because of limitations in the ZIP utility used by the Update Manager, the cumulative log file size cannot exceed 2GB, although the script seems to complete successfully.

To generate Update Manager log files, exclude the generation of the vCenter Server logs using the `vum-support.wsf` script file.

Procedure

1 Log in to the computer on which Update Manager is installed, and open a Command Prompt window.

2 Change to the directory where Update Manager is installed.

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

3 Run the script and exclude the vCenter Server logs by entering:

```
cscript vum-support.wsf /n
```

The Update Manager log files are generated as a ZIP package successfully.

No Baseline Updates Available

Baselines are based on metadata that Update Manager downloads from the Shavlik and VMware Web sites.

Table 11-3 shows a list of possible causes and solutions for unavailable baseline updates.

Table 11-3. No Available Baseline Updates Causes

Cause	Solution
Misconfigured Web server proxy	See "Configure Update Manager Network Connectivity Settings," on page 42.
Shavlik servers are unavailable	Check the Shavlik Web site (http://www.shavlik.com) to determine whether it is available.
VMware update service is unavailable to provide information about ESX host updates	
Poor network connectivity	Check whether other applications that use networking are functioning as expected. Consult your network administrator to best assess whether the network is working as expected.

All Updates in Compliance Reports Are Not Applicable

The results of a scan might be that all baselines are marked as Not Applicable. Such a condition typically indicates an error in scanning.

Table 11-4 shows a list of possible causes and solutions for not applicable baselines.

Table 11-4. Not Applicable Updates Causes

Cause	Solution
Scan results usually consist 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 only a concern when this is the universal result or when you know that the patches should be applicable.	Examine the server logs for scan tasks that are marked as failed, or retry the scan operation. If problems persist, collect logs and contact VMware support for further assistance.

All Updates in Compliance Reports Are Unknown

All results of a scan might be listed as unknown.

Table 11-5 displays a list of possible causes and solutions for the unknown state of updates in a baseline.

Table 11-5. Unknown State of Updates Causes

Cause	Solution
Error at the start of the scan.	Schedule a scan or manually initiate a scan.
No scanning occurred.	Schedule a scan or manually initiate a scan.

Remediated Updates Continue to Be Noncompliant

When remediated updates continue to be noncompliant, you must check whether the updates are installed on the virtual machine.

Table 11-6 shows a list of possible causes and solutions for updates that are in a noncompliant state after remediation.

Table 11-6. Causes for Noncompliant Updates State

Cause	Solution
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 Patches or All Critical Patches Fails

In some instances, remediating virtual machines with the All Updates or All Critical Updates default baselines fails.

Table 11-7 shows a list of the problems and possible causes and solutions for virtual machine remediation failure.

Table 11-7. Causes for Virtual Machine Patch Remediation Failure

Problem	Cause	Solution
Remediation fails to complete	Remediation might stop on a particular virtual machine. In rare cases, this results from a patch application displaying a message box after it is partially completed. Patches are applied by the VMware vCenter Update Manager Guest Agent, which runs in the local system context. Running the Guest Agent in this context prevents users from interfering with the patch application process. However, message boxes are never displayed in a form where they can be acknowledged and dismissed. Consequently, the patch application process cannot be completed.	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 vSphere Client. Update Manager posts events to identify the start and completion of a patch installation, along with the error code, if applicable. If the most recent events indicate the start of a patch installation but not its completion, use the name of the update to identify the patch process. Microsoft patches are easier to identify because they typically contain the KB number in their filenames.
Remediation fails for some patches	Patches are not available. For example, a test indicates that versions of Windows localized for languages other than English or patches for 64-bit applications might be unavailable.	Review the Events tab of the Update Manager plug-in to determine if patches were not downloaded.
Remediation completes but the baseline is still non compliant.	This condition might occur when applying patches that subsequently make other patches applicable. For example, a patch might be applicable only after a service pack is applied, so applying that service pack might address all known issues from when the remediation started, but the act of applying the service pack made other patches applicable.	Repeat the remediation.

VMware Tools Upgrade Fails if VMware Tools Is Not Installed

Update Manager upgrades only an existing installation of VMware Tools in a virtual machine running on an ESX 4.0 host.

Table 11-8 shows a list of possible causes for the VMware Tools upgrade failure.

Table 11-8. Causes for VMware Tools Upgrade Failure

Cause	Solution
If there is no VMware Tools installation on a virtual machine, when you scan the virtual machine against the VMware Tools Upgrade to Match Host baseline or a baseline group containing this baseline, the result is an incompatible compliance state of the virtual machine.	A virtual machine in incompatible compliance state cannot be remediated. The workaround is to install VMware Tools manually or right-click the virtual machine in the vSphere Client Inventory and select **Guest > Install/Upgrade VMware Tools**.

ESX/ESXi Hosts Scanning Fails

Scanning ESX 4.0 and ESXi 4.0 hosts might fail.

Table 11-9 shows a list of possible causes and solutions for the host scan failure.

Table 11-9. Causes for Host Scanning Failure

Cause	Solution
If the VMware vCenter Update Manager Update Download task has not completed successfully after you add a host to the vSphere inventory, no host patch metadata is downloaded.	After you add a host or a virtual machine to the vSphere inventory, run the VMware vCenter Update Manager Update Download task before performing the scan. For more information, see "Run the VMware vCenter Update Manager Update Download Task," on page 50.

ESXi Host Upgrade Fails

During the remediation process of an ESXi host against an upgrade baseline or a baseline group containing an upgrade baseline, the remediation process might fail.

Table 11-10 lists the possible causes and solutions for ESXi host upgrade failure.

Table 11-10. Causes for ESXi Host Upgrade Failure

Cause	Solution
When you upgrade an ESXi host with less than 10MB of free space in its `/tmp` directory, although Update Manager indicates that the remediation process completes successfully, the ESXi host is not upgraded.	If you see an Agent Deploy failure, make sure that the `/tmp` directory has at least 10MB of free space, and then repeat the remediation process to upgrade the host.

Incompatible Compliance State

After you perform a scan, the compliance state of the attached baseline might be incompatible. The incompatible compliance state requires more attention and further action to be resolved.

Incompatibility might be caused by an update in the baseline for a number of reasons.

Conflict The update conflicts with either an existing update on the host or another update in the Update Manager depot. Update Manager reports what type of conflict it is. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you must take action to resolve the conflict.

Missing Package This state occurs when metadata for the update is in the depot but the corresponding binary payload is missing. The reasons can be that the product might not have an update for a given locale; the Update Manager patch repository is deleted or corrupt, and Update Manager no longer has Internet access to download updates; or you have manually deleted an upgrade package from the Update Manager repository.

Not Installable The update cannot be installed. The scan operation might succeed on the target object, but remediation cannot be performed. For example, missing updates on a Linux virtual machine are reported as Not Installable, because Update Manager does not support remediation of Linux virtual machines.

New Module The host update is a brand new module, that provides a software for the first time and Update Manager cannot install an update in this state.

Incompatible Hardware The hardware of the selected object is incompatible or has insufficient resources to support the update. For example, when you perform a host upgrade scan against a 32 bit host or the host has insufficient RAM.

Unsupported Upgrade The upgrade path is not possible. For example, the current hardware version of the virtual machine is greater than the highest version supported on the host.

Table 11-11 lists the possible update statuses, causes, and solutions, if any, for the incompatible compliance state.

Table 11-11. Incompatible Compliance State Causes and Solutions

Update Status	Cause	Remarks	Solution
Conflict	The baseline contains a host patch that conflicts with another patch already installed on the host.	The scan operation succeeds, but the state is incompatible.	Detach or remove the baseline. If Update Manager suggests a replacement patch for the conflicting patch, remove the conflicting patch and add the replacement into the baseline. Retry the scan operation.
Conflict	The baseline contains a host patch that conflicts with other patches in the same baseline.	The scan operation succeeds, but the state is incompatible.	Remove the conflicting patches and perform the scan again. If Update Manager suggests a replacement patch for the conflicting patch, remove the conflicting patch and add the replacement into the baseline. Retry the scan operation.
Conflict	The dynamic baseline criteria results in a conflicting set.	The scan operation succeeds, but the state is incompatible.	Edit the dynamic baseline criteria or exclude the conflicting patches and scan again. If Update Manager suggests a replacement patch for the conflicting patch, remove the conflicting patch and add the replacement to the baseline using the Dynamic Patches to Exclude and Other Patches to Add pages of the New Baseline wizard. Retry the scan operation.
Conflict	The baseline is attached to a container object and has conflicts for one or more inventory objects in the folder. This is an indirect conflict.	The scan operation succeeds, but the state is incompatible.	You can remediate the container object, but only the objects that are not in conflict are remediated. VMware recommends that you resolve the conflicts or move the inventory objects that are in conflict, and then remediate.
Missing Package	When you perform a host upgrade scan and the binary package for the host is missing or not uploaded, or you upload the wrong binary package.	The scan operation fails.	Edit the host upgrade baseline and import the required package.

Table 11-11. Incompatible Compliance State Causes and Solutions (Continued)

Update Status	Cause	Remarks	Solution
Unsupported Upgrade	The upgrade path for the virtual hardware of the virtual machine is not possible, because the current hardware version is higher than the latest version supported on the host.	The Upgrade Details window shows the actual hardware version.	None
Not Installable	A baseline containing Linux patches is attached to a RHEL virtual machine.	If there are one or more updates that are missing during the scan, they appear as Not Installable.	No action, or detach the baseline.
Not Installable	A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine with no installed VMware Tools.	The Upgrade Details window shows the actual reason for the Incompatible state.	If VMware Tools is not installed on the virtual machine, install a version of VMware Tools and retry the scan operation.
Not Installable	A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine with Tools not managed by VMware.	The Upgrade Details window shows the actual reason for the Incompatible state.	Detach the baseline.

Database Views

12

Update Manager uses Microsoft SQL Server and Oracle databases to store information. The database views for Microsoft SQL Server and Oracle databases are the same.

This chapter includes the following topics:

VUMV_VERSION

This database view contains Update Manager version information.

Table 12-1. VUMV_VERSION

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

VUMV_UPDATES

This database view contains software update metadata.

Table 12-2. VUMV_UPDATES

Field	Notes
UPDATE_ID	Unique ID generated by the Update Manager
TYPE	Entity type: virtual machine, virtual appliance, or host
TITLE	Title
DESCRIPTION	Description
META_UID	Unique ID provided by the vendor for this update (for example, MS12444 for Microsoft updates)
SEVERITY	Update severity information: values are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
RELEASE_DATE	Date on which this update was released by the vendor
DOWNLOAD_TIME	Date and time this update was downloaded by the Update Manager server into the Update Manager database
SPECIAL_ATTRIBUTE	Any special attribute associated with this update (for example, all Microsoft Service packs are marked as Service Pack)
COMPONENT	Target component, such as HOST_GENERAL, HOST_THIRDPARTY, and so on

VUMV_HOST_UPGRADES

This database view provides detailed information about the host upgrade packages.

Table 12-3. VUMV_HOST_UPGRADES

Field	Notes
RELEASE_ID	Database-generated ID, which refers to VUMV_UPDATES and UPDATE_ID
PRODUCT	ESX or ESXi host
VERSION	Version number represented in x.y.z format
BUILD_NUMBER	Build number of the ESX/ESXi host version
DISPLAY_NAME	Name displayed to the user
FILE_NAME	Name of the upgrade file

VUMV_VA_UPGRADES

This database view represents detailed information about the virtual appliance upgrade packages.

Table 12-4. VUMV_VA_UPGRADES

Field	Notes
UPGRADE_ID	Upgrade ID used as a primary key
TITLE	Short description used in the user interface
VENDOR_NAME	Vendor name
VENDOR_UID	Unique ID from the vendor
PRODUCT_NAME	Product name
PRODUCT_RID	Unique ID of the product
SEVERITY	Security impact
LOCALE	Locale information, if any
RELEASEDATE	Release date of the upgrade

VUMV_PATCHES

This database view contains patch binary metadata.

Table 12-5. VUMV_PATCHES

Field	Notes
DOWNLOAD_URL	URL for the patch binary
PATCH_ID	Unique ID for the current patch, generated by the Update Manager server
TYPE	Patch type: a virtual machine or host
NAME	Name of the patch
DOWNLOAD_TIME	Date and time the patch was downloaded by the Update Manager server into the Update Manager database
PATCH_SIZE	Size of the patch in KB

VUMV_BASELINES

This database view contains the details for a particular Update Manager baseline.

Table 12-6. VUMV_BASELINES

Field	Notes
BASELINE_ID	Unique ID generated for this baseline by the Update Manager server
NAME	Name of the baseline
BASELINE_VERSION	History of when the baseline has been changed (old version remains in the database)
TYPE	Baseline type: virtual machine, virtual appliance, or host
BASELINE_UPDATE_TYPE	Baseline type: fixed or dynamic

Table 12-6. VUMV_BASELINES (Continued)

Field	Notes
TARGET_COMPONENT	Type of targets that this baseline applies to: virtual machine, virtual appliance, or host
BASELINE_CATEGORY	Baseline category, such as patch or upgrade

VUMV_BASELINE_GROUPS

This database view contains the details for a particular Update Manager baseline group.

Table 12-7. VUMV_BASELINE_GROUPS

Field	Notes
BASELINE_GROUP_ID	Unique ID generated for this baseline group by the Update Manager server
VERSION	Version of the baseline group
NAME	Name of the baseline group
TYPE	Type of targets that this baseline applies to: virtual machine, virtual appliance, or ESX/ESXi host
DESCRIPTION	Description of the baseline group
DELETED	Information about the baseline group deletion, if it is deleted
LASTUPDATED	Information about the last update time of the baseline group

VUMV_BASELINE_GROUP_MEMBERS

This database view contains information about the relationship between the baseline and the baseline group in which it is included.

Table 12-8. VUMV_BASELINE_GROUP_MEMBERS

Field	Notes
BASELINE_GROUP_ID	Unique ID generated for this baseline group by the Update Manager server
BASELINE_GROUP_VERSION	Version of the baseline group
BASELINE_ID	Name of the baseline included in the baseline group

VUMV_PRODUCTS

This database view contains product metadata, including operating systems and applications.

Table 12-9. VUMV_PRODUCTS

Field	Notes
PRODUCT_ID	Unique ID for the product generated by the Update Manager server
NAME	Name of the product
VERSION	Product version
FAMILY	Windows, Linux, ESX host, or Embedded ESX host

VUMV_BASELINE_ENTITY

This database view contains the objects to which a particular baseline is attached.

Table 12-10. VUMV_BASELINE_ENTITY

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

VUMV_UPDATE_PATCHES

This database view contains patch binaries that correspond to a software update.

Table 12-11. VUMV_UPDATE_PATCHES

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

VUMV_UPDATE_PRODUCT

This database view contains products (operating systems and applications) to which a particular software update applies.

Table 12-12. VUMV_UPDATE_PRODUCT

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

VUMV_ENTITY_SCAN_HISTORY

This database view contains the history of the scan operations.

Table 12-13. VUMV_ENTITY_SCAN_HISTORY

Field	Notes
SCAN_ID	Unique ID generated by the Update Manager server
ENTITY_UID	Unique ID of the entity the scan was initiated on
START_TIME	Start time of the scan operation
END_TIME	End time of the scan operation
SCAN_STATUS	Result of the scan operation (for example, Success, Failure, or Canceled)
FAILURE_REASON	Error message describing the reason for failure
SCAN_TYPE	Type of scan: patch or upgrade
TARGET_COMPONENT	Type of targets that are scanned: virtual machine, virtual appliance, or host

VUMV_ENTITY_REMEDIATION_HIST

This database view contains the history of remediation operations.

Table 12-14. VUMV_ENTITY_REMEDIATION_HIST

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

VUMV_UPDATE_PRODUCT_DETAILS

This database view contains information about the products (operating systems and applications) to which a particular software update applies.

Table 12-15. VUMV_UPDATE_PRODUCT_DETAILS

Field	Notes
UPDATE_METAUID	Software update ID (foreign key, VUMV_UPDATES)
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update impact information: values are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
PRODUCT_NAME	Product name
PRODUCT_VERSION	Product version

VUMV_BASELINE_UPDATE_DETAILS

This database view information about the software updates that are part of a baseline.

Table 12-16. VUMV_BASELINE_UPDATE_DETAILS

Field	Notes
BASELINE_NAME	Baseline name
BASELINE_ID	Unique ID generated for this baseline by the Update Manager server
BASELINE_VERSION	History about when the baseline was changed (old version remains in the database)
TYPE	Baseline type: virtual machine, virtual appliance, or host
TARGET_COMPONENT	Type of targets this baseline applies to: virtual machine, virtual appliance, or host
BASELINE_UPDATE_TYPE	Baseline type: fixed or dynamic
UPDATE_METAUID	Update meta ID
TITLE	Update title

Table 12-16. VUMV_BASELINE_UPDATE_DETAILS (Continued)

Field	Notes
SEVERITY	Update severity: values are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
ID	Unique ID generated by the database: UPDATE_ID for updates and patches; RELEASE_ID for host upgrades; UPGRADE_ID for virtual appliance upgrades

VUMV_ENTITY_SCAN_RESULTS

This database view contains status history of a particular entity for an update.

Table 12-17. VUMV_ENTITY_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
UPDATE_METAUID	Update meta unique ID
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update severity: values are Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
ENTITY_STATUS	Status of the entity with regard to the update: values are Missing, Installed, Not Applicable, Unknown, Staged, Conflict, ObsoletedByHost, MissingPackage, NotInstallable, NewModule, UnsupportedUpgrade, and IncompatibleHardware

VUMV_VMTOOLS_SCAN_RESULTS

This database view contains information about a particular virtual machine regarding VMware Tools installation.

Table 12-18. VUMV_VMTOOLS_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
ENTITY_STATUS	Status of the entity against the latest VMware Tools version

VUMV_VMHW_SCAN_RESULTS

This database view contains status information for a particular virtual machine regarding its hardware version.

Table 12-19. VUMV_VMHW_SCAN_RESULTS

Field	Notes
SCANH_ID	Unique ID of the scan generated by the database
ENTITY_UID	Entity unique ID (a managed object ID assigned by vCenter Server)

Table 12-19. VUMV_VMHW_SCAN_RESULTS (Continued)

Field	Notes
SCAN_START_TIME	Start time of the scan process
SCAN_END_TIME	End time of the scan process
VM_HW_VERSION	Virtual machine hardware version
HOST_HW_VERSION	Hardware version recommended on the host

VUMV_VA_APPLIANCE

This database view contains information about the virtual appliances.

Table 12-20. VUMV_VA_APPLIANCE

Field	Notes
VAID	Managed object ID of the virtual appliance, used as the primary key
MGMTPORT	Port through which the virtual appliance is contacted or managed
MGMTPROTOCOL	Management protocol
SUPPORTEDFEATURES	Fee-form string for API feature compatibility
LASTGOODIP	Last known IP the virtual appliance had (can be IPv6 or IPv4)
VADKVERSION	VMware Studio version
PRODUCTID	ID in VUMV_VA_PRODUCTS
UPDATEVERSION	Current patch version of the virtual appliance
DISPLAYVERSION	Current patch display version of the virtual appliance
SERIALNUMBER	Serial number of the virtual appliance
UPDATEURL	Current software update URL of the virtual appliance
ORIGUPDATEURL	Factory default software update URL of the virtual appliance

VUMV_VA_PRODUCTS

This database view contains information about the virtual appliance vendor.

Table 12-21. VUM_VA_PRODUCTS

Field	Notes
ID	Unique ID, a generated sequence number
VENDORNAME	Vendor name
VENDORUUID	Unique ID of the vendor
PRODUCTNAME	Product name (minus the release, for example, Database)
PRODUCTRID	Product release ID (for example, 10gr2)
VENDORURL	Vendor URL (this field is optional)
PRODUCTURL	Product URL (this field is optional)
SUPPORTURL	Support URL (this field is optional)

Index

V