VMware vCenter Update Manager Installation and Administration Guide

vCenter Update Manager 4.1

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-000236-03

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 *Update Manager Installation and Administration Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *Update Manager Installation and Administration Guide*.

Revision	Description
EN-000236-03	■ "Upgrade the Update Manager Server," on page 50 now contains the prerequisite to stop only the Update Manager service and not the vCenter Service before upgrading the Update Manager server.
EN-000236-02	■ "Upgrade the Update Manager Server," on page 50 now contains the prerequisite to stop the Update Manager and vCenter Server services before upgrading the Update Manager server. ■ "Change the UMDS Patch Repository Location," on page 63 now contains the correct command that you must enter to change the UMDS patch repository location. ■ Minor revisions.
EN-000236-01	■ "Upgrade UMDS," on page 61 now contains information about the UMDS configuration and a recommended task you might want to perform before upgrading UMDS. ■ "Configuring the Update Manager Patch Download Source," on page 16, "Configuring Update Manager Patch Download Sources," on page 69 and "Import Patches Manually," on page 73 now contain information that the import of offline bundles is supported only for hosts running ESX/ESXi 4.0 and later. ■ "Remediating Hosts," on page 114 now describes the correct Update Manager behavior when you start a host remediation on hosts in a cluster. ■ Minor revisions.
EN-000236-00	Initial release.

About This Book

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

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.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to: http://www.vmware.com/support/pubs.

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.

Understanding Update Manager 1

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 that you specify can be applied to operating systems, as well as to applications on ESX/ESXi hosts, virtual machines, and virtual appliances that you scan. With Update Manager, you can perform the following tasks:

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

Update Manager requires network connectivity with VMware vCenter Server. Each installation of 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 of 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 part of a connected group in vCenter Linked Mode, and you want to use Update Manager for each vCenter Server system, you must install and register Update Manager instances with each vCenter Server system. You can use an Update Manager instance only with the vCenter Server system with which it is registered.

To install Update Manager, you must have Windows administrator credentials for the computer on which you install Update Manager.

With Update Manager, you can scan and remediate (update) ESX/ESXi hosts. You can also scan and remediate virtual machines and templates. Update Manager can scan and remediate virtual appliances that are created with VMware Studio 2.0 and later. If the remediation fails, you can revert virtual machines back to their prior condition without losing data.

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 (UMDS) to download patch metadata and patch binaries.

This chapter includes the following topics:

Security Best Practices

Keeping the patch versions up to date 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 do the following:

- Be aware of where vulnerabilities exist in your environment.
- Efficiently bring vulnerable 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, appliances, 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 the tactics that you want to use to implement the plan.

Update Manager Client Overview

The Update Manager Client has two main views, Administration view and Compliance view.

To access the Administration 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. In the Update Manager Client Administration view, you can do the following tasks:

- Configure the Update Manager settings
- Create and manage baselines and baseline groups
- View Update Manager events
- Review the patch repository
- Add or remove patches or extensions from a baseline
- Review and check notifications
- Import host upgrade releases

To view Compliance view information for a selected inventory object, click 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 do the following 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 or extensions to hosts
- Remediate a selected inventory object

If your vCenter Server system is 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.

For a vCenter Server system that is a part of a connected group in vCenter Linked Mode, you can also 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 and extensions with 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 (metadata) about a set of patches and extensions. One or more of these patches or extensions are aggregated to form a baseline. You can add multiple baselines 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 scan and remediate an inventory object against all of them as a whole. If a baseline group contains both upgrade and patch or extension baselines, the upgrade runs 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. You can initiate these processes manually or through scheduled tasks.

- Configuring the Update Manager Patch Download Source on page 16

  You can configure the Update Manager server to download patches and extensions either from the Internet or from a shared repository of UMDS data. You can also import patches and extensions manually from a ZIP file.

- Downloading Patches, Extensions, Notifications, and Related Metadata on page 17

  Downloading patches, extensions, and related metadata is an automatic process that can also be modified. By default, at regular configurable intervals, Update Manager contacts Shavlik, VMware, or third-party sources to gather the latest information (metadata) about available patches or extensions.

- Importing Host Upgrade Release Files on page 18

  You can upgrade the hosts in your environment by using host upgrade baselines. To create a host upgrade baseline, you must first upload host upgrade files to the Update Manager repository.

- Creating Baselines and Baseline Groups on page 18

  Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades, and can be classified as upgrade, extension, or patch baselines. Baseline groups are assembled from existing baselines. Baseline groups might contain a number of patch or extension baselines, and only one upgrade baseline per upgrade type (like VMware Tools, virtual machine hardware, virtual appliance, or host).

- Attaching Baselines and Baseline Groups to vSphere Objects on page 18

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

- Scanning Selected vSphere Objects on page 18

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

- Reviewing Scan Results on page 20

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

- Staging Patches and Extensions to Hosts on page 20

  If you want to apply patches or extensions to the hosts in your environment, you can stage the patches and extensions before remediation to ensure that the patches and extensions are downloaded to the host. Staging patches and extensions is an optional step.

- Remediating Selected vSphere Objects on page 20

  Remediation is the process in which Update Manager applies patches, extensions, 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 and extensions either from the Internet or from a shared repository of UMDS data. You can also import patches and extensions manually from a ZIP file.

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

If your deployment system is connected to the Internet, you can use the default settings and links for downloading patches and extensions to the Update Manager patch repository. You can also add URL addresses to download third-party patches and extensions that are applicable only to ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the patches and extensions by using the UMDS. For more information, see Chapter 10, "Installing, Setting Up, and Using Update Manager Download Service," on page 59.

With Update Manager 4.1, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. You download these patches or extensions from the Internet or copy them from a media drive, and save them as offline bundle ZIP files on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later.

IMPORTANT You can import offline bundles only for hosts that are running ESX/ESXi 4.0 or later.

For detailed descriptions of the procedures, see "Configuring Update Manager Patch Download Sources," on page 69.

Downloading Patches, Extensions, Notifications, and Related Metadata

Downloading patches, extensions, and related metadata is an automatic process that can also be modified. By default, at regular configurable intervals, Update Manager contacts Shavlik, VMware, or third-party sources to gather the latest information (metadata) about available patches or extensions.

VMware provides information about patches for ESX/ESXi hosts, and Shavlik provides information for all major applications and operating systems.

Update Manager downloads the following types of information:

- Information about all virtual machines patches regardless of whether the application or operating system to which the patch applies is currently in use in your environment.
- Information about all ESX/ESXi 4.0.x and ESX/ESXi 4.1 patches regardless of whether you have hosts of such versions in your environment.
- Patches for ESX/ESXi 3.5 and ESX 3.0.3 hosts, which are downloaded after you add an ESX 3.5, ESXi 3.5, or ESX 3.0.3 host to your environment.
- Information about ESX/ESXi 4.0.x and ESX/ESXi 4.1 patches as well as extensions from third-party vendor URL addresses.
- Notifications, alerts and patch recalls about ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts.

Downloading information about all patches or extensions 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 hosts, applications, or operating systems at any time.

In addition to downloading patches, extensions, and related metadata, Update Manager 4.1 supports the recall of patches for ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts. A patch is recalled if the released patch has problems or potential issues. After you scan the hosts in your environment, Update Manager alerts you if the recalled patch has been installed on a certain host. Recalled patches cannot be installed on hosts with Update Manager. Update Manager also deletes all the recalled patches from the Update Manager patch repository. After a patch fixing the problem is released, Update Manager downloads the new patch in its patch repository. If you have already installed the problematic patch, Update Manager notifies you that a fix was released and prompts you to apply the new patch.

When you remediate a virtual machine for the first time, Update Manager has the following behavior:

1 Update Manager downloads the applicable patches to the patch repository.

2 Update Manager applies the patches.

3 The downloaded patches are kept in the patch download repository, so that when other machines are remediated, the patch resource is already present in the Update Manager patch repository.

If Update Manager cannot download patches or extensions—for example, if it is deployed on an internal network segment that does not have Internet access—you can use VMware vCenter Update Manager Download Service to download and store patches and extensions on the machine on which it is installed so that the Update Manager server can use the patches and extensions later.

You can configure Update Manager to use an Internet proxy to download patches, extensions, and related metadata.

You can change the time interval at which Update Manager downloads patches, extensions, and metadata, or downloads binaries and metadata. You can also change the time interval at which Update Manager checks for notifications. For detailed descriptions of the procedures, see "Configure Checking for Patches," on page 74 and "Configure Notifications Checks," on page 75.

Importing Host Upgrade Release Files

You can upgrade the hosts in your environment by using host upgrade baselines. To create a host upgrade baseline, you must first upload host upgrade files to the Update Manager repository.

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

Each upgrade file that you upload contains information about the target version to which it will upgrade the host. Update Manager checks for these target versions and combines the uploaded files into host upgrade releases on the basis of the version to which they will upgrade the hosts in your environment. A host upgrade release is a combination of host upgrade files, which allows you to upgrade hosts to a particular release.

You can upload upgrade files and manage them from the **Host Upgrade Releases** tab of the Update Manager Administration view.

Upgrade files that you upload can be later included in host upgrade baselines. You cannot delete an upgrade release if it is included in a baseline. When you delete a host upgrade baseline you do not delete the upgrade releases included in it. Host upgrade release files that you import are kept in the Update Manager repository.

For more information about importing host upgrade release files and creating host upgrade baselines, see "Create a Host Upgrade Baseline," on page 90.

Creating Baselines and Baseline Groups

Baselines contain a collection of one or more patches, extensions, service packs, bug fixes, or upgrades, and can be classified as upgrade, extension, or patch baselines. Baseline groups are assembled from existing baselines. Baseline groups might contain a number of patch or extension baselines, and only one upgrade baseline per upgrade type (like VMware Tools, virtual machine hardware, virtual appliance, or host).

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, or create patch, extension, 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 21 and Chapter 12, "Working with Baselines and Baseline Groups," on page 83.

Attaching Baselines and Baseline Groups to vSphere Objects

To use baselines and baseline groups, you must attach them to selected inventory objects such as container objects, 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, vApps, 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 98.

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, extensions, and upgrades in the attached baselines or baseline groups, depending on the type of scan you select.

You can scan a host installation to determine whether the latest patches or extensions 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 perform patch scan on online as well as offline Microsoft Windows virtual machines and templates. Patch scans can be performed only on online Red Hat Linux virtual machines.
Host extensions scan	You can scan ESX 4.0 and later and ESXi 4.0 and later for extensions (additional software).
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.x and ESX/ESXi 4.1.
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. You should 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 hardware-upgrade scans on online as well as offline virtual machines and templates.
Virtual appliance upgrade scan	You can scan powered-on virtual appliances, that are created with VMware Studio 2.0 and later.

You can use VMware Studio 2.0 and later to automate the creation of ready-to-deploy vApps with pre-populated application software and operating systems. VMware Studio adds a network agent to the guest so that vApps bootstrap with minimal effort. Configuration parameters specified for vApps appear as OVF properties in the vCenter Server deployment wizard. For more information about VMware Studio, see the VMware SDK and API documentation for VMware Studio. For more information about vApp, you can also check the VMware blog site. You can download VMware Studio from the VMware Web site.

IMPORTANT Update Manager does not scan PXE booted ESXi hosts. A PXE booted installation of ESXi is completely stateless (it does not rely on the presence of a local disk). Therefore, the installation and post-install configuration are not persistent across reboot.

You can initiate scans on container objects, such as datacenters, clusters, vApps, 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. You should 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 13, “Scanning vSphere Objects and Viewing Scan Results,” on page 101.

Reviewing Scan Results

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

When you select a container object, you view the overall compliance status of the attached baselines, as well as all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

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 103.

Staging Patches and Extensions to Hosts

If you want to apply patches or extensions to the hosts in your environment, you can stage the patches and extensions before remediation to ensure that the patches and extensions are downloaded to the host. Staging patches and extensions is an optional step.

Staging patches and extensions to ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts allows you to download the patches and extensions from the Update Manager server to the ESX/ESXi hosts without applying the patches or extensions immediately. Staging patches and extensions speeds up the remediation process because the patches and extensions are already available locally on the hosts.

IMPORTANT Update Manager does not stage patches to PXE booted ESXi hosts.

For more information about staging patches, see "Stage Patches and Extensions to ESX/ESXi Hosts," on page 116.

Remediating Selected vSphere Objects

Remediation is the process in which Update Manager applies patches, extensions, 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.

Remediation also makes upgrade baselines compliant with the selected vSphere objects.

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 host, virtual machine, or virtual appliance, but you can also initiate remediation on a folder, cluster, or datacenter, or on all objects in your virtual infrastructure. As with scanning, resource pools are the only vSphere object type that can never be remediated.

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.
- Powered on, suspended, or powered off Microsoft Windows virtual machines and templates for patch remediation.
- Powered on virtual appliances, that are created with VMware Studio 2.0 and later, for virtual appliance upgrade.

- ESX/ESXi hosts for patch, extension, and upgrade remediation.

IMPORTANT Update Manager does not remediate PXE booted ESXi hosts. Update Manager skips PXE booted ESXi hosts when you remediate hosts in a container object, such as a folder.

After you upload host upgrade release files, upgrades for ESX/ESXi hosts are managed through baselines and baseline groups. Update Manager lets you upgrade ESX/ESXi 3.x hosts to ESX/ESXi 4.0 and later. In some upgrade scenarios, in case of failure, you can roll back the upgrades for ESX hosts. Update Manager supports rollback of ESX hosts when you upgrade hosts from version 3.x to versions 4.0.x and 4.1. For upgrades of ESX hosts from version 3.x to versions 4.0.x and 4.1, you can also set up custom postupgrade scripts to run after an upgrade. You use postupgrade scripts to automate the configuration of the ESX hosts after the upgrade, for example to assign the ports which the host will use. Update Manager supports postupgrade scripts in the Bash (`.sh`) and Python (`.py`) formats.

You can upgrade virtual appliances, VMware Tools, and the virtual hardware of virtual machines to a later version. Upgrades for virtual machines are managed through the Update Manager default virtual machine upgrade baselines. Upgrades for virtual appliances can be managed through both the Update Manager default virtual appliance baselines and custom virtual appliance upgrade baselines that you create.

With Update Manager 4.0 and later, 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.

Typically 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 and if VMware Distributed Resource Scheduler (DRS) and VMware Enhanced vMotion Compatibility (EVC) are enabled. EVC is not a prerequisite for vMotion. EVC guarantees that the CPUs of the hosts are compatible. For other containers or individual hosts that are not in a cluster, migration with vMotion cannot be performed.

You can remediate the objects in your vSphere inventory by using either manual remediation or scheduled remediation. For more information about manual and scheduled remediation, see Chapter 14, "Remediating vSphere Objects," on page 113.

Using Baselines and Baseline Groups

Baselines contain a collection of one or more updates such as service packs, patches, extensions, 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 on page 22

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

- Update Manager Default Baselines on page 23

  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.

- Baseline Groups on page 23

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

- Baseline Attributes on page 24

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

Baseline Types

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

Update Manager provides upgrade, patch, or extension baselines.

Upgrade Baseline Defines which version a particular host, virtual hardware, VMware Tools, or virtual appliance should be. With Update Manager, you can upgrade ESX/ESXi hosts from versions 3.x and 4.0.x to version 4.1.

Patch Baseline Defines a number of patches that must be applied to a given host or virtual machine.

Extension Baseline Contains extensions (additional software such as third-party device drivers) that must be applied to a given host. Extensions are installed on hosts that do not have such software installed on them, and patched on hosts that already have the software installed. All third-party software for ESX/ESXi hosts is classified as a host extension, although host extensions are not restricted to just third-party software.

At regular intervals, Update Manager queries patch 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 Patch Baseline The contents of a dynamic baseline are based on available patches that meet the specified criteria. As the set of available patches changes, dynamic baselines are updated as well. You can explicitly include or exclude any patches.

Fixed Patch Baseline The user manually specifies all patches included in the baseline from the total set of patches available in Update Manager. Fixed baselines 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 hosts that are running ESX/ESXi 4.0 and later.
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 hosts that are running ESX/ESXi 4.0 and later.
VA Upgrade to Latest	Checks virtual appliance compliance with the latest released 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 patch, extension, and upgrade baselines.

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

- Multiple patch and extension baselines.
- One upgrade baseline and multiple patch as well as extension baselines.

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

  For example, VMware Tools Upgrade to Match Host baseline, VM Hardware 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 as well as extension baselines.

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

Baseline Attributes

Baselines have baseline attributes that you can use to identify the baseline type, the patches or upgrades that 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 and extension baselines, 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 can 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, Host Extension, VM Patches, VMware Tools, VM Hardware, VA Upgrade, 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.
- How to handle failures to put hosts in maintenance mode.
- Whether to disable certain cluster features.
- Download patch binaries and patch metadata from the Internet or use a shared repository.
- Download patch binaries and patch metadata using an offline bundle.
- When to download notifications.
- Proxy usage and authentication.
- Enable or disable smart reboot of virtual appliances and virtual machines in a vApp after remediation.

System Requirements 2

To be able to run and use the Update Manager server and the Update Manager Client plug-in you must ensure that your environment satisfies certain conditions. You also must ensure that the vCenter Server, vSphere Client and Update Manager are of compatible versions.

Before you install Update Manager, you must set up an Oracle or Microsoft SQL Server database. If your deployment is relatively small and contains up to 5 hosts and 50 virtual machines, you can use the bundled 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 without registering Update Manager instances with them.

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. You should use a dedicated database for Update Manager, not a database shared with vCenter Server, and should 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, 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*.

Supported Operating Systems and Database Formats

Update Manager works with specific databases and operating systems.

The Update Manager server requires Windows XP, Windows Server 2003, or Windows Server 2008. The Update Manager plug-in requires the vSphere Client, and works with the same operating systems as the vSphere Client.

IMPORTANT You can install Update Manager 4.1 only on a 64-bit machine.

Update Manager scans and remediates Windows guest operating systems. Update Manager does not support patch remediation of Linux virtual machines and only scans powered-on Linux guest operating machines for patches. Update Manager scans and remediates Linux virtual machines for VMware Tools and virtual hardware upgrades.

The Update Manager server requires SQL Server 2005, SQL Server 2008, Oracle 10g, or Oracle 11g database. Update Manager can handle small-scale environments using the bundled SQL Server 2005 Express. For environments with more than 5 hosts and 50 virtual machines, create either an Oracle or a SQL Server database for Update Manager. For large scale environments, you should set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database. For more information about setting up the Update Manager database, see Chapter 3, "Preparing the Update Manager Database," on page 29.

For detailed information about supported operating systems and database formats, see *vSphere Compatibility Matrixes*.

Update Manager Compatibility with VirtualCenter Server, vCenter Server, VI Client, and vSphere Client

Update Manager, VirtualCenter Server, and vCenter Server must be of compatible versions. You can install the Update Manager server and register it with VirtualCenter Server or vCenter Server of a compatible version only. The Update Manager plug-in can be installed and enabled only on VI Client or vSphere Client of a compatible version.

Generally, Update Manager is compatible with VirtualCenter Server, vCenter Server, VI Client, and vSphere Client of the same version.

Update Manager 4.1 is compatible only with vCenter Server 4.1. Although multiple versions of the Update Manager Client plug-in might coexist on the same computer, the Update Manager Client plug-in of version 4.1 can be installed and enabled only on vSphere Client 4.1.

For more information about the Update Manager compatibility with VirtualCenter Server, vCenter Server, VI Client, and vSphere Client, see the *vSphere Compatibility Matrixes.*

Required Database Privileges

Before you install or upgrade Update Manager, you must create a database and grant a specific list of permissions to the database user. To run Update Manager you can use a set of minimum privileges.

Table 2-2 lists the database privileges that you must grant to the database user before installing or upgrading Update Manager.

Table 2-2. Database Privileges Needed for Installation or Upgrade of Update Manager

Database	Permissions
Oracle	Either assign the DBA role, or grant the following set of privileges to the Update Manager Oracle database user. ■ **connect** ■ **execute on dbms_lock** ■ **create view** ■ **create procedure** ■ **create table** ■ **create sequence** ■ **create any sequence** ■ **create any table** ■ **create type** ■ **unlimited tablespace**
Microsoft SQL Server	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 or upgrade.

Table 2-3 lists the minimum database privileges required to run and use Update Manager.

Table 2-3. Database Privileges Needed for Using Update Manager

Database	Privileges
Oracle	The minimum required privileges of the Oracle database user are the following: ■ **create session** ■ **create any table** ■ **drop any table**
Microsoft SQL Server	The database user must have either a **sysadmin** server role or the **db_owner** fixed database role on the Update Manager database and the MSDB database.

Preparing the Update Manager Database

3

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 the Update Manager server, you must create a database instance and configure it to ensure that all Update Manager database tables can be created in it. If you are using Microsoft SQL Server 2005 Express, you can 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 Microsoft SQL Server and Oracle databases, you must configure a 32-bit system DSN and test it with ODBC.

IMPORTANT Although you can install the Update Manager server only on 64-bit machines, Update Manager is a 32-bit application and requires a 32-bit DSN.

The Update Manager database you use can be the same as the vCenter Server database. You can also use a separate database, or you can use existing database clusters. For best results in a large scale environment, you should use a dedicated Update Manager database that is located on a different computer than the vCenter Server system database.

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

Before you begin the database setup, review the supported databases. For more information about the supported database patches, see *vSphere Compatibility Matrixes*. If you do not prepare your database correctly, the Update Manager installer might display error or warning messages.

This chapter includes the following topics:

Create a 32-Bit DSN on a 64-Bit Operating System

You can install or upgrade the Update Manager server on 64-bit operating systems. Even though Update Manager runs on 64-bit operating systems, it is a 32-bit application and requires a 32-bit DSN.

The requirement for a 32-bit DSN applies to all supported databases. By default, any DSN created on a 64-bit system is a 64-bit DSN.

Procedure

1 Install the ODBC drivers.

- For Microsoft SQL Server database servers, install the 64-bit database ODBC drivers on your Microsoft Windows system. When you install the 64-bit drivers, the 32-bit drivers are installed automatically.
- For Oracle database servers, install the 32-bit database ODBC drivers on your Microsoft Windows system.

2 Run the 32-bit ODBC Administrator application, located at *[WindowsDir]*\SysWOW64\odbcad32.exe.

3 Use the application to create your DSN.

You now have a DSN that is compatible with the Update Manager server. When the Update Manager installer prompts you for a DSN, you should select the 32-bit DSN.

About the Bundled Microsoft SQL Server 2005 Express Database Package

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 server 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.

Configure a Microsoft SQL Server Database Connection

When you install Update Manager, you can establish an ODBC connection with a SQL Server database.

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

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

Procedure

1 Create a SQL Server database by using SQL Server Management Studio on SQL Server.

The Update Manager installer creates all tables, procedures, and user-defined functions (UDF) within the default schema of the database user that you use for Update Manager. This default schema does not necessarily have to be dbo schema.

2 Create a SQL Server database user with database operator (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, run the 32-bit ODBC Administrator application, located at *[WindowsDir]*\SysWOW64\odbcad32.exe.

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 that you want to modify.

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

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.

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

5 Configure the SQL Server authentication, and click **Next**.

- If you are using a local SQL Server, you can select **Integrated Windows NT authentication**.
- If you are using a remote SQL Server, you must use the SQL Server authentication method.

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, where to save 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 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.

Identify the SQL Server Authentication Type

You can identify whether your 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.

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 32-bit system DSN. For more information about creating a 32-bit DSN, see "Create a 32-Bit DSN on a 64-Bit Operating System," on page 29.

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 the **dba** permission to the user, or grant the following specific permissions to the user.

```
grant connect to vumAdmin
grant resource to vumAdmin
grant create any job to vumAdmin
grant create view to vumAdmin
grant create any sequence to vumAdmin
grant create any table to vumAdmin
grant lock any table to vumAdmin
grant create procedure to vumAdmin
grant create type to vumAdmin
grant execute on dbms_lock to vumAdmin
grant unlimited tablespace to vumAdmin
# 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.

Prerequisites

The ODBC data source you use must be a 32-bit system DSN. For more information about creating a 32-bit DSN, see "Create a 32-Bit DSN on a 64-Bit Operating System," on page 29.

Before configuring a remote connection, first set up the database as described in "Configure an Oracle Database," on page 32.

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
```

Installing Update Manager 4

Update Manager consists of a server part and a plug-in part. You can install the Update Manager server and Update Manager Client plug-in on Windows machines only.

You can install the Update Manager server component either 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.

IMPORTANT You can install the Update Manager 4.1 server component only on a 64-bit machine.

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

To install Update Manager, you must be either a local Administrator or a domain user that is part of the Administrators group. During the Update Manager installation, you must register the Update Manager server with the vCenter Server system and set it up to work correctly. To register Update Manager with vCenter Server, you must provide the credentials of the vCenter Server user that has the **Register extension** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Datacenter Administration*.

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

The Update Manager server requires SQL Server 2005, SQL Server 2008, Oracle 10g, or Oracle 11g database. Update Manager can handle small-scale environments using the bundled SQL Server 2005 Express. For environments with more than 5 hosts and 50 virtual machines, create either an Oracle or a SQL Server database for Update Manager. For large scale environments, you should set up the Update Manager database on a different computer than the Update Manager server and the vCenter Server database. For more information about setting up the Update Manager database, see Chapter 3, "Preparing the Update Manager Database," on page 29.

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 the following information about the environment in which you are installing Update Manager:

- 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 port 80 is 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, the Update Manager server connects to vCenter Server, ESX/ESXi hosts, and the 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.

You can install vCenter Server and the Update Manager server in a heterogeneous network environment, where one of the machines is configured to use IPv6 and the other is configured to use IPv4. In this case, to install and enable the Update Manager plug-in, the machine on which vSphere Client is installed must be configured to use both IPv6 and IPv4.

This chapter includes the following topics:

Install the 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.

Prerequisites

- Make sure that your system meets the requirements specified in Chapter 2, "System Requirements," on page 25.
- Before installation, you must create and set up an Update Manager database and 32-bit DSN, unless you are using SQL Server 2005 Express. For more information, see Chapter 3, "Preparing the Update Manager Database," on page 29.
- Ensure that the database privileges meet the requirements listed in "Required Database Privileges," on page 27.
- Before installing Update Manager, install vCenter Server. For more information about installing vCenter Server, see the *ESX and vCenter Server Installation Guide*.

Procedure

1. Insert the installer DVD into the DVD 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 DVD and run `VMware-UpdateManager.exe`.
2. Select a language for the installer and click **OK**.
3. Review the Welcome page and click **Next**.
4. Read the patent agreement and click **Next**.
5. Accept the terms in the license agreement and click **Next**.
6. Enter the vCenter Server IP address or name, HTTP port, and the administrative account that the Update Manager server will use to connect to the vCenter Server system, and click **Next**.

7 Select the type of database that you want to use.

- If you do not have an existing database, select **Install a Microsoft SQL Server 2005 Express instance (for small scale deployments)** and click **Next**.

  This database is suitable for 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. If the DSN does not use Windows NT authentication, enter the user name and password for the DSN and click **Next**.

  IMPORTANT The DSN must be a 32-bit DSN.

8 (Optional) Select the database options.

- 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.
- If the system DSN you enter points to an older schema, 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.**

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

  If the computer on which you install Update Manager has one NIC, the Update Manager installer automatically detects the IP address. If the computer has multiple NICs, 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 (Optional) In the warning message about the disk free space, click **OK**.

  This message appears when you try to install Update Manager on a computer that has less than 20GB free space.

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

15 Click **Finish**.

The Update Manager server component is installed, and the client appears in the Available Plug-ins list of vSphere Plug-in Manager.

What to do next

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

Install the Update Manager Client Plug-In

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 can install the Update Manager Client plug-in on both 32-bit and 64-bit operating systems.

Prerequisites

Before installing the Update Manager Client plug-in, you must install the Update Manager server.

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 status for the Update Manager extension is displayed as Enabled.

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

Installing the Guest Agent 5

The VMware vCenter Update Manager Guest Agent facilitates the 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 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 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 on the guest operating system.

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

For best results of Update Manager operations, ensure that the latest version of the Guest Agent is installed on a virtual machine.

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 (x86)\VMware\Infrastructure\Update Manager`, the Guest Agent installers are in `C:\Program Files (x86)\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.

Migrating the Update Manager Data and Upgrading Update Manager on a Different Machine

6

You can install Update Manager 4.1 only on 64-bit operating system platform. If you are running an earlier version of Update Manager on a 32-bit platform, you can use the data migration tool to back up the existing data on the 32-bit system, and to restore your data on the 64-bit machine on which you are installing Update Manager 4.1.

The Update Manager installation media includes a data migration tool that you can use to migrate your existing configuration information and database. The configuration information that you can migrate includes the following parameters:

- Port settings
- Proxy settings
- Patch repository location
- Patch metadata, patch binaries, and host upgrade binaries

You can use the data migration tool to migrate the Update Manager database if it is a SQL Server Express database installed on the same machine as Update Manager.

If you use a different database (for example, Oracle or Microsoft SQL Server database) installed on the Update Manager machine, you can back up and move the database manually or you can detach the database from the source (32-bit) machine and attach it to the destination (64-bit) machine. You can also leave the database on the existing machine and connect to it from the new 64-bit machine by using a DSN.

If your database is installed on a different machine from the Update Manager server, you can back up the database manually, and create a DSN to connect to the database remotely.

When Update Manager and vCenter Server are installed on the same machine, you can use the data migration tool to migrate configuration data for vCenter Server as well. The data migration tool first backs up the vCenter Server data and then backs up the Update Manager data on the source machine. When you run the tool to restore the data, the data migration tool first restores the vCenter Server data on the destination machine and then restores the Update Manager data on the same destination machine.

When Update Manager and vCenter Server are installed on the same machine, Update Manager and vCenter Server must use dedicated databases. If the Update Manager server shares its database with the vCenter Server database, you receive an error message from the data migration tool and you cannot migrate your data.

If Update Manager and vCenter Server are installed on different machines, you can use the data migration tool to separately back up and restore the Update Manager and vCenter Server data. First you can back up the vCenter Server data and restore it on the 64-bit machine on which you are installing vCenter Server. Then you can use the data migration tool to back up the Update Manager data and restore it on the 64-bit machine on which you are installing Update Manager. In this case, the machine on which you install Update Manager must be different from the machine on which you install vCenter Server. For more information about backing up and restoring the vCenter Server configuration and database, see the *vSphere Upgrade Guide*.

You use the data migration tool by running two scripts `backup.bat` and `install.bat`. The `backup.bat` script backs up the configuration and database on the source machine, and the `install.bat` script restores the backed up data on the destination machine.

The overall scenario to migrate your Update Manager data includes the following steps:

1 (Optional) Back up the database manually.

2 Run the `backup.bat` script of the data migration tool on the source machine and respond to the script prompts to create a backup of the Update Manager configuration.

   If Update Manager and vCenter Server are installed on the same machine, the script first takes a backup of the vCenter Server configuration and then backs up the Update Manager configuration.

3 Copy the backed up configuration data to the destination machine. Database data in the backup bundle is present only if your database is SQL Server Express.

4 (Optional) If you are using a different database, for example Oracle database, installed on a different machine than Update Manager, back up the database manually and create a DSN on the 64-bit machine to connect to the database remotely.

5 (Optional) If you are using a different database, for example Oracle database, installed on the same machine as Update Manager, move the database from the source (32-bit) machine to the destination (64-bit) machine and restore it manually.

6 If your database is not SQL Server Express, create a 32-bit DSN on the 64-bit machine to connect to the database.

7 Run the `install.bat` script on the destination machine. This script examines the backup bundle and if you have backed up both Update Manager and vCenter Server data, the script installs both Update Manager and vCenter Server. If you have backed up only Update Manager or only vCenter Server data, the script installs only Update Manager or only vCenter Server. When the script prompts you, specify the location of the installation ISO. The script launches the installer, and you can install Update Manager, or both Update Manager and vCenter Server with the configuration settings and the database backed up by the data migration tool.

In case of failure, you can check the `logs` folder. The folder contains `backup.log` file for the backup process and `restore.log` for the restore process.

This chapter includes the following topics:

Back Up and Move the Update Manager Database

Before upgrading Update Manager, back up your database. If the Update Manager server is installed on a 32-bit machine, you must migrate your data to a 64-bit machine.

Procedure

- If your database is remote from the machine on which Update Manager is installed, and you want it to remain remote after the upgrade, leave the database where it is after you back it up.

- If your database is local to the Update Manager server, and you want it to remain local after the upgrade, you have various options depending on the type of database.

Option	Description
Microsoft SQL Server Express database	Back up the database, and move the database along with other configuration data by using the data migration tool. A separate database migration step is not necessary.
Microsoft SQL Server database	Back up the database, detach the database, and attach it to the 64-bit machine on which you are installing Update Manager.
Other local databases	Back up the database, and restore it onto the machine on which you are installing Update Manager.

What to do next

Back up the Update Manager configuration and database by using the data migration tool.

Back Up and Restore a Microsoft SQL Database

You can back up the Update Manager database and then restore it on the same or another machine. Backing up the Update Manager database helps you preserve your data. Before you perform an upgrade to Update Manager 4.1, you might want to back up the Update Manager database so that you can restore it later.

Consult your database administrator or see your database documentation about backing up and restoring databases.

The machine with the original database that you want to back up is referred to as the source machine. The machine on which the backup of the database will reside is referred to as the destination machine.

Prerequisites

- You must have an Update Manager system running with a local or remote Microsoft SQL Server database.
- You must have Microsoft SQL Server Management Studio installed on the source machine and the destination machine. The Express versions (`SQLServer2005_SSMSEE.msi` and `SQLServer2005_SSMSEE_x64.msi`) are free downloads from Microsoft.

Procedure

1. In SQL Server Management Studio, make a full backup of the source machine database.
2. Copy the backup file (`.bak`) to the `C:\` drive on the destination machine.
3. On the destination machine, open SQL Server Management Studio and right-click the **Databases** folder.
4. Select **New Database**, enter the source machine database name, and click **OK**.
5. Right-click the new database icon and select **Task > Restore > Database**.
6. Select **From Device** and click **Browse**.
7. Click **Add**, navigate to the backup file, and click **OK**.
8. In the Restore Database window, select the checkbox next to your `.bak` file.
9. On the Options page, select the **Overwrite the existing database** checkbox and click **OK**.

The database from the source machine is restored on the destination machine.

What to do next

See "Create a 32-Bit DSN on a 64-Bit Operating System," on page 46.

Detach and Attach a Microsoft SQL Server Database

You can detach the Update Manager database from a source machine and attach it to a destination machine. This is an alternative to the backup and restore operation.

Consult your database administrator or see your database documentation about detaching and attaching databases. You should take the necessary steps to back up your data.

The machine with the original database that you want to detach is referred to as the source machine. The machine on which the database will be reattached is referred to as the destination machine.

Prerequisites

- You must have an Update Manager system running with a local or remote Microsoft SQL Server database.
- You must have Microsoft SQL Server Management Studio installed on the source machine and the destination machine. The Express versions (`SQLServer2005_SSMSEE.msi` and `SQLServer2005_SSMSEE_x64.msi`) are free downloads from Microsoft.

Procedure

1. On the source machine, stop the Update Manager service.
   a. Click **Start > Control Panel > Administrative Tools > Services**.
   b. Right-click **VMware Update Manager Service** and select **Stop**.
2. In SQL Server Management Studio, open the **Databases** directory, right-click the Update Manager database, and select **Tasks > Detach**.
3. Select the database and click **OK**.
4. When the detach operation is complete, copy the data files (`.mdf` and `.ldf`) to the destination machine's database folder.

   The default location of the database folder in 64-bit Windows is `C:\Program Files (x86)\Microsoft SQL Server\MSSQL.1\MSSQL\Data`.
5. In SQL Server Management Studio on the destination machine, right-click the **Databases** directory and select **Attach**.
6. Select the `.mdf` file that you copied to the destination machine's database folder and click **OK**.

The database from the source machine is attached to the destination machine.

What to do next

See "Create a 32-Bit DSN on a 64-Bit Operating System," on page 46.

Back Up and Restore an Oracle Database

You can back up the Update Manager database and then restore it on the same or another machine. Backing up the Update Manager database helps you preserve your data.

Consult your database administrator or see your database documentation about backing up and restoring databases.

The machine with the original database that you want to back up is referred to as the source machine. The machine on which the backup of the database will reside is referred to as the destination machine.

Prerequisites

You must have an Update Manager system with a local or remote Oracle 10g or Oracle 11g database.

Procedure

1 On the source machine, log in to Oracle SQL*Plus as the Update Manager database user and export the database as a `.dmp` file.

2 Copy the `.dmp` file to the `C:\` drive of the destination machine.

3 Create a new empty database on the destination machine.

4 On the destination machine, in Oracle SQL*Plus, run the following command to create the tablespace.

```
create tablespace vumtest datafile 'c:\vumtest.dbf' size 100m autoextend on;
```

5 On the destination machine, create a user and grant the user either the **dba** permission, or the set of permissions required for administering an Update Manager database.

```
create user VUMUSER identified by CENSORED default tablespace vumtest;
```

6 Import the `.dmp` file into the Oracle database on the destination machine.

The database from the source machine is restored on the destination machine.

What to do next

See "Create a 32-Bit DSN on a 64-Bit Operating System," on page 46.

Back Up and Migrate the Existing Configuration and Database Using the Migration Tool

You can use the migration tool to migrate your Update Manager configuration data and database.

If your database is a SQL Server Express database that is local to the machine on which Update Manager is installed, the data migration tool backs up the configuration and the database, and restores it to the new machine.

Prerequisites

- The Update Manager database must be a SQL Server Express database installed on the same machine as Update Manager.
- If Update Manager server and vCenter Server are installed on the same machine, they must use dedicated databases (that means that the servers must not share one database instance).
- Stop the Update Manager service.

Procedure

1 Log in as an administrator to the source machine and insert the Update Manager installation media in the DVD drive of the source machine.

2 Explore the media to locate and open the `datamigration` folder.

3 Extract the `datamigration.zip` file to a writeable filesystem (for example, `datamigration` folder) on the source machine.

4 From the Windows command prompt, navigate to the `datamigration` folder, type **`backup.bat`**, and press Enter to run the backup script of the data migration tool.

5 Wait until the script backs up the Update Manager configuration and database, upgrades the database, and restores the original database.

6 Enter **`y`** to back up the available host patches, and press Enter.

The time to back up the host patches and host upgrade files (if any) depends on the size of the patches, extensions, and upgrade files.

7 Enter **y** to back up the available virtual machine patches, and press Enter.

The time to back up the virtual machine patches depends on the size of downloaded patches.

8 Respond to the script prompts and wait until the script completes.

The Update Manager configuration data and database are successfully backed up.

In case of failure, examine the log file that the script generates. This is the `backup.log` file located in the `datamigration\logs` folder.

What to do next

- If your database is a SQL Server Express database local to the Update Manager machine, go to "Restore the Update Manager Configuration and Install Update Manager on the 64-Bit Machine," on page 46.
- If you use another database, go to "Create a 32-Bit DSN on a 64-Bit Operating System," on page 46.

Create a 32-Bit DSN on a 64-Bit Operating System

You can install or upgrade the Update Manager server on 64-bit operating systems. Even though Update Manager runs on 64-bit operating systems, it is a 32-bit application and requires a 32-bit DSN.

The requirement for a 32-bit DSN applies to all supported databases. By default, any DSN created on a 64-bit system is a 64-bit DSN.

Procedure

1 Install the ODBC drivers.

- For Microsoft SQL Server database servers, install the 64-bit database ODBC drivers on your Microsoft Windows system. When you install the 64-bit drivers, the 32-bit drivers are installed automatically.
- For Oracle database servers, install the 32-bit database ODBC drivers on your Microsoft Windows system.

2 Run the 32-bit ODBC Administrator application, located at *[WindowsDir]*`\SysWOW64\odbcad32.exe`.

3 Use the application to create your DSN.

You now have a DSN that is compatible with the Update Manager server. When the Update Manager installer prompts you for a DSN, you should select the 32-bit DSN.

Restore the Update Manager Configuration and Install Update Manager on the 64-Bit Machine

You can use the data migration tool to start the Update Manager installer and restore the Update Manager configuration and database on the 64-bit machine.

You can use the same host name for the destination machine that was used for the source machine.

If you use the tool to back up a SQL Server Express database that is local to the machine on which Update Manager is installed, the migration tool restores the database to the new 64-bit machine as well.

Procedure

1 Copy the `datamigration` folder from the source (32-bit) machine to the destination (64-bit) machine.

2 Insert the Update Manager installation media into the DVD-ROM drive on the destination machine, or copy the installation ISO image to the destination machine.

3 From the Windows command prompt, navigate to the `datamigration` folder copied from the source machine and run **`install.bat`**.

The script imports the backed up configuration data and the database.

4 Enter the path to the Update Manager installer.

The install script verifies that migration data is present, and launches the Update Manager installer.

5 Select a language for the installer and click **OK**.

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

7 Read the patent agreement and click **Next**.

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

9 Enter the vCenter Server IP address or name, HTTP port, and the administrative account that the Update Manager server will use to connect to the vCenter Server system, and click **Next**.

10 Select the type of database that you want to use.

- If you used the bundled SQL Express database on the source machine and you want to install and import the backed up database, click **Install SQL Server 2005 Express instance (for small-scale deployments)**.
- If you want to use an existing non-bundled database, click **Use an existing supported database**, select the DSN that was used for the database on the source machine, enter the user name and password for the DSN, and click **Next**.

  The database user name and password for the DSN are required only if the DSN uses SQL Server authentication. Update Manager does not support the use of a remote SQL Server database that uses Windows NT authentication.

11 (Optional) Select the database options.

- 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.
- If the system DSN you enter points to an older schema, 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.**

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

If the computer on which you install Update Manager has one NIC, the Update Manager installer automatically detects the IP address. If the computer has multiple NICs, 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.

13 Enter the port numbers to use or accept the port numbers shown, specify whether you want to configure the proxy settings, and click **Next**.

The port numbers displayed are those that were backed up from the source Update Manager installation.

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

15 Select the Update Manager installation and patch download locations and click **Next**.

The location for downloading patches is the one, that was backed up from the source Update Manager installation.

16 (Optional) In the warning message about the disk free space, click **OK**.

This message appears when you try to install Update Manager on a computer that has less than 20GB free space.

17 Click **Install**.

18 When the Update Manager installation is completed, click **Finish**.

The data migration tool restores the backed up configuration data.

Update Manager is installed, and the settings that you backed up are restored. If you migrated a SQL Server Express database, and selected to install this database during the Update Manager installation, the database is also restored on the new machine. After the installation is complete, Update Manager service is started.

In case of failure examine the log file that the script generates. This is the `restore.log` file located in the `datamigration\logs` folder.

Upgrading Update Manager 7

You can upgrade Update Manager 1.0 and later to Update Manager 4.1.

You can install Update Manager 4.1 only on 64-bit operating system platform. If you are running an earlier version of Update Manager on a 32-bit platform, you must either back up or database manually, or you can use the data migration tool to back up the existing data on the 32-bit machine, and to restore your data on the 64-bit machine on which you are installing Update Manager 4.1. For more information about how to use the data migration tool to migrate your data and install Update Manager, see Chapter 6, "Migrating the Update Manager Data and Upgrading Update Manager on a Different Machine," on page 41.

During the Update Manager upgrade process, the `vci-integrity.xml` is overwritten. Any changes that you might have made to the following parameters in the `vci-integrity.xml` file are not lost during the upgrade.

- vCenter Server host and port settings – The IP address of the computer on which vCenter Server is installed and the port that 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 address of the computer on which Update Manager server is installed. These settings can be configured using the `<PatchDepotUrl>` tag. If there is no such a setting, the ESX/ESXi hosts use the Update Manager server and Web server port as a URL 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. This setting can be configured using the `<PatchDepotProxyUrl>` tag. If no value is specified, Update Manager uses the proxy server in the proxy settings to download host patches.
- 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 4.1, the value in the `<PatchMetadataDownloadUrl>` tag is moved to the `<ESX3xUpdateUrl>` tag.

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

This chapter includes the following topics:

Upgrade the Update Manager Server

When you upgrade Update Manager, you must first upgrade VirtualCenter Server or vCenter Server to a compatible version, and then upgrade Update Manager..

This upgrade scenario is for upgrading from an earlier Update Manager version installed on a 64-bit machine.

Prerequisites

- Before upgrading Update Manager, ensure that you grant the database user the required list of privileges. For more information, see "Required Database Privileges," on page 27.
- Before upgrading, make sure that you created a 32-bit DSN on the 64-bit operating system. For more information about creating a 32-bit DSN on a 64-bit operating system, see "Create a 32-Bit DSN on a 64-Bit Operating System," on page 29.
- Before upgrading Update Manager, stop the Update Manager service and back up the Update Manager database. The installer upgrades the database schema, making the database irreversibly incompatible with previous Update Manager versions.

Procedure

1 Upgrade VirtualCenter Server or vCenter Server to a compatible version.

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

2 Insert the installer DVD in the DVD 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 Read the patent agreement and click **Next**.

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

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

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

9 Enter the database password for the Update Manager database and click **Next**.

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

10 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**.

You should create a backup copy of the existing database before proceeding with the upgrade.

11 (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 choose to replace your existing database with an empty one, you lose all of your existing data.

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

   Configure the proxy settings if the computer on which Update Manager is installed has access to the Internet.

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

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

15 Click **Finish**.

You upgraded the Update Manager server.

What to do next

Upgrade the Update Manager Client plug-in.

Upgrade the Update Manager Client Plug-In

The Update Manager server and the Update Manager Client plug-in must be of the same version.

Prerequisites

Before upgrading the Update Manager Client plug-in, you must upgrade the Update Manager server.

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 status for the Update Manager extension is displayed as Enabled.

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

Update Manager Best Practices and Recommendations

8

You can install Update Manager on the same computer as the vCenter Server system or on a different computer.

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 "Update Manager Compatibility with VirtualCenter Server, vCenter Server, VI Client, and vSphere Client," on page 26.

Update Manager has two deployment models:

- Internet-connected model - The Update Manager server has connectivity to the VMware patch repository, Shavlik, and third-party patch repositories (for ESX/ESXi 4.0.x and ESX/ESXi 4.1 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, you can use UMDS to download patch metadata and patch binaries and store them in a shared repository. You can configure the Update Manager server to use a shared repository of UMDS data as a patch datastore to scan and remediate the objects that you select from the inventory. For more information about using UMDS, see Chapter 10, "Installing, Setting Up, and Using Update Manager Download Service," on page 59.

You should not install Update Manager or vCenter Server on a virtual machine that is managed by the same vCenter Server system, if the host that is running the virtual machine is not in a DRS cluster. In such a case, if you try to remediate the host, Update Manager does not remediate the host, to make sure that the virtual machine running Update Manager or vCenter Server is not suspended or shut down during the remediation. If the host on which the virtual machine is running is in a DRS cluster, and you start a remediation task on the host, DRS attempts to migrate the virtual machine to another host, so that the remediation succeeds. If DRS cannot migrate the virtual machine running Update Manager or vCenter Server, the remediation fails. Remediation failure occurs even if you have selected to power off or suspend the virtual machines on the host, in case the host fails to enter maintenance mode.

This chapter includes the following topics:

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 8-1.

Table 8-1. 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.

- 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 residing on a separate machine.

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

For more information about the Update Manager best practices and recommendations, see *VMware vCenter Update Manager Performance and Best Practices*.

Uninstalling Update Manager 9

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 Update Manager Client plug-in can be uninstalled separately.

This chapter includes the following topics:

Uninstall the 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. All downloaded metadata and binaries, as well as log data remain on the machine where Update Manager was installed.

Uninstall the Update Manager Client Plug-In

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 4.1** and click **Remove**.

After you uninstall the Update Manager plug-in, the Update Manager icon is no longer available in the vSphere Client.

Installing, Setting Up, and Using Update Manager Download Service 10

VMware vCenter Update Manager Download Service (UMDS) is an optional module of Update Manager. UMDS downloads patch metadata, patch binaries, and notifications that would not otherwise be available to the Update Manager server.

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 a semi-air-gap deployment (where the machine on which Update Manager is installed has no Internet access, but is connected to a server that has Internet access), you can automate the export process and transfer files from UMDS to the Update Manager server by using a Web server on the machine on which UMDS is installed.

UMDS 4.1 supports patch recalls and notifications. A patch is recalled if the released patch has problems or potential issues. After you download patch data and notifications with UMDS, and export the downloads so that they become available to the Update Manager server, Update Manager deletes the recalled patches and displays the notifications on the Update Manager **Notifications** tab. For more information about patch recalls and notifications, see "Configuring Notification Checks and Viewing Notifications," on page 75.

This chapter includes the following topics:

Installing and Upgrading UMDS

You can install and use UMDS to download patch binaries, patch metadata, and notifications if Update Manager does not have access to the Internet. The machine on which you install UMDS must have Internet access.

IMPORTANT You can install UMDS on both 32-bit and 64-bit machines.

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 32-bit DSN and test the DSN from ODBC. If you are using Microsoft SQL Server 2005 Express, you can install and configure the database when you install UMDS.

The amount of space required to store the patches and notifications 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/ESXi patching, and 11GB for each virtual machine operating system and locale combination.

Compatibility Between UMDS and the Update Manager Server

UMDS must be of a version that is compatible with the Update Manager server.

Update Manager can work with a certain UMDS version if the metadata and structure of the patch store that UMDS exports is compatible with Update Manager, and if the data can be imported and used by the Update Manager server.

For information on which versions are compatible, see Table 10-1.

Table 10-1. Compatibility Between UMDS and the Update Manager Server

Update Manager Server	Update Manager Download Service									
	1.0	1.0 Update 1	1.0 Update 2	1.0 Update 3	1.0 Update 4	1.0 Update 6	4.0	4.0 Update 1	4.0 Update 2	4.1
1.0	Yes	No	No	No	No	No	No	No	No	No
1.0 Update 1	No	Yes	No	No	No	No	No	No	No	No
1.0 Update 2	No	No	Yes	No	No	No	No	No	No	No
1.0 Update 3	No	No	No	Yes	No	No	No	No	No	No
1.0 Update 4	No	No	No	No	Yes	No	No	No	No	No
1.0 Update 6	No	No	No	No	No	No	No	No	No	No
4.0	No	No	No	No	No	No	Yes	Yes	Yes	Yes
4.0 Update 1	No	No	No	No	No	No	Yes	Yes	Yes	Yes
4.0 Update 2	No	No	No	No	No	No	Yes	Yes	Yes	Yes
4.1	No	No	No	No	No	No	No	No	No	Yes

Install UMDS

Install UMDS if the machine on which Update Manager is installed does not have access to the Internet.

Prerequisites

- Ensure that the machine on which you install UMDS has Internet access, so that UMDS can download patch metadata and patch binaries.
- Uninstall UMDS 1.0.x, if it is installed on the machine. If such a version of UMDS is already installed, the installation wizard displays an error message and the installation cannot proceed.
- Before you install UMDS create a database instance and configure it. If you install UMDS on 64-bit machine, you must configure a 32-bit DSN and test it from ODBC. The database privileges and preparation steps are the same as the ones used for Update Manager. For more information, see Chapter 3, "Preparing the Update Manager Database," on page 29.
- UMDS and Update Manager must be installed on different machines.

Procedure

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

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

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

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

5 Read the patent agreement and click **Next**.

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

7 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)**.
- If you want to use an existing database, select **Use an existing supported database** and select your database from the list of DSNs. If the DSN does not use Windows NT authentication, enter the user name and password for the DSN and click **Next**.

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

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

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

10 In the warning message about the disk free space, click **OK**.

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

12 Click **Finish**.

UMDS is installed.

Upgrade UMDS

You can upgrade UMDS 4.0 to UMDS 4.1. You cannot upgrade from UMDS 1.0.x versions to UMDS 4.1. The patches you download with UMDS 1.0.x cannot be reused by UMDS 4.1.

To avoid losing the UMDS configuration settings during the upgrade, the best practice is to upgrade UMDS from version 4.0 to version 4.1 and then re-configure the UMDS settings. To preserve your UMDS configuration settings, you can also back up the `downloadConfig.xml` file before the upgrade, upgrade UMDS, and then restore the backed up `downloadConfig.xml` file.

To use UMDS 4.1, you must first uninstall UMDS 1.0.x, if it is present on the machine. Before you uninstall UMDS 1.0.x, import the downloaded patch data into Update Manager 1.0.x by using `vmware-updateDownloadCli.exe`. You can then uninstall UMDS 1.0.x, install UMDS 4.1, and upgrade Update Manager.

Prerequisites

You should create a backup copy of the existing UMDS database before proceeding with the upgrade. The upgrade makes the database incompatible with older UMDS and Update Manager versions.

Procedure

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

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

3 Click **OK** in the message warning you that an upgrade will be performed.

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

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

6 Enter your database information and click **Next**.

The database user name and password are required, if your DSN does not use Windows NT authentication.

7 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**.

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

9 Click **Finish**.

UMDS is upgraded to UMDS 4.1.

Setting Up and Using UMDS

You can set up UMDS to download patches for Windows or Linux virtual machines, or patches and notifications for ESX/ESXi hosts. You can also set up UMDS to download ESX/ESXi 4.0.x and ESX/ESXi 4.1 patch binaries, patch metadata, and notifications from third-party portals.

After you download the patch binaries, patch metadata, and notifications, you can export the data to a Web server or a portable media drive and set up Update Manager to use a folder on the Web server or the media drive (mounted as a local disk) as a shared repository.

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

- ESX 3i or later, and ESX 3.5 or later
- All Update Manager supported versions of Windows virtual machines
- All Update Manager supported versions of Linux virtual machines (only patch metadata, but not patch binaries)

You can also set up UMDS to download ESX/ESXi 4.0.x and ESX/ESXi 4.1 patches and notifications from third-party portals.

To use UMDS, the machine on which you install it must have Internet access. After you download the patch binaries, patch metadata, and notifications, you can copy them to a local Web server or a portable storage device, such as a CD or USB flash drive.

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.

Set Up Which Patches to Download with UMDS

By default UMDS downloads patch binaries, patch metadata, and notifications for hosts. You can specify which patch binaries and patch metadata to download with UMDS.

Procedure

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

2 Navigate to the directory where UMDS is installed.

- The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Specify the updates to download.

- To set up a download of all ESX/ESXi host updates, run the following command:

  ```
  vmware-umds --set-config --enable-host 1 --enable-win 0 --enable-lin 0
  ```

- To set up a download of all Windows updates, run the following command:

  ```
  vmware-umds --set-config --enable-host 0 --enable-win 1 --enable-lin 0
  ```

- To set up a download of all Linux updates, run the following command:

  ```
  vmware-umds --set-config --enable-host 0 --enable-win 0 --enable-lin 1
  ```

- To set up a download of all available updates, run the following command:

  ```
  vmware-umds --set-config --enable-host 1 --enable-win 1 --enable-lin 1
  ```

What to do next

Download the selected data.

Change the UMDS Patch Repository Location

UMDS downloads patch binaries, patch metadata, and notifications to a folder that you can specify during the UMDS installation. The default folder to which UMDS downloads patch binaries and patch metadata is `C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Data`. You can change the folder in which UMDS downloads patch binaries, patch metadata, and notifications after you install UMDS.

If you have already downloaded patch binaries, metadata, and notifications, make sure that you copy all the files and folders from the old location to the new patch store location. The folder in which UMDS downloads patch binaries and patch metadata must be located on the machine on which UMDS is installed.

Procedure

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

2 Navigate to the directory where UMDS is installed.

- The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Change the patch repository directory by running the following command:

```
vmware-umds --set-config --patch-store your_new_patchstore_folder
```

In this example, *your_new_patchstore_folder* is the path to the new folder to which you want to download the patch binaries and patch metadata.

You successfully changed the directory in which UMDS stores patch data.

What to do next

Download patch binaries, patch metadata, and notifications using UMDS.

Configure UMDS to Download Third-Party Patches for ESX/ESXi Hosts

You can configure UMDS to connect to the Web sites of third-party vendors to download ESX/ESXi 4.0.x and ESX/ESXi 4.1 host patches and notifications.

Procedure

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

2 Navigate to the UMDS installation directory and open the `downloadConfig.xml` file for editing.

- The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- The default path in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Add the third-party URL address between the `<HostConfig>` and `</HostConfig>` tags.

For example, add the following URL address:

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

NOTE You can add a third-party URL address only for ESX/ESXi 4.0.x and ESX/ESXi 4.1 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. For example,

```
<HostConfig>
<ESXThirdPartyUpdateUrl id="url1">http://third_party_URL1/index.xml</ESXThirdPartyUpdateUrl>
<ESXThirdPartyUpdateUrl id="url2">http://third_party_URL2/index.xml</ESXThirdPartyUpdateUrl>
<ESXThirdPartyUpdateUrl id="url3">http://third_party_URL3/index.xml</ESXThirdPartyUpdateUrl>
</HostConfig>
```

4 Save and close the file.

UMDS is configured to download ESX/ESXi patches and notifications from third-party URL addresses.

What to do next

Download the patches and notifications using UMDS.

Download Patches and Notifications Using UMDS

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

Procedure

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

2 Navigate to the directory where UMDS is installed.

- The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Download the selected patches.

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

This command downloads all the patches and notifications from the configured sources for the first time. Subsequently, it downloads all new patches and notifications released after the previous UMDS download.

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

The command to re-download patches and notifications deletes the existing data from the patch store (if present) and re-downloads it.

To re-download the patches and notifications that were downloaded in May 2009, for example, run the following command:

```
vmware-umds --re-download --start-time 2009-05-01T00:00:00 --end-time 2009-05-31T23:59:59
```

The data previously downloaded for the specified period is deleted and downloaded again.

What to do next

Export the downloaded patches and notifications.

Export the Downloaded Patches and Notifications

You can export downloaded patches and notifications 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 Navigate to the directory where UMDS is installed.

- The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`.
- The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`.

3 Specify the export parameters and export the data.

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

In the command, you must specify the full path of the export directory.

If you are working in a semi-air-gap deployment, *repository_path* can be the path to the folder on the Web server that serves as a shared repository.

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.

The data you downloaded by using UMDS is exported to the path you specify. Make sure that all files are exported. You can periodically perform export from UMDS and populate the shared repository so that Update Manager can use the new patch binaries and patch metadata.

4 (Optional) You can export the patches that you downloaded during a specified time window.

For example, to export the patches downloaded in May 2009, run the following command:

```
vmware-umds -E --export-store repository-path --start-time 2009-05-01T00:00:00 --end-time
2009-05-31T23:59:59
```

What to do next

Configure Update Manager to use a shared repository as a patch download source. For more information, see “Use a Shared Repository as a Patch Download Source,” on page 72.

Configuring Update Manager 11

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 Administration view.

You can modify the Update Manager settings only if you have the privileges 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 Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

If your vCenter Server system is 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:

Update Manager Network Connectivity Settings

After you install Update Manager with the default installation settings, 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.

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

- 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 (SSL) port 9087 for uploading the host upgrade files.

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

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

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

If you have ESX 3.x hosts in your inventory and Update Manager is installed on a computer with IPv6, the scan and remediation operations on the hosts fail, because the hosts cannot connect to the Update Manager server. You should install Update Manager on a computer with IPv4 enabled to scan and remediate ESX 3.x hosts.

vCenter Server, Update Manager, and your ESX/ESXi hosts might exist in a heterogeneous IPv6 and IPv4 network environment. In such an environment, if there is no dual stack IPv4 and IPv6 DNS server, and if you use IP addresses, the ESX/ESXi hosts configured to use only IPv4 address cannot access the IPv6 network resources. The hosts configured to use only IPv6 cannot access the IPv4 network resources either.

You can install Update Manager on a machine on which both IPv4 and IPv6 are enabled. During host operations such as scanning, staging, and remediation, Update Manager provides the address of its patch store location to the ESX/ESXi hosts. If Update Manager is configured to use an IP address, it provides an IP address of either IPv4 or IPv6 type, and can be accessed by only some of the hosts. For example, if Update Manager provides an IPv4 address, the hosts that use only an IPv6 address cannot access the Update Manager patch store. In such a case consider the following configuration:

- For hosts that use only IPv4, configure Update Manager to use either an IPv4 address or host name. Using a host name lets all hosts rely on the DNS server to resolve to an IPv4 address.
- For hosts that use only IPv6, configure Update Manager to use either an IPv6 address or host name. Using a host name lets hosts rely on the DNS server to resolve to an IPv6 address.
- For hosts that use both IPv4 and IPv6 addresses, configure Update Manager to use either IPv4 or IPv6.

Configure Update Manager Network Connectivity Settings

After you install Update Manager with the default installation settings, 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.

Prerequisites

- Before changing the network connectivity settings, check for conflicts with other port settings. If any remediation or scan tasks are running, cancel them or wait until they complete.
- Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page.

  If your vCenter Server system is 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.
- 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.

Procedure

1 On the **Configuration** tab, under Settings, click **Network Connectivity**.

2 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: 80, 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.

3 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 and extensions either from the Internet or from a shared repository of UMDS data. You can also import patches and extensions manually from a ZIP file.

If your deployment system is connected to the Internet, you can use the default settings and links for downloading patches and extensions to the Update Manager patch repository. You can also add URL addresses to download third-party patches and extensions that are applicable only to ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts.

Downloading host patches from the VMware Web site is a secure process.

- Patches are cryptographically signed with the VMware private keys. Before you try to install a patch on a host, the host verifies the signature. This signature enforces the end-to-end protection of the patch itself, and can also address any concerns about patch download.

- Update Manager downloads patch metadata and patch binaries over SSL connections. Update Manager downloads patch metadata and patch binaries only after verification of both the validity of the SSL certificates and the common name in the certificates. The common name in the certificates must match the names of the servers from which Update Manager downloads patches.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the patches and extensions by using the UMDS. For more information, see Chapter 10, "Installing, Setting Up, and Using Update Manager Download Service," on page 59.

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

If the VMware vCenter Update Manager Update Download task is running when you apply the new configuration settings, the task continues to use the old settings until it completes. The next time the task to download updates starts, it uses the new settings.

With Update Manager 4.1, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. You download these patches or extensions from the Internet or copy them from a media drive, and save them as offline bundle ZIP files on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later.

IMPORTANT You can import offline bundles only for hosts that are running ESX/ESXi 4.0 or later.

Offline bundles contain one `metadata.zip` file and one or more vSphere Installation Bundle (VIB) files. When you import an offline bundle to the Update Manager patch repository, Update Manager extracts it and checks whether the `metadata.zip` file has already been imported. If the `metadata.zip` file has never been imported, Update Manager performs sanity testing, and imports the files successfully. After you confirm the import, Update Manager saves the files into the Update Manager database and copies the `metadata.zip` and VIB files into the Update Manager patch repository.

- Configure Update Manager to Use the Internet as a Patch Download Source on page 71

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

- Add a Third-Party Download URL Source for ESX/ESXi Hosts on page 71

  If you use the Internet as a download source for patches, you can add a third-party URL address to download ESX/ESXi 4.0.x and ESX/ESXi 4.1 host patches and extensions.

- Use a Shared Repository as a Patch Download Source on page 72

  You can configure Update Manager to use a shared repository as a source for downloading patches and notifications.

- Import Patches Manually on page 73

  Instead of using a shared repository or the Internet as a patch download source, you can import patches and extensions manually by using an offline bundle. You can import offline bundles only for hosts that are running ESX/ESXi 4.0 or later.

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.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **Patch Download Settings**.

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

3 Select the patch type that you want to download.

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

4 (Optional) Add an additional third-party patch download source for ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts.

5 Click **Apply**.

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

Add a Third-Party Download URL Source for ESX/ESXi Hosts

If you use the Internet as a download source for patches, you can add a third-party URL address to download ESX/ESXi 4.0.x and ESX/ESXi 4.1 host patches and extensions.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **Patch Download Settings**.

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

3 Click **Add Patch Source**.

4 In the Add Patch Source window, enter the third-party source URL.

`https://source_path/index.xml`

Update Manager supports both HTTP and HTTPS URL addresses. You should enter HTTPS URL addresses, so that the patch metadata is downloaded securely. Patch URL addresses must be complete and contain the `index.xml` file which lists the vendor and the vendor index.

NOTE The proxy settings for Update Manager are applicable to third-party patch URL addresses too. You can configure the proxy settings from the Proxy Settings pane.

5 (Optional) Enter a URL description.

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

7 Click **OK**.

8 Click **Apply**.

9 Click **Download Now** to run the VMware vCenter Update Manager Update Download task and to download the patches and extensions 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 source for downloading patches and notifications.

Prerequisites

You must create the shared repository using the UMDS and host it on a Web server or a local disk. The UMDS you use must be of a version compatible with Update Manager. You cannot set up Update Manager to use a shared repository if the patch binaries, patch metadata, and notifications are downloaded with a version of UMDS that is not compatible with the current version of Update Manager.

For more information, about the compatibility, see "Compatibility Between UMDS and the Update Manager Server," on page 60. You can find the detailed procedure about exporting the patch binaries, patch metadata, and notifications in "Export the Downloaded Patches and Notifications," on page 65.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **Patch Download Settings**.

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

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

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

In these examples, *repository_path* is the path to the folder to which you have exported the patches and notifications. In a semi-air-gap environment (where the Update Manager server does not have direct access to the Internet, but is connected to a machine that has Internet access), the folder can be 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, patch metadata, and notifications 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:\`).

---

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

Important If the patch binaries, patch metadata, and notifications in the folder you specify are downloaded with a UMDS version that is not compatible with the Update Manager version you use, the validation fails and you receive an error message.

Make sure that the validation is successful. If the validation fails, Update Manager reports a reason for the failure. You can use the path to the shared repository only when the validation is successful.

5 Click **Apply**.

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

The shared repository is used as a source for downloading patches and notifications.

Example: Using a Folder or a Server as a Shared Repository

You can use a folder or a Web server as a shared repository.

- When you use a folder as a shared repository, *repository_path* is the top-level directory where patches and notifications exported from UMDS are stored.

  For example, export the patches and notifications using UMDS to `F:\`, which is a drive mapped to a plugged-in USB device on the machine on which UMDS is installed. Then, plug in the USB device to the machine on which Update Manager is installed. On this machine the device is mapped as `E:\`. The folder to configure as a shared repository in the Update Manager is `E:\`.

- When you use a Web server as a shared repository, *repository_path* is the top-level directory on the Web server where patches exported from UMDS are stored.

  For example, export the patches and notifications from UMDS to `C:\docroot\exportdata`. If the folder is configured in a Web server and is accessible from other machines at the URL `https://umds_host_name/exportdata`, the URL to configure as a shared repository in Update Manager is `https://umds_host_name/exportdata`.

Import Patches Manually

Instead of using a shared repository or the Internet as a patch download source, you can import patches and extensions manually by using an offline bundle. You can import offline bundles only for hosts that are running ESX/ESXi 4.0 or later.

Prerequisites

The patches and extensions you import must be in ZIP format.

To import patches and extensions, you must have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **Patch Download Settings**.

2 Click **Import Patches** at the bottom of the Patch Download Sources pane.

3 On the Select Patches page of the Import Patches wizard, browse to and select the `.zip` file containing the patches you want to import.

4 Click **Next** and wait until the file upload completes successfully.

  In case of upload failure, check whether the structure of the `.zip` file is correct or whether the Update Manager network settings are set up correctly.

5 Click **Next**.

6 On the Confirm Import page of the Import Patches wizard, review the patches that you import into the Update Manager repository.

7 Click **Finish**.

You imported the patches into the Update Manager patch repository. You can view the imported patches on the Update Manager **Patch Repository** tab.

Configure Update Manager Proxy Settings

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

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **Patch Download Settings**.

2 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.

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

4 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.

By default the task to download patch metadata and patch binaries is enabled and is called 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** view of the vSphere Client or the **Configuration** tab of the Update Manager Client Administration view.

Prerequisites

To download patch data, the machine on which Update Manager is installed must have Internet access.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab under Settings, click **Patch Download Schedule**.

2 Make sure that the **State** check box is selected.

NOTE If you deselect the check box, the scheduled task that checks for patches is disabled.

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

The Schedule Update Download wizard appears.

4 Specify a task name and, optionally, a description, or keep the defaults.

5 Specify the **Frequency**, **Start Time** , **Interval** of the patch download, and click **Next**.

6 (Optional) Specify one or more email addresses to be notified when the new patches are downloaded, and click **Next**.

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

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

The task runs according to the time you specified.

Configuring Notification Checks and Viewing Notifications

At regular time intervals, Update Manager 4.1 contacts VMware to download information (notifications) about patch recalls, new fixes, and alerts.

In case patches with issues or potential issues are released, these patches are recalled in the metadata, and Update Manager marks them as recalled. If you try to install a recalled patch, Update Manager notifies you that the patch is recalled and does not install it on the host. If you have already installed such a patch, Update Manager notifies you that the recalled patch is installed on certain hosts. Update Manager also deletes all the recalled patches from the Update Manager patch repository.

When a patch fixing the problem is released, Update Manager 4.1 downloads the new patch and prompts you to install it to fix the issues that the recalled patch might cause. If you try to install the recalled patch, Update Manager alerts you that the patch is recalled and that there is a fix you must install.

Update Manager 4.1 supports patch recalls for offline bundles you have imported. Recalling patches from an imported offline bundle happens when you import a new offline bundle. The `metadata.zip` file contains information about the patches that must be recalled. Update Manager removes the recalled patches from the patch repository and after you import a bundle containing the new fixes, Update Manager notifies you about the fixes and sends email notifications in case you configure it to do that.

Update Manager 4.1 also supports the recall of patches and notification checks when you use a shared repository as a patch download source, but emails are not sent when a patch is recalled. If you use a shared repository as a source for downloading patches and notifications, recall notifications are downloaded from the shared repository to the Update Manager patch repository, but recall email alerts are not sent. For more information about using a shared repository, see "Use a Shared Repository as a Patch Download Source," on page 72.

Notifications in Update Manager 4.1 can also be informative or actionable alerts. Alerts can have moderate, important, and critical severity.

Configure Notifications Checks

By default Update Manager checks for notifications about patch recalls, patch fixes, and alerts at certain time intervals. You can modify this schedule.

By default the task to check for notifications and to send notifications alerts is enabled and is called the VMware vCenter Update Manager Check Notification task. By modifying this task, you configure when Update Manager checks for patch recalls or for the release of patch fixes, and sends notifications to the email addresses you specify. You can modify the VMware vCenter Update Manager Check Notification task from either the **Scheduled Tasks** view of the vSphere Client or the **Configuration** tab of the Update Manager Client Administration view.

Prerequisites

To configure notification checks, make sure that the machine on which Update Manager is installed has Internet access.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab under Settings click **Notification Check Schedule**.

2 Make sure that the **State** check box is selected.

NOTE If you deselect the check box, the scheduled task that checks for notifications is disabled.

3 Click **Edit Notifications** on the upper right.

The Schedule Notification wizard appears.

4 Specify a task name and, optionally, a description, or keep the defaults.

5 Specify the **Frequency**, **Start Time**, and **Interval** of the task, and click **Next**.

6 (Optional) Specify one or more email addresses where notifications about patch recalls or email alerts are sent, and click **Next**.

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

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

The task runs according to the time you specified.

View Notifications and Run the Notification Checks Task Manually

Notifications that Update Manager downloads are displayed on the **Notifications** tab of the Update Manager Administration view.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 Click the **Notifications** tab in the Update Manager Administration view.

2 Double-click a notification to view the notification details.

3 Click **Check Notifications** on the upper-right to check for notifications immediately.

If there are new notifications on the VMware Web site, they are immediately downloaded.

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.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, select **Virtual Machine Settings**.

2 To take snapshots of the virtual machines before remediating them, leave **Snapshot the virtual machines before remediation to enable rollback** selected.

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

4 Click **Apply**.

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

Configuring Host and Cluster Settings

When you update vSphere objects in a cluster with DRS, VMware High Availability (HA), and VMware Fault Tolerance (FT) enabled, you should temporarily disable VMware Distributed Power Management (DPM), HA admission control, and FT for the entire cluster. When the update completes, Update Manager restores these features.

Patches might require that the host enters maintenance mode during remediation. 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 into maintenance mode. vCenter Server migrates the virtual machines if the cluster is configured for vMotion, and if DRS is enabled.

You should enable Enhanced vMotion Compatibility (EVC) to help ensure vMotion compatibility between the hosts in the cluster. EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. Using EVC prevents migrations with vMotion from failing because of incompatible CPUs. For more information about EVC and the requirements which the hosts in an EVC cluster must meet, see *vSphere Datacenter Administration Guide*.

If a host has no running virtual machines, VMware DPM might put the host in standby mode and interrupt an Update Manager operation. To make sure that scanning, staging, and remediation are successful, temporarily disable VMware DPM and HA admission control before you start a scan, stage or remediation operation. After the operation completes, Update Manager restores VMware DPM and HA admission control.

If VMware DPM has already put hosts in standby mode, Update Manager powers on the hosts before scanning, staging, and remediation. After the scanning, staging, or remediation is complete, Update Manager turns on VMware DPM and HA admission control and lets DPM put hosts into standby mode, if needed. Update Manager does not remediate powered off hosts.

If hosts are put into standby mode and VMware DPM is manually disabled for a reason, Update Manager does not remediate the hosts.

Within a cluster, you should disable HA admission control to allow vMotion to proceed, so that there is no downtime of the machines on the hosts you remediate. After the remediation of the entire cluster, Update Manager restores HA admission control settings.

If FT is turned on for any of the virtual machines on hosts within a cluster, you should temporarily turn off FT before performing any Update Manager operations on the cluster. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. You should remediate all hosts in a cluster with the same updates, so that FT can be re-enabled after the remediation, because a primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESX/ESXi version and patch level.

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

ESX/ESXi host patches might 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 the host fails to enter into maintenance mode.

For hosts in a container different from a cluster or for individual hosts, migration of the virtual machines with vMotion cannot be performed. If vCenter Server cannot migrate the virtual machines to another host, you can configure how Update Manager responds.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Under Maintenance Mode Settings, 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** field. If Update Manager cannot put a host into maintenance mode, you can take an action to make sure that the operation succeeds next time when Update Manager tries to put the host into maintenance mode. For example, you can manually power off the virtual machines or migrate them to another host using vMotion to ensure that entering maintenance mode is successful next time.
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.

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

4 (Optional) Select **Temporarily disable any removable media devices that might prevent a host from entering maintenance mode**.

Update Manager does not remediate hosts on which virtual machines are with connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host, might prevent the host from entering maintenance mode and interrupt remediation.

5 Click **Apply**.

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

Configure Cluster Settings

For ESX/ESXi hosts in a cluster, the remediation process runs in a sequence. Certain features might cause remediation failure. If you have VMware DPM, HA admission control, or Fault Tolerance enabled, you should temporarily disable these features to make sure that the remediation is successful.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **ESX Host/Cluster Settings**.

2 Select the check boxes of the features you have configured and you want to disable.

Option	Description
Distributed Power Management (DPM)	VMware DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. If you do not select to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you select to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates it, and re-enables VMware DPM after remediation is complete.
High Availability (HA) admission control	Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion. If you do not select to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you select to temporarily disable HA admission control, Update Manager disables HA admission control, remediates the cluster, and re-enables HA admission control after remediation is complete.
Fault Tolerance (FT)	FT provides continuous availability for virtual machines by automatically creating and maintaining a secondary virtual machine that is identical to the primary virtual machine. If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host.

3 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 restarts the virtual appliances and virtual machines in the vApp to maintain startup dependencies. You can enable and disable smart rebooting of virtual appliances and virtual machines in a vApp after remediation.

A vApp is a prebuilt software solution, consisting of one or more virtual machines and applications, which are potentially operated, maintained, monitored, and updated as a unit.

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

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Configuration** tab, under Settings, click **vApp Settings**.

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

Configure Update Manager Patch Repository Location

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

Procedure

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

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 **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 (x86)\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.

8 Start the Update Manager service by right-clicking **VMware Update Manager Service** in the Computer Management window and selecting **Start**.

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 **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 address of the sender.

For example, `mail_server@datacenter.com`

6 Click **OK**.

Restart the Update Manager Service

In certain 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 vCenter Update Manager Service** and select **Restart**.

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, extensions, and notifications.

Procedure

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

If your vCenter Server system is 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 and select **Run**.

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

Update Manager Privileges

To configure Update Manager settings, to manage baselines, patches, and upgrades, you must have the proper privileges. You can assign Update Manager privileges to different roles from the vSphere Client.

Update Manager privileges and their descriptions are listed in Table 11-1.

Table 11-1. Update Manager Privileges

Privilege Group	Privilege	Description
Configure	**Configure Service**	Configure the Update Manager service and the scheduled patch download task.
Manage Baseline	**Attach Baseline**	Attach baselines and baseline groups to objects in the vSphere inventory.
	Manage Baseline	Create, edit, or delete baseline and baseline groups.
Manage Patches and Upgrades	**Remediate to Apply Patches, Extensions, and Upgrades**	Remediate virtual machines, virtual appliances, and hosts to apply patches, extensions, or upgrades. In addition, this privilege allows you to view compliance status.
	Scan for Applicable Patches, Extensions, and Upgrades	Scan virtual machines, virtual appliances, and hosts to search for applicable patches, extensions, or upgrades.
	Stage Patches and Extensions	Stage patches or extensions to hosts. In addition, this privilege allows you to view compliance status of the hosts.
	View Compliance Status	View baseline compliance information for an object in the vSphere inventory.
Upload File	**Upload File**	Upload host upgrade release bundles and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see the *vSphere Datacenter Administration Guide*.

Working with Baselines and Baseline Groups 12

Baselines might be upgrade, extension, or patch baselines. Baselines contain a collection of one or more patches, service packs, bug fixes, extensions, or upgrades.

Baseline groups are assembled from existing baselines and might contain one upgrade baseline per type and one or more patch and extension baselines, or a combination of multiple patch and extension baselines. When you scan hosts, virtual machines, and virtual appliances, you evaluate them against baselines and baseline groups to determine their level of compliance.

To create, edit, or delete baselines and baseline groups, you must have the **Manage Baseline** privilege. To attach baselines and baseline groups, you must have the **Attach Baseline** privilege. Privileges 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 Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

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 hosts that are running ESX/ESXi 4.0 and later.
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 hosts that are running ESX/ESXi 4.0 and later.
VA Upgrade to Latest	Checks virtual appliance compliance with the latest released 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 Administration view.

If your vCenter Server system is 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 can use an Update Manager instance only with a vCenter Server system on which the instance is registered.

This chapter includes the following topics:

Creating and Managing Baselines

You can create patch, extension, 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 and manage baselines in the Update Manager Client Administration view.

Create and Edit Patch or Extension Baselines

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.

Extension baselines contain additional software for ESX/ESXi hosts. This additional software might be VMware software or third-party software.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, and you have more than one Update Manager instance, patch and extension 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.

Prerequisites

To create baselines, you must have the **Manage Baseline** privilege.

Create a Fixed Patch Baseline

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

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.

The New Baseline wizard opens.

2 In the New Baseline wizard, under Baseline Type, select either **Host Patch** or **VM Patch**, and click **Next**.

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

4 Select individual patches to include, and click the down arrow to add them to the Fixed Patches to Add list.

5 (Optional) Click **Advanced** to find specific patches to include in the baseline.

6 Click **Next**.

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

The fixed patch baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

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. Patches you select to add or exclude do not change with new patch downloads.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.

The New Baseline wizard opens.

2 In the New Baseline wizard, under Baseline Type, select either **Host Patch** or **VM Patch**, and click **Next**.

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

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

Option	Description
Patch Vendor	Specifies which patch vendor to use.
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.

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

For example, when you select a product and severity option, the patches are restricted to the patches for the selected product and are of the specified severity level.

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

6 (Optional) Click **Advanced** to select specific patches to exclude from the baseline.

7 Click **Next**.

8 (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 Fixed Patches to Add list.

The patches you add to the dynamic baseline stay in the baseline regardless of the new downloaded patches.

9 (Optional) Click **Advanced** to select specific patches to include in the baseline.

10 Click **Next**.

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

The dynamic patch baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Create a Host Extension Baseline

Extension baselines contain additional software for ESX/ESXi hosts. This additional software might be VMware software or third-party software. You create host extension baselines using the New Baseline wizard.

Extensions can provide additional features, updated drivers for hardware, Common Information Model (CIM) providers for managing third-party modules on the host, improvements to the performance or usability of existing host features, and so on.

Host extension baselines that you create are always fixed. You must carefully select the appropriate extensions for the ESX/ESXi hosts in your environment.

To perform the initial installation of an extension, you must use an extension baseline. After the extension is installed on the host, you can update the extension module with either patch or extension baselines.

When applying extension baselines by using Update Manager, you must be aware of the functional implications of new modules to the host. Extension modules might alter the behavior of ESX/ESXi hosts. During installation of extensions, Update Manager only performs the checks and verifications expressed at the package level.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.

The New Baseline wizard opens.

2 Under Baseline Type select **Host Extension** and click **Next**.

3 On the Extensions page, select individual extensions to include in the baseline, and click the down arrow to add them to the Included Extensions list.

4 (Optional) Filter the extensions to include specific extensions in the baseline.

5 Click **Next**.

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

The extension baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Filter Patches or Extensions in the New Baseline Wizard

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

Procedure

1 In the New Baseline wizard, click **Advanced**.

- If you are creating a fixed patch baseline, on the Patches page of the New Baseline wizard, click **Advanced**.
- If you are creating a dynamic patch baseline, on the Patches to Exclude or Additional patches page of the New Baseline wizard, click **Advanced**.
- If you are creating a host extension baseline, on Extensions page of the New Baseline wizard, click **Advanced**.

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

Option	Description
Patch Vendor	Specifies which patch or extension vendor to use.
Product	Restricts the set of patches or extensions 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 or extensions to include.
Released Date	Specifies the range for the release dates of the patches or extensions.
Text	Restricts the patches or extensions to those containing the text that you enter.

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

3 Click **Find**.

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

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 Administration view.

Prerequisites

To edit baselines, you must have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

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

2 Select a patch baseline and click **Edit** above the Baselines pane.

3 Edit the name and description of the baseline and click **Next**.

4 Go through the Edit Baseline wizard to change the criteria, patches to include or exclude.

5 Click **Finish** on the Ready to Complete page, to save your changes.

Edit a Host Extension Baseline

You can change the name, description, and composition of an existing extension baseline.

You can edit extension baselines from the Update Manager Client Administration view.

Prerequisites

To edit baselines, you must have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click the **Hosts** button.

2 Select an extension baseline and click **Edit** above the Baselines pane.

3 Edit the name and description of the baseline and click **Next**.

4 Make your changes by going through the Edit Baseline wizard.

5 Click **Finish** on the Ready to Complete page, to save your changes.

Create and Edit Host Upgrade Baselines

You can create an ESX/ESXi host upgrade baseline by using the New Baseline wizard. You can create host baselines with already uploaded ESX/ESXi upgrade release files.

You can upload upgrade files and manage them from the **Host Upgrade Releases** tab of the Update Manager Administration view.

Update Manager 4.1 supports upgrades from ESX 3.0.0 and later as well as from ESX 3i version 3.5 and later to ESX/ESXi 4.0.x and 4.1. The remediation from version 4.0 to version 4.0.x is a patching operation, while the remediation from version 4.0.x to 4.1 is considered an upgrade.

NOTE You cannot upgrade ESX 3.0.x hosts directly to ESX 4.1. To upgrade ESX hosts of version 3.0.x to version 4.1 you must first upgrade them to version 4.0 or 4.0.x and then upgrade to 4.1.

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

Upgrade files that you upload are ISO or ZIP files. The file type depends on the host type, host version, and on the upgrade that you want to perform. Table 12-1 represents the types of the upgrade files that you must upload for upgrading the ESX/ESXi hosts in your environment.

Table 12-1. File Type of the Upgrade Release File

Target ESX/ESXi host version	Source ESX/ESXi host version			
	ESX 4.0.x	ESXi 4.0.x	ESX 3.x	ESXi 3.x
4.0.x	N/A	N/A	ISO	ZIP
4.1	ZIP	ZIP	ISO	ZIP

A host upgrade release is a combination of host upgrade files that allow you to upgrade hosts to a particular release version. Depending on the files that you upload, host upgrade releases can be partial or complete.

Partial upgrade release

Partial upgrade releases are host upgrade releases that do not contain all of the upgrade files required for an upgrade of both the ESX and ESXi hosts in your environment to a specific version.

For example, a partial release is when you upload only an ISO file to upgrade the ESX 3.x hosts in your environment to version 4.1, but you do not upload the ZIP files required for upgrading the hosts of versions ESXi 3.x and ESX/ESXi 4.0.x to version 4.1.

Complete upgrade release

Complete upgrade releases are host upgrade releases that contain all of the upgrade files required for an upgrade of both the ESX and ESXi host in your environment to a specific version.

For example, to upgrade all the ESX/ESXi hosts in your vSphere environment to version 4.1, you must upload all of the files required for this upgrade (three ZIP files and one ISO file):

- `esx-DVD-4.1.0-`*`build_number`*`.iso` for ESX 3.x hosts
- `upgrade-from-ESXi3.5-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 3.x hosts
- `upgrade-from-ESX4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESX 4.0.x hosts
- `upgrade-from-ESXi4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 4.0.x hosts

Here *build_number* is the build number of the upgrade release.

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

Import Host Upgrade Releases

You can create upgrade baselines for ESX/ESXi hosts with upgrade release files that you import to the Update Manager repository.

Host upgrade release files contain software that upgrades ESX/ESXi hosts to a particular target version. Upgrade releases can be partial or complete.

You can upgrade multiple ESX/ESXi hosts of different versions simultaneously if you import a complete release bundle.

Prerequisites

To upload upgrade files, you must have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Host Upgrade Releases** tab click **Import Upgrade Release** on the upper-right.

The Import Upgrade Release wizard appears.

2 On the Select Upgrade Files page of the Import Upgrade Release wizard, browse to and locate the upgrade release files that you want to upload.

NOTE You can select to upload multiple files at the same time, but some files are large and might take significant time to upload.

3 Click **Next**. The upload process starts.

CAUTION Do not close the Import wizard. Closing the Import wizard stops the upload process.

4 (Optional) In the Security Warning window select the method you want the system to use to ignore the warning.

A trusted certificate authority does not sign the certificates that are generated for vCenter Server and ESX/ESXi hosts during installation. Because of this, each time an SSL connection is made to one of these systems, the client displays a warning.

Option	Description
Ignore	Click **Ignore** to continue using the current SSL certificate.
Cancel	Click **Cancel** to close the window. Clicking **Cancel** might cause a failure in the upload because the connection with the vCenter Server is untrusted.
Install this certificate and do not display any security warnings	Select this check box and click **Ignore** to install the certificate and stop receiving security warnings.

5 After the file upload completes, click **Finish**.

The uploaded host upgrade release files appear in the Imported Upgrade Releases pane as an upgrade release.

What to do next

Create host upgrade baselines with the upgrade files that you uploaded.

Create a Host Upgrade Baseline

To upgrade the hosts in your vSphere environment you must create host upgrade baselines.

The remediation from version 4.0 to version 4.0.x is a patching operation, and does not involve upgrade baselines, while the remediation from version 4.0.x to 4.1 is considered an upgrade.

NOTE The ESX Upgrade - COS VMDK Location and the ESX Upgrade - Post-upgrade option pages are specific for upgrading ESX hosts from version 3.x to versions 4.0.x and 4.1.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Upload at least one upgrade release file.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.

The New Baseline wizard opens.

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

3 On the Upgrade Version page, select a host upgrade release and click **Next**.

The Upgrade Release Details pane of the page displays additional information about the selected upgrade release.

4 On the ESX Upgrade - 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 fails 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 datastore that is accessible to this host only and is not shared with other hosts. The operation fails if the 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.

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

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

6 (Optional) On the ESX Upgrade - Post-Upgrade Options page, specify whether to use a post-upgrade script to run after the upgrade completes, and when the post-upgrade script times out.

You can browse to locate a Bash (`.sh`) or Python (`.py`) post-upgrade script on your system. You can use post-upgrade scripts to automate the configuration of ESX hosts after the upgrade.

7 Click **Next**.

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

The host upgrade baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

Edit a Host Upgrade Baseline

You can change the name, description, and upgrade options of an existing host upgrade baseline. You cannot delete an upgrade release by editing the host upgrade baseline.

You can edit upgrade baselines from the Update Manager Client Administration view.

Prerequisites

To edit baselines, you must have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click the **Hosts** button.

2 Select an existing host upgrade baseline and click **Edit** above the Baselines pane.

3 Edit the name and description of the baseline, and click **Next**.

4 Make your changes by going through the Edit Baseline wizard.

Option	Description
Upgrade Version	Change the upgrade version and click **Next**.
COS VMDK Location	Edit the specified location of the VMDK to which to migrate the COS of the ESX host. This is applicable only when you upgrade ESX hosts from version 3.x to versions 4.0.x and 4.1.
Post-Upgrade Options	Click to edit the settings to reboot the host in case of failure and the post-upgrade usage settings. This is applicable only when you upgrade ESX hosts from version 3.x to versions 4.0.x and 4.1.

5 Click **Finish** on the Ready to Complete page to save your changes.

Delete Host Upgrade Release Files

You can delete upgrade releases from the Update Manager repository if you no longer need them.

You can delete upgrade release files from the **Host Upgrade Releases** tab of the Update Manager Administration view.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Prerequisites

Before you delete imported upgrade releases, make sure that they are not included in baselines.

Procedure

1 Click the **Host Upgrade Releases** tab.

2 Under Imported Upgrade Releases, select the release you want to delete and click **Delete**.

3 Click **Yes** to confirm the deletion.

The upgrade release is deleted and no longer available under Imported Upgrade Releases.

Create and Edit a Virtual Appliance Upgrade Baseline

A virtual appliance upgrade baseline contains a set of patches to the operating system of the appliance and to the applications installed in the virtual appliance. The virtual appliance vendor considers these patches an upgrade.

Virtual appliance baselines that you create consist 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.

Create a Virtual Appliance Upgrade Baseline

You upgrade virtual appliances by using a virtual appliance upgrade baselines.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

After you import a VMware Studio created virtual appliance in the vSphere Client, power it on so that it is discovered as a virtual appliance.

Procedure

1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.

The New Baseline wizard opens.

2 Under Baseline Type, select **VA Upgrade**, and click **Next**.

3 Select **Vendor** and **Appliance** options from the respective drop-down menu.

The options listed in these menus depend on the virtual appliances that you imported in your inventory. After you import a virtual appliance and power it on for the first time, it is discovered and registered as a virtual appliance. The vendor and appliance information about the detected virtual appliance are imported in the Update Manager database and listed in the **Vendor** and **Appliance** drop-down menus. If there are no detected and registered virtual appliances, the options are All Vendors and All Products, respectively.

4 Select an option from the **Upgrade To** drop-down menu.

Option	Description
Latest	Upgrades the virtual appliance to the latest version.
Do not Upgrade	Does not upgrade the virtual appliance.

5 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 any conflicts within the rules you apply.

a In the Upgrade Rule Conflict window select whether to keep the existing rules, to use the newly created rules, or to manually resolve the conflict.

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 Baselines pane of the **Baselines and Groups** tab.

Edit a Virtual Appliance Upgrade Baseline

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

You can edit upgrade baselines from the Update Manager Client Administration view.

Prerequisites

To edit baselines, you must have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, click the **VMs/VAs** button.

2 Select an existing virtual appliance upgrade baseline and click **Edit** above the Baselines pane.

3 Edit the name and the description of the baseline and click **Next**.

4 Edit the upgrade options and click **Next**.

5 Click **Finish** on the Ready to Complete page to save your changes.

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 can delete baselines from the Update Manager Client Administration view.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 In the **Baselines** pane of the **Baselines and Groups** tab, select the baselines to remove, and click **Delete**.

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

The baseline is deleted.

Creating and Managing 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 the same time.

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

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

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

- You can include all patch and extension 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 that you create are displayed on the **Baselines and Groups** tab of the Update Manager Client Administration view.

If your vCenter Server system is 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 host upgrade baseline with multiple patch or extension baselines, or combine multiple patch and extension baselines in a baseline group.

NOTE You can click **Finish** in the New Baseline Group wizard at any time to save your baseline group and add baselines to it at a later stage.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab click **Create** above the Baseline Groups pane.

2 Enter a unique name for the baseline group.

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

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

5 (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.

6 Click **Next**.

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

8 (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.

9 Click **Next**.

10 Select the extension baselines to include in the baseline group.

11 (Optional) Create a new extension baseline by clicking **Create new Extension Baseline** at the bottom of the Patches page and complete the New Baseline wizard.

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 that you include must be nonconflicting.

NOTE You can click **Finish** in the New Baseline Group wizard at any time to save your baseline group and add baselines to it at a later stage.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab click **Create** above the Baseline Groups pane.

2 In the New Baseline Group wizard, under Baseline Group Type, select **Virtual Machines and Virtual Appliances Baseline Group** and click **Next**.

3 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 you select to remediate only virtual appliances, the patches and upgrades for virtual machines are ignored. If only virtual machines are to be 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.

4 (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.

5 Click **Next**.

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

7 (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.

8 Click **Next**.

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

The baseline group is displayed in the Baseline Groups pane.

Edit a Baseline Group

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

You edit baseline groups from the Update Manager Client Administration view.

Prerequisites

You can edit baseline groups only if you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab select the type of baseline group to edit by clicking either **Hosts** or **VMs/VAs**.

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 Change the included extension baselines (if any).

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

Add Baselines to a Baseline Group

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

You can add baselines to baseline groups from the Update Manager Client Administration view.

Prerequisites

You can edit baseline groups only if you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

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

2 From the Baseline Groups pane, select a baseline group and expand it to view the baselines included in the baseline group.

3 Select a baseline from the list in the Baselines pane, and click the right 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 can remove baselines from baseline groups from the Update Manager Client Administration view.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

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

2 From the Baseline Groups pane, select a baseline group and expand it to view the baselines included in the baseline group.

3 Select a baseline from the Baseline Groups pane on the right and click the left arrow.

The baseline is removed from the selected baseline group.

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 can delete baseline groups from the Update Manager Client Administration view.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 On the **Baselines and Groups** tab, select the baseline group to remove, and click **Delete**.

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

The baseline group is deleted.

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 can attach baselines and baseline groups 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, vApps, 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 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.

Prerequisites

To attach baselines and baseline groups, you must have the **Attach Baseline** privilege.

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

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

5 In the Attach Baseline or Group window, 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 Baseline Groups and Attached Baselines 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 search within the baselines and baseline groups.

You can 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, a host, or a container object.

4 Click the **Update Manager** tab.

If your vCenter Server system is 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 bottom pane of the **Update Manager** 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 container object where the baseline or baseline group is attached and then detach it from the container object.

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

Prerequisites

To detach baselines and baseline groups you must have the **Attach Baseline** privilege.

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 or group 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 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 remains in the Compliance view until you detach it from all objects.

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

Scanning vSphere Objects and Viewing Scan Results

13

Scanning is the process in which attributes of a set of hosts, virtual machines, or virtual appliances are evaluated against all patches, extensions, and upgrades in the attached baselines and baseline groups 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.

To initiate or schedule scans, you need the **Scan for Applicable Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

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

Update Manager 4.1 does not support scanning of offline Linux virtual machines for patches.

IMPORTANT Update Manager does not scan PXE booted ESXi hosts. A PXE booted installation of ESXi is completely stateless (it does not rely on the presence of a local disk). Therefore, the installation and post-install configuration are not persistent across reboot.

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 run the scan immediately. You should 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.

You can scan for either **Patches and Extensions** or **Upgrades**.

4 Click **Scan**.

The selected inventory object is scanned against all patches and extensions 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.

Prerequisites

After you import a VMware Studio created virtual appliance in the vSphere Client, power it on so that it is discovered as a virtual appliance.

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 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 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 that 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 part of a connected group in vCenter Linked Mode, specify the Update Manager instance that you want 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 Schedule Task 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 In 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 and click **Next**.

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

8 Set the frequency and the start time for the task 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** view of the vSphere Client.

Viewing Scan Results and Compliance States for vSphere Objects

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

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

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

- 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 privileges. Users with the privilege to view a container, but not all the contents of the container are shown the aggregate compliance of all objects in the container. If a user does not have permission to view an object, its contents, or a particular virtual machine, the results of those scans are not displayed. To view the compliance status, the user must also have the privilege to view compliance status for an object in the inventory. Users that have privileges to remediate against patches, extensions, and upgrades and to stage patches and extensions on a particular inventory object, can view the compliance status of the same object even if they do not have the view compliance privilege. For more information about the Update Manager privileges, see "Update Manager Privileges," on page 82. For more information about managing users, groups, roles and permissions, see *vSphere Datacenter Administration Guide*.
- 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 applicable. Only the newer patches are installed after starting a remediation process.

In the hierarchical inventory structure of the objects in the vSphere Client, the baseline and baseline groups you attach to container objects are also attached to the child objects. Consequently, the computed compliance state is also inherited. For example, a baseline or baseline group attached to a folder is inherited by all objects in the folder (including sub-folders), but the status of inherited baselines or baseline groups propagates upwards - from the contained objects to the folder. Consider a folder that contains two objects A and B. If you attach a baseline (baseline 1) to the folder, both A and B inherit baseline 1. If the baseline state is non-compliant for A and compliant for B, the overall state of baseline 1 against the folder is non-compliant. If you attach another baseline (baseline 2) to B, and baseline 2 is in incompatible compliance state with B, the overall status of the folder is incompatible.

View Compliance Information for vSphere Objects

You can review compliance information for the virtual machines, virtual appliances, and hosts against baselines and baseline groups that you attach.

When you select a container object, you view the overall compliance status of the attached baselines, as well as all the individual compliance statuses. If you select an individual baseline attached to the container object, you see the compliance status of the baseline.

If you select an individual virtual machine, appliance, or host, you see the overall compliance status of the selected object against all attached baselines and the number of updates. If you further select an individual baseline attached to this object, you see the number of updates grouped by the compliance status for that baseline.

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.

Review Compliance with Individual 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 and receive detailed information about the patches, extensions, and upgrades included in a baseline or a baseline group.

The following information is included in the scan results:

- 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 individual object from the inventory, such as a virtual machine, virtual appliance, or host.

4 Click the **Update Manager** tab.

5 Select a baseline group or baseline.

Select **All Groups and Independent Baselines** in the Attached Baseline Groups pane and **All** in the Attached Baselines pane to view the overall compliance of all attached baselines and baseline groups.

6 In the Compliance pane, select the **All Applicable** compliance status to view the overall compliance status of the selected object.

The selected object together with the number of patches, upgrades, and extensions (if the selected object is a host) appear in the bottom pane of the **Update Manager** tab.

7 Click the link in the Patches column in the bottom pane of the **Update Manager** tab.

The Patch Details window appears.

8 Click the link in the Upgrades column in the bottom pane of the **Update Manager** tab. The link indicates the number of upgrades in the selected compliance state.

The Upgrade Details window appears.

9 Click the link in the Extensions column in the bottom pane of the **Update Manager** tab. The link indicates the number of Extensions in the selected compliance state.

The Extension Details window appears.

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 13-1. 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.

Table 13-1. Update Manager Tab Panes (Continued)

Pane	Description
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 are not applicable. The applicability of a baseline is determined on the basis of whether the baseline is directly attached to the virtual machine, appliance, or host, or whether it is attached to a container object. Applicability also depends on whether the baseline contains patches, extensions, 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, extension, 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, extension, 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, extensions, or upgrades in the selected baselines and baseline groups. **Compliant** — Number of compliant virtual machines, appliances, or hosts in the selected container object.
Bottom pane	The information in this pane depends on whether you select an individual object or a container object. If you select a container object, the bottom pane of the **Update Manager** tab displays the following information: ■ A list of virtual machines, appliances, or hosts that meet the selections from the Attached Baseline Groups, Attached Baselines and Compliance panes. ■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups. If you select an individual object (such as virtual machine, appliance, or host), the bottom pane of the **Update Manager** tab displays the following information: ■ The number of patches, extensions, or upgrades included in the baseline or baseline group that you select. ■ The number of staged patches or extensions to a host. ■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups.

Compliance States for Updates

In Update Manager, update stands for all patches, extensions, and upgrades that you can apply with Update Manager. The compliance state of the updates in baselines and baseline groups that you attach to objects in your inventory is calculated after you perform a scan.

Unknown A patch is in unknown state for a target object until Update Manager successfully scans the object. A scan might not succeed if the target object is of an unsupported version, if Update Manager lacks metadata, or if the patch metadata is corrupt.

Missing Missing compliance state indicates that the update is applicable to the target object, but not yet installed. You must perform a remediation on the target object with this update, so that the update becomes compliant.

Not Applicable Not applicable compliance state indicates that the patch is not applicable to the target object. A patch might be in not applicable compliance state for one of the following reasons:

- There are other patches in the Update Manager patch repository that obsolete this patch.
- The update does not apply to the target object. For example, if you attach and scan a Linux virtual machine against a baseline containing Windows patches.

Conflict The update conflicts with either an existing update on the host or another update in the Update Manager patch repository. Update Manager reports the type of conflict. 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 can take action to resolve the conflict.

Obsoleted By Host This compliance state applies mainly to patches. The target object has a newer version of the patch. For example, if a patch has multiple versions, after you apply the latest version to the host, the earlier versions of the patch are in Obsoleted By Host compliance state.

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.

Installed Installed compliance state indicates that the update is installed on the target object, and no further user action is required.

Staged This compliance state applies to host patches and host extensions. It indicates that the update is copied from the Update Manager repository to the host, but is not yet installed. Staged compliance state might occur only when you scan hosts running ESX/ESXi 4.0 and later.

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	New module compliance state indicates that the update is a new module. An update in this compliance state cannot be installed when it is part of a host patch baseline. When it is part of a host extension baseline, the new module state signifies that the module is missing on the host and can be provisioned by remediation. The compliance state of the baseline depends on the type of baseline containing the update in new module state. If the baseline is a host patch baseline, the overall status of the baseline is compliant. If the baseline is a host extension baseline, the overall status of the baseline is not compliant.
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 if a 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.
Conflicting New Module	The host update is a new module that provides software for the first time, but is in conflict with either an existing update on the host or another update in the Update Manager repository. Update Manager reports the type of conflict. 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.

Baseline and Baseline Group Compliance States

Compliance states are computed after you scan the objects in your inventory against baselines or baseline groups. Update Manager computes the compliance state based on the applicability of the patches, extensions, and upgrades contained in attached baselines or baseline groups.

Compliant

Compliant state indicates that all baselines in the attached baseline group and all patches, extensions, and upgrades in the baseline are compliant. Compliant state requires no further action. If a baseline contains patches or upgrades that are not relevant to the target object, the individual updates, and baselines or baseline groups that contain them, are treated as not applicable, and represented as compliant. For example, if you attach a virtual machine patch baseline to a virtual appliance, the baseline is displayed as compliant. Compliant are also host patch baselines containing extensions or patches in Obsoleted By Host state.

Compliant state of baselines, baseline groups, or the updates included in the baselines occurs under the following conditions:

- Baselines and baseline groups are compliant when all updates in the baseline or baseline group are either installed on the target object, obsoleted by host, or are not applicable to the target object.
- The updates in a baseline are compliant when they are installed on the target object, or are not applicable to the object.

A baseline or baseline group can be compliant if all of the updates or baselines in the group are compliant.

Non-Compliant

Non-compliant state indicates implies that one or more baselines in a baseline group, or one or more patches, extensions, or upgrades in a baseline are applicable to the target object, but are not installed (missing) on the target. You must remediate the target object to make it compliant.

When a baseline contains a non-compliant update, the overall status of the baseline is non-compliant. When a baseline group contains a non-compliant baseline, the overall status of the baseline group is non-compliant. The non-compliant state takes precedence over incompatible, unknown, and compliant states.

Unknown

When you attach a baseline or a baseline group to a vSphere object, and you do not scan the object, the state of the baseline or baseline group is Unknown. This state indicates that a scan operation is required, that the scan has failed, or that you initiated a scan on an unsupported platform (for example, you performed a VMware Tools scan on a virtual machine running on an ESX 3.5 host).

When a baseline contains updates in compliant and unknown states, the overall status of the baseline is unknown. When a baseline group contains unknown baselines as well as compliant baselines, the overall status of the baseline group is unknown. The unknown compliance state takes precedence over compliant state.

Incompatible

Incompatible state requires attention and further action. You must determine the reason for incompatibility by probing further. You can remediate the objects in this state, but there is no guarantee that the operation will succeed. In most cases Update Manager provides sufficient details for incompatibility. For more information about incompatible compliance state, see "Incompatible Compliance State," on page 169.

When a baseline contains updates in incompatible, compliant, and unknown states, the overall status of the baseline is incompatible. When a baseline group contains incompatible, unknown, and compliant baselines, the overall status of the baseline group is incompatible. The incompatible compliance state takes precedence over compliant and unknown compliance states.

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 in the Patch Details window 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 patch in the Patch Details window.

The columns in the patch details window table and their descriptions are listed in Table 13-2.

Table 13-2. Patch Details Window

Option	Description
Update Name	Name of the update.
Vendor	Vendor of the update.
Compliance	Compliance status of the patch. The state might be Missing (Non-compliant), Not Applicable, Unknown, Installed (Compliant), and so on.
Vendor ID	Vendor assigned identification code of the update.
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	The action that you must take to apply the update. This action might include a reboot of the system or entering maintenance mode (for hosts).
Release Date	Release date of the update.

Viewing Extension Details

The Extension Details window displays a table of the extensions in the order of their compliance status with the selected host.

You can obtain complete information about an extension by double-clicking an extension in the Extension Details window.

The information represented in the Extension Details window is listed in Table 13-3.

Table 13-3. Extension Details Window

Option	Description
Update Name	Name of the update.
Compliance	Compliance status of the extension. The value can be Missing (Non-compliant patch to an installed extension), New Module (non-compliant extension that can be installed for the first time), Not Applicable, Unknown, Installed (compliant), Conflicting New Module (extension can be installed, but is conflicting with some package on the host or some update in the patch repository), and so on.
Vendor	Vendor of the update.
Vendor ID	Vendor assigned identification code of the update.
Severity	Severity of the update. For hosts the severity status might be Critical, General, Security, and so on.
Impact	The action that you must take to apply the update. This action might include a reboot of the system or entering maintenance mode.
Release Date	Release date of the update.

Viewing Upgrade Details

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

The information represented in the Upgrade Details window for host upgrades is displayed in Table 13-4.

Table 13-4. Host Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	The type baseline type is host upgrade.
Baseline Description	Description of the baseline, if any. If the baseline has no description, it is not displayed.
Compliance State	Compliance status for the upgrade. It represents the compliance state of the selected object against the upgrade baseline.
Upgrade Release	Displays the upgrade release included in the baseline. It can be either partial or complete.
Upgrade Version	Target version of the upgrade baseline.
Can upgrade from	Hosts of versions from which the upgrade can be performed with the selected upgrade baseline.

Table 13-4. Host Upgrade Details Window (Continued)

Option	Description
Cannot upgrade from	Hosts of version from which an upgrade cannot be performed with the selected baseline.
Additional options	Lists the COS VMDK location and post-upgrade options that you have specified. These options can be used and applied only for upgrades of ESX hosts from version 3.x to versions 4.0.x and 4.1 although they are always displayed. ■ VMDK Location ■ Roll Back on Failure ■ Post-Upgrade Script

The information represented in the Upgrade Details window for VMware Tools and virtual hardware upgrades is listed in Table 13-5.

Table 13-5. VMware Tools and Virtual Machine Hardware Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	Type of the baseline. The values can be VMware Tools upgrade or virtual machine hardware upgrade.
Baseline Description	Description of the baseline.
Compliance State	The compliance status for the upgrade. It represents the compliance state of the selected object against the upgrade baseline.
VM Tools Status	Status of VMware Tools on the machine.
Current Hardware Version	Hardware version of the virtual machine.
Target Hardware Version	Target hardware version of the virtual machine.

The information represented in the Upgrade Details window for virtual appliance upgrades is listed in Table 13-6

Table 13-6. Virtual Appliance Upgrade Details Window

Option	Description
Vendor	Vendor of the upgrade.
Product	Product installed on the virtual appliance, for example guest operating system.
Version	Target version of the product.
Compliance	Compliance status of the virtual appliance upgrade.
Severity	Severity of the upgrade.
Release Date	Release date of the upgrade.

14 Remediating vSphere Objects

You can remediate virtual machines, virtual appliances, and hosts using either user-initiated remediation or scheduled remediation at a time that is convenient for you.

You can remediate virtual machines and appliances together.

If your vCenter Server is 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.

To remediate vSphere objects, you need the **Remediate to Apply Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see the *vSphere Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

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 all the virtual machines in the vSphere inventory at the same time, using baseline groups containing the following 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 object 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 impossible if VMware Tools is not installed, is out of date, or is 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 the powered off or suspended state before remediation, Update Manager powers it on. After the upgrade completes, Update Manager restarts the machine and restores the original power state of the virtual machine.

During the virtual hardware upgrade, the virtual machines must be shut down. If a virtual machine is powered on, Update Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

Remediating Hosts

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

Remediation of Hosts in a Cluster

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 remediated hosts in the cluster stay at the updated level. The ones that are not remediated after the failed host remediation are not updated. If a host in a DRS enabled cluster runs a virtual machine on which Update Manager or vCenter Server are installed, DRS first attempts to migrate the virtual machine running vCenter Server or Update Manager to another host, so that the remediation succeeds. In case the virtual machine cannot be migrated to another host, the remediation fails for the host, but the process does not stop. Update Manager proceeds to remediate the next host in the cluster.

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

Remediation of hosts in a cluster requires that you temporarily disable cluster features such as VMware DPM and HA admission control. You must also turn off FT if it is enabled on any of the virtual machines on a host, and disconnect the removable devices connected to the virtual machines on a host, so that they can be migrated with vMotion. Before you start a remediation process, you can generate a report that shows which cluster, host, or virtual machine is with enabled cluster features. For more information, see "Cluster Remediation Options Report," on page 123.

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.

Remediation Against Baseline Groups

When you remediate hosts against baseline groups containing an upgrade baseline and patch or extension 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.

Host Upgrade Remediation

When you upgrade hosts, all third-party modules are reserved after the upgrade. In case of conflicts between the third-party modules on the host and the upgrade release bundle, Update Manager searches for a suitable upgrade of the third-party module in the patch repository. This upgrade of the third-party module must match the upgrade bundle. If Update Manager finds such an upgrade for the module, it installs the upgrade on the host together with the upgrade bundle. Otherwise, Update Manager reports the conflicts and does not upgrade the host.

Host Patch Remediation

Update Manager handles host patches in the following ways:

- If a patch in a patch baseline requires the installation of another patch, Update Manager detects the prerequisite in the patch repository 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, consider a baseline that contains patch A and patch C, and patch A conflicts with patch B, which is already installed on the host. If patch C obsoletes patch B, and patch C is not in conflict with patch A, the remediation process installs patches A and C.
- If a patch is in conflict with the patches in the Update Manager patch repository and is not in conflict with the host, after a scan, Update Manager reports this patch as a conflicting one. You can stage and apply the patch to the host.
- When multiple versions of the same patch are selected, Update Manager installs the latest version and skips the earlier versions.

During patch remediation, Update Manager automatically installs the prerequisites of patches.

With Update Manager 4.1, you can remediate hosts against offline bundles that you have imported manually.

Host Extension Remediation

During extension remediation, Update Manager does not automatically install the prerequisites of the extension. This might cause some remediations to fail. If the missing prerequisite is a patch, you can add it to a patch baseline. If the missing prerequisite is an extension, you can add it to the same or another extension baseline. You can then remediate the host against the baseline or baselines that contain the prerequisite and the original extension. For more information about troubleshooting failures of host extension remediation or staging, see "Host Extension Remediation or Staging Fails Due to Missing Prerequisites," on page 164.

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.x and ESX 4.1 patch remediation process, Update Manager operates with vSphere Installation Bundles (`.vib` files). A bundle is the smallest installable unit on an ESX 4.0.x and ESX 4.1 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 3.x 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 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.x or ESX 4.1, and reconnected to the vCenter Server system. During the upgrade, the ESX 3.x installation is moved from its own partition to a VMDK (its own virtual disk) located in the datastore. If the upgrade fails, you can roll back to the previous version.

Update Manager 4.1 supports upgrades from ESX 3.0.0 and later as well as from ESX 3i version 3.5 and later to ESX/ESXi 4.0.x and 4.1. The remediation from version 4.0 to version 4.0.x is a patching operation, while the remediation from version 4.0.x to 4.1 is considered an upgrade.

NOTE You cannot upgrade ESX 3.0.x hosts directly to ESX 4.1. To upgrade ESX hosts of version 3.0.x to version 4.1 you must first upgrade them to version 4.0 or 4.0.x and then upgrade to 4.1.

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 in 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.

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.x or ESX 4.1 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.x or ESXi 4.1 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.x and ESXi 4.1 host stores up to two builds, one boot build and one standby build.

IMPORTANT Update Manager does not remediate PXE booted ESXi hosts.

Remediation of ESXi hosts from version 4.0 to 4.0.x is a patching process, while the remediation from version 4.0.x to 4.1 is considered an upgrade.

Stage Patches and Extensions to ESX/ESXi Hosts

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

You can reduce the downtime during remediation, by staging patches and extensions whose installation requires that a host enters maintenance mode. Staging patches and extensions itself does not require that the hosts enter maintenance mode.

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 patch 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 prescan and postscan operations, and updates the compliance state of the baseline.

After you stage patches or extensions to hosts, you should remediate the hosts against all staged patches or extensions.

After a successful remediation of hosts, the host deletes all staged patches or extensions from its cache regardless of whether they were applied during the remediation. The compliance state of patches or extensions that were staged but not applied to the to the hosts reverts from Staged to its previous value.

IMPORTANT Staging patches and extensions is supported for hosts that are running ESX/ESXi 4.0 and later. You cannot stage patches to PXE booted ESXi hosts.

Prerequisites

To stage patches or extensions to hosts, first attach a patch or extension baseline or a baseline group containing patches and extensions to the host.

To stage patches or extensions to ESX/ESXi hosts, you need the **Stage Patches and Extensions** privilege. For more information about managing users, groups, roles, and permissions, see *vSphere Datacenter Administration Guide*. For a list of Update Manager privileges and their descriptions, see "Update Manager Privileges," on page 82.

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 On the Baseline Selection page of the Stage wizard, select the patch and extension baselines to stage.

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

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

5 (Optional) Deselect the patches and extensions to exclude from the stage operation.

6 (Optional) To search within the list of patches and extensions, 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 and extensions for the specific host is displayed in the Patches and Extensions columns in the bottom pane of the **Update Manager** tab.

After a remediation is successfully completed, all staged patches and extensions, whether installed or not during the remediation, are deleted from the host.

Remediate Hosts Against Patch or Extension Baselines

You can remediate hosts against attached patch or extension baselines.

The remediation process for host extension baselines is similar to the remediation process for host patch baselines. You can remediate a host against a single baseline or multiple baselines of the same type. To remediate against baselines of different types, you must create a baseline group. For more information about remediating hosts against baseline groups containing host upgrade, patch, and extension baselines, see "Remediate Hosts Against Baseline Groups," on page 121.

To upgrade hosts from version 4.0 to version 4.0.x, you must use a patch baseline.

Prerequisites

Before remediating a host against patch or extension baselines, ensure that a baseline is attached to the host.

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

Procedure

1 On the **Home** page, select **Hosts and Clusters**, and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

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.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and baselines to apply.

4 (Optional) Select the hosts that you do want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process and click **Next**.

6 (Optional) On the Dynamic Patches and Extensions to Exclude page, review the list of patches or extensions to be excluded and click **Next**.

7 On the Host Remediation Options page, enter a unique name, and optionally a description, for the task.

8 Select **Immediately** to begin the process right after you complete the wizard, or specify a time for the remediation process to begin.

9 Specify the failure response for the remediation process from the **Failure response** drop-down menu, the delay in the retry, 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** field. If Update Manager cannot put a host into maintenance mode, you can take an action to make sure that the operation succeeds next time when Update Manager tries to put the host into maintenance mode. For example, you can manually power off the virtual machines or migrate them to another host using vMotion to ensure that entering maintenance mode is successful next time.
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.

10 (Optional) Configure the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. FT requires that the hosts, on which the Primary and Secondary virtual machines run, are of the same version and have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.

11 (Optional) Generate a pre-remediation check report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

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

Remediate Hosts Against an Upgrade Baseline

You can remediate ESX/ESXi hosts against a single attached upgrade baseline at a time. You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline containing both ESX and ESXi upgrade release files.

Update Manager 4.1 supports upgrades from ESX 3.0.0 and later as well as from ESX 3i version 3.5 and later to ESX/ESXi 4.0.x and 4.1. The remediation from version 4.0 to version 4.0.x is a patching operation, while the remediation from version 4.0.x to 4.1 is considered an upgrade.

NOTE You cannot upgrade ESX 3.0.x hosts directly to ESX 4.1. To upgrade ESX hosts of version 3.0.x to version 4.1 you must first upgrade them to version 4.0 or 4.0.x and then upgrade to 4.1.

Prerequisites

To remediate a host against an upgrade baseline, attach the baseline to the host.

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

Procedure

1 On the **Home** page, select **Hosts and Clusters**, and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

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.

3 On the Remediation Selection page of the Remediate wizard, select the upgrade baseline to apply.

4 (Optional) Select the hosts that you do want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

The End User License Agreement page is applicable only when you upgrade ESX hosts from version 3.x to version 4.0.x and 4.1.

6 (Optional) On the ESX 4.x Upgrade page, click the links of the settings that you want to edit.

Option	Description
COS VMDK location (ESX only)	In the ESX 4.x COS VMDK Location window, specify the datastore location for the VMDK to migrate the COS of the ESX host.
Rollback on failure (ESX only)	In the ESX 4.x Post Upgrade Options window, specify whether to disable rollback in case of failure.
Post-Upgrade script (ESX only)	In the ESX 4.x 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.x Upgrade page options in the Remediate wizard are applicable only when you upgrade ESX hosts from version 3.x to version 4.0.x and 4.1.

7 On the Host Remediation Options page, enter a unique name, and optionally a description, for the task.

8 Select **Immediately** to begin the process right after you complete the wizard, or specify a time for the remediation process to begin.

9 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.

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** field. If Update Manager cannot put a host into maintenance mode, you can take an action to make sure that the operation succeeds next time when Update Manager tries to put the host into maintenance mode. For example, you can manually power off the virtual machines or migrate them to another host using vMotion to ensure that entering maintenance mode is successful next time.
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.

10 Disable any removable media devices connected to the virtual machines on the host, and click **Next**.

11 (Optional) Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. FT requires that the hosts, on which the Primary and Secondary virtual machines run, are of the same version and have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.

12 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next.**

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

Remediate Hosts Against Baseline Groups

You can remediate hosts against attached groups of upgrade, patch, and extension baselines. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines.

Prerequisites

Before remediating a host against a baseline group containing an upgrade baseline and patch or extension baselines, ensure that a baseline group is attached to the host.

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

Procedure

1 On the **Home** page, select **Hosts and Clusters**, and click the **Update Manager** tab.

2 Right-click the inventory object you want to remediate and select **Remediate**.

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.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and baselines to apply.

4 (Optional) Select the hosts that you do want to remediate and click **Next**.

If you have chosen to remediate a single host and not a container object, the host is selected by default.

5 On the End User License Agreement page, accept the terms and click **Next**.

The End User License Agreement page is applicable only when you upgrade ESX hosts from version 3.x to version 4.0.x and 4.1.

6 (Optional) On the ESX 4.x Upgrade page, click the links of the settings that you want to edit.

Option	Description
COS VMDK location (ESX only)	In the ESX 4.x COS VMDK Location window, specify the datastore location for the VMDK to migrate the COS of the ESX host.
Rollback on failure (ESX only)	In the ESX 4.x Post Upgrade Options window, specify whether to disable rollback in case of failure.
Post-Upgrade script (ESX only)	In the ESX 4.x 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.x Upgrade page options in the Remediate wizard are applicable only when you upgrade ESX hosts from version 3.x to version 4.0.x and 4.1.

7 Click **Next**.

8 (Optional) On the Patches and Extensions page, deselect specific patches or extensions to exclude them from the remediation process and click **Next**.

9 (Optional) On the Dynamic Patches and Extensions to Exclude page, review the list of patches or extensions to be excluded and click **Next**.

10 On the Host Remediation Options page, enter a unique name, and optionally a description, for the task.

11 Select **Immediately** to begin the process right after you complete the wizard, or specify a time for the remediation process to begin.

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.

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** field. If Update Manager cannot put a host into maintenance mode, you can take an action to make sure that the operation succeeds next time when Update Manager tries to put the host into maintenance mode. For example, you can manually power off the virtual machines or migrate them to another host using vMotion to ensure that entering maintenance mode is successful next time.
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 Disable any removable media devices connected to the virtual machines on the host, and click **Next**.

14 (Optional) Edit the cluster remediation options.

The Cluster Remediation Options page is available only when you remediate hosts in a cluster.

Option	Details
Disable Distributed Power Management (DPM) if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active DPM. DPM monitors the resource use of the running virtual machines in the cluster. If sufficient excess capacity exists, DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. Putting hosts into standby mode might interrupt remediation.
Disable High Availability admission control if it is enabled for any of the selected clusters.	Update Manager does not remediate clusters with active HA admission control. Admission control is a policy used by VMware HA to ensure failover capacity within a cluster. If HA admission control is enabled during remediation, the virtual machines within a cluster might not migrate with vMotion.
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host. FT requires that the hosts, on which the Primary and Secondary virtual machines run, are of the same version and have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.

15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next.**

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

Cluster Remediation Options Report

The Cluster Remediation Options Report window contains a table with name of the cluster, host, or virtual machine on which an issue is reported, as well as recommendations on how to fix the issue.

Table 14-1 lists the possible issues, changes required for the remediation, and additional details.

Table 14-1. Cluster Remediation Options Report

Current Configuration/Issue	Changes applied for remediation	Details
A CD/DVD drive is attached.	Disconnect the CD/DVD drive.	Any CD/DVD drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
A floppy drive is attached.	Disconnect the floppy drive.	Any floppy drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
HA admission control prevents migration of the virtual machine.	Disable HA admission control.	HA admission control prevents migration of the virtual machines with vMotion and the hosts cannot enter maintenance mode. Disable HA admission control on a cluster to make sure that remediation is successful.
DPM is enabled on the cluster.	Disable DPM on the cluster.	DPM might put hosts into standby mode before or during remediation and Update Manager cannot remediate them. Disable DPM on a cluster to ensure that the remediation process is successful.

Table 14-1. Cluster Remediation Options Report (Continued)

Current Configuration/Issue	Changes applied for remediation	Details
EVC is disabled on the cluster.	Enable EVC on the cluster.	EVC helps ensure vMotion compatibility between hosts in a cluster. When enabled on compatible hosts, EVC ensures that all hosts in a cluster present a common set of CPU features to virtual machines. EVC must be enabled so that the virtual machines are migrated successfully within the cluster during remediation.
DRS is disabled on the cluster. This prevents migration of the virtual machines.	Enable DRS on the cluster.	DRS enables vCenter Server to automatically place and migrate virtual machines on hosts to attain the best use of cluster resources.
FT is enabled for a VM on a host in the cluster. FT prevents successful remediation.	Disable FT on the virtual machine.	If FT is enabled on for any of the virtual machines on a host, Update Manager does not remediate that host.

Remediating Virtual Machines and Virtual Appliances

You can manually remediate virtual machines and virtual appliances at the same time against baseline groups containing patch and upgrade baselines. You can also schedule a remediation operation at a time that is convenient for you.

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.

You can remediate only powered-on virtual appliances that are created with VMware Studio 2.0 and later.

IMPORTANT Update Manager 4.1 supports remediation of virtual appliances and vApps created with VMware Studio 2.0 and later.

Remediation of Templates

A template is a master copy of a virtual machine that can be used to create and provision new virtual machines. You can remediate templates by using Update Manager..

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, you must start the template 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 during remediation, 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 to keep them indefinitely or for a specific period of time. After the remediation is completed, you can validate the remediation and delete the snapshots if you do not need them.

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.

Remediate Virtual Machines and Virtual Appliances

You can manually remediate virtual machines and virtual appliances immediately, or can schedule a remediation at a time that is convenient for you.

Prerequisites

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

After you import a VMware Studio created virtual appliance in the vSphere Client, power it on so that it is discovered as a virtual appliance.

Procedure

1 On the Home page, select **VMs and Templates** and click the **Update Manager** tab.

2 Right-click an object from the inventory and select **Remediate**.

All virtual machines and appliances under the selected object are also remediated.

3 On the Remediation Selection page of the Remediate wizard, select the baseline group and baselines to apply.

4 Select the virtual machines and appliances that you want to remediate and click **Next**.

5 (Optional) On the Patches page, deselect the check boxes for patches that you want to exclude from the remediation process and click **Next**.

6 (Optional) Review the list of excluded patches and click **Next**.

7 On the Schedule page, enter a name and optionally a description for the task.

8 Select **Immediately** to begin the remediation process right after you complete the wizard, or enter specific times for powered on, powered off, or suspended virtual machines.

9 (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 (or virtual appliance) is taken before remediation. If the virtual machine (or 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 by using the Remediate wizard.

You can schedule remediation for all hosts or all virtual machines in a container object from the vSphere inventory. You can perform scheduled orchestrated upgrades of the hosts or virtual machines in a selected container object.

To schedule remediation, you must enter a specific time for the remediation process on the Host Remediation Options page (for hosts) or the Schedule page (for virtual machines or appliances) of the Remediate wizard.

If your vCenter Server system is 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. From the navigation bar, you can specify an Update Manager instance by selecting the name of the vCenter Server system with which the Update Manager instance is registered.

15 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 are completed.

You can view events in the Update Manager Administration view.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- 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 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.

   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 displays events that help you monitor the processes that the system is completing.

Table 15-1. Update Manager Events

Type	Message Text	Action
Info	Successfully downloaded guest patch definitions. New patches: *number_of_patches*.	
Error	Could not download guest patch definitions.	Check your network connection to make sure that your metadata source is reachable.
Info	Successfully downloaded guest patch definitions for UNIX. New patches: *number_of_patches*.	
Error	Could not download guest patch definitions for UNIX.	Check your network connection to make sure that your metadata source is reachable.
Info	Successfully downloaded host patch definitions. New patches: *number_of_patches*.	
Error	Could not download host patch definitions.	Check your network connection to make sure that your metadata source is reachable.
Info	Successfully downloaded guest patch packages. New packages: *number_of_packages*.	
Error	Could not download guest patch packages.	Check your network connection to make sure that your patch source is reachable.
Info	Successfully downloaded guest patch packages for UNIX. New packages: *number_of_packages*.	
Error	Could not download guest patch packages for UNIX.	Check your network connection to make sure that your patch source is reachable.
Info	Successfully downloaded host patch packages. New packages: *number_of_packages*.	
Error	Could not download host patch packages.	Check your network connection to make sure that your patch source is reachable.
Info	Successfully downloaded notifications. New notifications: *number_of_notifications*.	
Error	Could not download notifications.	Check your network connection.
Info	Successfully scanned *vSphere_object_name* for patches.	
Error	Scanning of *vSphere_object_name* is canceled by user.	
Error	Could not scan *vSphere_object_name* for patches.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for scan errors.
Warning	Found a missing patch: *patch_name* when scanning *vSphere_object_name*. Re-downloading patch definitions might resolve this problem.	
Info	Successfully scanned *virtual_appliance_name* for VA upgrades.	
Error	Could not scan *virtual_appliance_name* for VA upgrades.	
Info	Successfully scanned *vSphere_object_name* for VMware Tools upgrades.	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not scan *vSphere_object_name* for VMware Tools upgrades.	
Warning	VMware Tools is not installed on *vSphere_object_name*. VMware vCenter Update Manager supports upgrading only an existing VMware Tools installation.	
Warning	VMware Tools upgrade was not performed on *virtual_machine_name*. VMware Tools upgrade is supported only for VMs on ESX 4.0 hosts and higher.	
Error	Could not scan *virtual_machine_name* because of an invalid state: *virtual_machine_connection_state*.	Check the state of the virtual machine. Reboot the virtual machine to facilitate scanning.
Error	Could not scan *host_name* because of an invalid state: *host_connection_state*.	Check the state of the host. Reboot the host to facilitate scanning.
Info	Remediation succeeded for *vSphere_object_name*.	
Error	Remediation did not succeed for *vSphere_object_name*, *error_message*.	Check the Update Manager log (`vmware-vum-server-log4cpp.log`) for remediation errors.
Info	VMware Tools upgrade succeeded for *vSphere_object_name*.	
Error	VMware Tools upgrade did not succeed for *vSphere_object_name*.	
Error	Could not remediate *virtual_machine_name* because of an invalid state: *virtual_machine_connection_state*.	Check the virtual machine's state. Restart the virtual machine to facilitate remediation.
Error	Could not remediate *host_name* because of an invalid state: *host_connection_state*.	Check the state of the host. Restart the host to facilitate remediation.
Info	Staging succeeded for *vSphere_object_name*.	
Error	Staging did not succeed for *vSphere_object_name*, *error_message*.	
Error	Could not stage patches to *host_name* because of an invalid state: *host_connection_state*.	
Error	Patch scan or remediation is not supported on *vSphere_object_name* because of unsupported or unknown OS: *operating_system_name*.	
Error	Cannot remediate *vSphere_object_name* for patches. Remediation of Linux VMs is not supported.	
Error	Cannot scan *vSphere_object_name* for patches. Scan of powered off or suspended 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.
Info	VMware vCenter Update Manager notification download alert	
Info	VMware vCenter Update Manager recall alert	
Info	VMware vCenter Update Manager recall fix alert	
Info	VMware vCenter Update Manager informative notification (moderate) alert	
Info	VMware vCenter Update Manager informative notification (important) alert	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	VMware vCenter Update Manager informative notification (critical) alert	
Error	Could not scan *virtual_machine_name* because host *host_name* is of unsupported version *host_version*.	For the latest information on which virtual machines can be scanned, see the release notes.
Error	Could not remediate *virtual_machine_name* because host *host_name* is of unsupported version *host_version*.	For the latest information on which hosts can be scanned, see the release notes.
Error	Could not scan *host_name* because it is of unsupported version *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.
Error	Could not stage patches to *host_name* because it is of unsupported version *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	Could not remediate *host_name* because it is of unsupported version *host_version*.	Hosts of versions later than ESX 3.0.3 and ESX 3i can be remediated. For the latest information on which ESX/ESXi hosts can be remediated, see the release notes.
Info	VMware vCenter Update Manager Guest Agent successfully installed on *virtual_machine_name*.	
Error	Could not install VMware vCenter Update Manager Guest Agent on *virtual_machine_name*. Make sure that the VM is powered on.	Update Manager Guest Agent is required for remediating virtual machines.
Error	Could not install VMware vCenter Update Manager Guest Agent on *virtual_machine_name* because VMware Tools is not installed or is of an incompatible 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 *vSphere_object_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 could not respond in time on *virtual_machine_name*. Verify that the VM is powered on and that the Guest Agent is running.	
Error	An internal error occurred in communication with VMware vCenter Update Manager Guest Agent on *virtual_machine_name*. Verify that the VM is powered on and retry the operation.	
Error	VMware vCenter Update Manager Guest Agent could not access the DVD drive on *virtual_machine_name*. Verify that a DVD drive is available and retry the operation.	
Error	An unknown internal error occurred during the required operation on *virtual_machine_name*. Check the logs for more details and retry the operation.	
Error	Could not install patches on *vSphere_object_name*.	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Installation of patches *patch_ID* on *vSphere_object_name*. Status: *message*.	
Info	The following additional patches are included to resolve a conflict for installation on *vSphere_object_name*: *message*.	
Info	To resolve a conflict for installation on *vSphere_object_name*, the following additional patches might need to be included in the baseline: *message*.	
Info	VMware vCenter Update Manager could not find patches to resolve the conflict for installation on *vSphere_object_name*.	
Info	Installation of patches succeeded on *vSphere_object_name*.	
Info	Start rebooting host: *host_name*.	
Info	Waiting for host: *host_name* to reboot.	
Info	Host *host_name* is successfully rebooted.	
Error	Cannot reboot host *host_name*.	
Error	Cannot stage patch *patch_name* to *host_name*.	
Error	Could not stage patch *patch_name* to *host_name*.	
Info	Staging of patch to *host_name* succeeded.	
Error	Could not reboot host *host_name*.	
Error	Could not stage patches to *host_name*.	
Info	Started staging of patches *patch_IDs* on *host_name*.	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Could not scan orphaned VM *virtual_machine_name*.	
Info	Could not remediate orphaned VM *virtual_machine_name*.	
Error	Could not download 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 VM might be incomplete.	
Info	Canceling task on *vSphere_object_name*.	
Warning	There are running tasks for the entity *vSphere_object_name* that cannot finish within a specific time. The operation will stop.	
Warning	Action is not supported for Linux VM/VA *virtual_machine_or_virtual_appliance_name*. VMware Tools is not installed or the machine cannot start.	
Warning	Action is not supported for offline or suspended virtual appliance *virtual_appliance_name*.	A scan or remediation process is not supported for offline or suspended virtual appliance. Power on the virtual appliance to scan or remediate it.
Info	Successfully discovered virtual appliance *virtual_appliance_name*.	
Info	Could not discover virtual appliance *virtual_appliance_name*.	An error occurred during the discovery of the virtual appliance.

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
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	No repository address is set for virtual appliance *virtual_appliance_name*. The appliance does not support updates by vCenter Server.	
Info	Open *vSphere_object_name* firewall ports.	
Info	Close *vSphere_object_name* firewall ports.	
Info	Patch definitions for *vSphere_object_name* are missing. Download patch definitions first.	
Info	Patch definition for *vSphere_object_name* is corrupt. Check the logs for more details. Re-downloading patch definitions might 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.	
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 postinstallation script.	
Info	Host upgrade installer completed.	
Error	Host upgrade installer stopped.	
Info	Host upgrade in progress.	
Error	Host CPU not supported. A 64-bit 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 must be on the same disk as the boot partition.	
Error	Error in `GRUB` configuration.	
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.	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Unsupported services found on the host.	
Warning	Unsupported configuration found on the host. This configuration cannot 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.	
Warning	Active directory must be disabled on host.	
Error	Upgrade precheck script error.	
Info	Successfully scanned *vSphere_object_name* for Virtual Hardware upgrades.	
Error	Could not scan *vSphere_object_name* for Virtual Hardware upgrades.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools is not the latest version. To upgrade virtual hardware, VMware Tools must be the latest version.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools state is unknown. To upgrade virtual hardware, VMware Tools must be the latest version.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools is not installed. To upgrade virtual hardware, VMware Tools must be the latest version.	
Error	Virtual Hardware upgrade did not succeed for *virtual_machine_name*, because VMware Tools state is not managed by VMware vSphere. To upgrade virtual hardware, VMware Tools must be the latest version.	
Warning	Virtual Hardware upgrade skipped for *virtual_machine_name*. Virtual Hardware upgrade is supported only for VMs on ESX 4.0 hosts and higher.	
Info	Virtual Hardware upgrade succeeded for *vSphere_object_name*.	
Error	Could not perform Virtual Hardware upgrade on *vSphere_object_name*.	
Error	VM *virtual_machine_name* has either VMware vCenter Update Manager or VMware vCenter Server installed. This VM will be ignored for scan and remediation.	Virtual machines on which Update Manager or vCenter Server is installed are not scanned or remediated.
Error	The host *host_name* has a VM *virtual_machine_name* with VMware vCenter Update Manager or VMware vCenter Server installed. The VM must be moved to another host for the remediation to proceed.	If a virtual machine on which Update Manager or vCenter Server is installed is on a host that is going to be remediated, the virtual machine must be migrated to another host.
Error	Error while waiting for VMware Tools to respond. Verify that 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. Upgrade VMware Tools manually.	
Info	Suspended VM *virtual_machine_name* has been skipped.	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Cannot remediate host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not remediate hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot scan host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not scan hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot stage host *host_name* because it is a part of a VMware DPM enabled cluster.	Update Manager does not stage patches to hosts in clusters with enabled VMware DPM. Disable VMware DPM.
Warning	Cannot remediate host *host_name* because it is a part of a HA admission control enabled cluster.	Update Manager does not remediate hosts in clusters with enabled HA admission control. Disable HA admission control.
Warning	Cannot remediate host *host_name* because it contains one or more Primary or Secondary VMs on which FT is enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.
Warning	Cannot remediate host *host_name* because it is a part of a VMware DPM enabled cluster and contains one or more Primary or Secondary VMs on which FT is enabled.	Update Manager does not remediate hosts in clusters with enabled VMware DPM and hosts on which virtual machines are with enabled FT. Disable VMware DPM and FT.
Warning	Host *host_name* has FT enabled VMs. If you apply different patches to hosts in a cluster, FT cannot be re-enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.
Warning	Host *host_name* has FT enabled VMs. The host on which the Secondary VMs reside is not selected for remediation. As a result FT cannot be re-enabled.	Update Manager does not remediate hosts in clusters on which virtual machines are with enabled FT. Disable FT.
Warning	Cannot remediate host *host_name* because it has VMs with a connected removable device. Disconnect all removable devices before remediation.	Update Manager does not remediate hosts in clusters on which the virtual machines are with connected removable devices such as CD/DVD or floppy drives. Disconnect any removable devices from the virtual machines on a host.
Error	Cannot migrate VM *virtual_machine_name* from *source_host_name* to *destination_host_name*.	If virtual machines cannot be migrated with vMotion, and the host cannot enter maintenance mode, Update Manager does not remediate the host.
Error	Cannot enable FT for VM *virtual_machine_name* on host *host_name*.	
Error	Cannot disable FT for VM *virtual_machine_name* on host *host_name*.	Update Manager does not scan, stage, or remediate hosts on which virtual machines are with enabled FT.
Error	Cannot check compatibility of the VM *virtual_machine_name* for migration with vMotion to host *host_name*.	
Error	VMware vCenter Update Manager could not restore HA admission control/DPM settings for cluster *cluster_name* to their original values. These settings have been changed for patch installation. Check the cluster settings and restore them manually.	

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Cannot deploy upgrade agent on host.	
Error	Unable to verify host reboot. To complete the upgrade reboot the host *host_name* manually.	Reboot the host.
Error	Cannot run upgrade script on host.	
Error	Host patch *patch_name* conflicts with patch *patch_name* included in the baseline and cannot be staged. Remove either of the patch from the baseline and retry the stage operation.	Remove one of the conflicting patches and retry the stage operation.
Error	Host patch *patch_name* conflicts with the package *package_name* installed on the host and cannot be staged. Remove the patch from the baseline or include any suggested additional patches in the baseline and retry stage operation.	Remove the conflicting patch from the baseline and retry the stage
Error	Host patch *patch_name* conflicts with patch *patch_name* included in the baseline and cannot be remediated. Remove either of the patch from the baseline and retry the remediation.	Remove one of the conflicting patches from the baseline and retry the remediation.
Error	Host patch *patch_name* conflicts with the package *package_name* installed on the host and cannot be remediated. Remove the patch from the baseline or include any suggested additional patches in the baseline and retry remediation operation.	Remove the conflicting patch from the baseline and retry the remediation.
Info	Package *package_name* is successfully imported.	
Error	Import of package: *package_name* did not succeed.	
Info	*number_bulletins* new bulletins uploaded successfully through offline bundle.	
Error	Host patch offline bundle upload did not succeed.	
Info	Host patch offline bundle upload is canceled by user.	
Info	Scanning, remediation, and staging are not supported on PXE booted ESXi hosts.	
Warning	Patch *patch_name* was excluded from the stage operation because its prerequisite *prerequisite_name* is neither installed on the host nor included in the baseline. Include the prerequisites in a Patch or Extension baseline and retry the stage operation. You can also add the baselines to a baseline group for convenience and perform the stage operation.	Include the prerequisites in a Patch or Extension baseline and retry the stage operation.
Warning	Patch *patch_name* was excluded from the remediation because its prerequisite *prerequisite_name* is neither installed on the host nor included in the baseline. Include the prerequisites in a Patch or Extension baseline and retry the remediation. You can also add the baselines to a baseline group for convenience and perform the remediation.	Include the prerequisites in a Patch or Extension baseline and retry the stage operation.
Error	Cannot scan the host *host_name* because its power state is *state*.	
Error	Cannot stage patches to the host *host_name* because its power state is *state*.	
Error	Cannot remediate the host *host_name* because its power state is *state*.	
Error	Could not scan host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.

Table 15-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not stage patches to host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.
Error	Could not remediate host *host_name* because its power state is invalid. The host is in standby mode and the individual VMware DPM settings of the host are set to Disabled or Manual.	Power on the host manually.

16 Patch Repository

Patch and extension metadata is kept in the Update Manager Patch Repository. You can use the repository to manage patches and extensions, check on new patches and extensions, view patch and extension details, view which baseline a patch or an extension is included in, view recalled patches, import patches, and so on.

If your vCenter Server system is part of a connected group in vCenter Linked Mode, and you have at least one Update Manager instance, you can select the Update Manager patch repository that you want to view.

The Patch Repository is displayed in the Update Manager Administration view.

This chapter includes the following topics:

View Available Patches and Extensions

The Patch Repository lets you view the available patches and extensions, and also lets you include available patches and extensions in a baseline that you select.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- Click the **Patch Repository** tab to view all the available patches and extensions.

The most recent patches and extensions are displayed in bold. The recalled patches are marked with a flag icon.

Add and Remove Patches or Extensions from a Baseline

From the Patch Repository, you can include available as well as recently downloaded patches and extensions in a baseline of your choice.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and click **Update Manager** under Solutions and Applications on the Home page. If your vCenter Server system is part of a connected group in vCenter Linked Mode, you must specify the Update Manager instance to use, by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

1 Click the **Patch Repository** tab to view all the available patches and extensions.

2 Click the **Add to baseline** link in the Baselines column for a selected patch.

3 In the Edit containing baselines window, select the baselines in which you want to include this patch or extension and click **OK**.

If your vCenter Server system is 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 or Extensions in the Patch Repository

You can search for specific patches or extensions in the patch repository by using various criteria. An advanced search provides a way to filter the list of patches and extensions to display only those items that match the criteria that you specify.

Procedure

1 To locate a patch or an extension based on a keyword or phrase, enter text in the text box in the upper-right corner of the Update Manager **Patch Repository** tab.

2 To search for patches or extensions using more specific criteria, click **Advanced** next to the text field.

3 In the Filter Patches window, enter the search criteria.

Option	Description
Patch Vendor	Specifies which patch or extension vendor to use.
Product	Restricts the set of patches or extensions 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 or extensions to include.
Released Date	Specifies the range for the release dates of the patches or extensions.
Text	Restricts the patches or extensions to those containing the text that you enter.

4 Click **Find**.

The contents of the Patch Repository are filtered according to the criteria you entered.

Common User Goals 17

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 goals provide task flows that you can perform with Update Manager to upgrade and patch your vSphere inventory objects and make them compliant against attached baselines and baseline groups.

- Applying Patches to Hosts on page 140

  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.

- Applying Third-Party Patches to Hosts on page 141

  You can use Update Manager to apply third-party software patches to the ESX/ESXi hosts in your vSphere inventory.

- Testing Patches or Extensions and Exporting Baselines to Another Update Manager Server on page 143

  Before you apply patches or extensions to ESX/ESXi hosts, you might want to test the patches and extensions by applying them to hosts in a test environment. You can then use Update Manager PowerCLI to export the tested baselines to another Update Manager server instance and apply the patches and extensions to the other hosts.

- Applying Extensions to Hosts on page 146

  With Update Manager you can apply extensions to ESX/ESXi hosts. An extension is any additional software that can be installed on the host or patched if the additional software already exists on the host.

- Orchestrated Datacenter Upgrades on page 147

  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.

- Upgrading and Applying Patches to Hosts Using Baseline Groups on page 150

  You can use baseline groups to apply upgrade and patch baselines together for upgrading and updating hosts in a single remediation operation.

- Applying Patches to Virtual Machines on page 152

  You can use Update Manager 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.

- Upgrading Virtual Appliances on page 153

  An upgrade remediation of a virtual appliance upgrades the entire software stack in the virtual appliance, including the operating system and applications. To upgrade the virtual appliance to the latest released or latest critical version, you can use one of the Update Manager predefined upgrade baselines or create your own.

- Keeping the vSphere Inventory Up to Date on page 154

  You can use Update Manager to keep your vSphere inventory updated with the most recent patches.

- Associating the UMDS Patchstore Depot with the Update Manager Server on page 155

  UMDS is an optional module of Update Manager. UMDS downloads patch metadata and patch binaries when Update Manager is installed in an air-gap or semi-air-gap deployment system and has no access to the Internet. The patch metadata and patch binaries that you download using UMDS must be associated with the Update Manager server so that Update Manager can patch the hosts and virtual machines in your vSphere environment.

- Generating Common Database Reports on page 159

  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.

Applying Patches to Hosts

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.

You must configure Update Manager network connectivity settings, patch download sources and schedule, as well as proxy settings, so that Update Manager downloads the host patches, patch metadata, and patch binaries. For more information, see Chapter 11, "Configuring Update Manager," on page 67.

During host patch operations (scanning, staging, and remediation), you can check Update Manager events for information about the status of the operations. You can also see which host patches are available in the Update Manager repository.

Some patches might require that the host enters maintenance mode during remediation. If you want to apply patches at a cluster level, you should configure the cluster settings as well. Configure Update Manager to temporarily disable VMware DPM, HA admission control, and FT, and to temporarily disconnect any removable media devices connected to the virtual machines on a host.

This workflow describes the process to apply patches to the hosts in your vSphere inventory. You can apply patches to hosts at a folder, cluster or datacenter level. You can also apply patches to a single host. This workflow describes the process to apply patches to multiple hosts in a container object.

1 Configure the Update Manager host and cluster settings.

  You can configure the Update Manager settings from the **Configuration** tab of the Update Manager Administration view. For more information and the detailed procedure about configuring host and cluster settings by using Update Manager, see "Configuring Host and Cluster Settings," on page 77.

2 Create fixed or dynamic host patch baselines.

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

  You can create patch baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating fixed patch baselines, see "Create a Fixed Patch Baseline," on page 84. For detailed instructions about creating a dynamic patch baseline, see "Create a Dynamic Patch Baseline," on page 85.

3 Attach the patch baselines to a container object containing the hosts that you want to scan or remediate.

The container object can be a folder, cluster, or datacenter. You can attach baselines and baseline groups to objects from the Update Manager Compliance view. For more information about attaching baselines and baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

4 Scan the container object.

After you attach baselines 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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

5 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

6 (Optional) Stage the patches in the attached baselines to the hosts that you want to update.

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 host downtime during remediation. For a detailed procedure about staging patches and extensions to hosts, see "Stage Patches and Extensions to ESX/ESXi Hosts," on page 116.

7 Remediate the container object.

Remediate the hosts that are in Non-Compliant state to make them compliant with the attached baselines. For more information about remediating hosts against patch or extension baselines, see "Remediate Hosts Against Patch or Extension Baselines," on page 117.

During patch staging and remediation, Update Manager performs prescan and postscan operations. After remediation is completed, the compliance state of the hosts against the attached baseline is updated to Compliant.

Applying Third-Party Patches to Hosts

You can use Update Manager to apply third-party software patches to the ESX/ESXi hosts in your vSphere inventory.

This workflow describes the overall process to apply third-party patches to the hosts in your vSphere inventory. You can apply patches to hosts at the folder, cluster or datacenter level. You can also apply patches to a single host. This workflow describes the process to apply patches to multiple hosts in a container object.

1 Make the third-party software patches available to the Update Manager server.

- Download the third-party patches from the Internet to make them available to the Update Manager server.

  If the machine on which the Update Manager server is installed has access to the Internet, you must either configure Update Manager to download patch binaries and patch metadata from third-party Web sites, or you must manually download the third-party patches and import them into the Update Manager patch repository as an offline bundle.

By default, Update Manager contacts VMware at regular configurable intervals to gather information about the latest available patches. You can add third-party URLs to download third-party patches that are applicable to the ESX/ESXi 4.0.x and ESX/ESXi 4.1 hosts in your inventory. You can configure the Update Manager download source from the **Configuration** tab of the Update Manager Administration view. For a detailed procedure about configuring Update Manager to use third-party download URL addresses as patch download sources, see "Add a Third-Party Download URL Source for ESX/ESXi Hosts," on page 71.

You can import offline bundles in the Update Manager repository from the **Configuration** tab of the Update Manager Administration view. For a detailed procedure about importing offline bundles, see "Import Patches Manually," on page 73.

- Use UMDS to download third-party patches and make the patches available to the Update Manager server.

  If the machine on which the Update Manager server is installed is not connected to the Internet, you can use UMDS to download the third-party patches. For more information about configuring UMDS to download third-party patches, see "Configure UMDS to Download Third-Party Patches for ESX/ESXi Hosts," on page 64.

  The patch metadata and patch binaries that you download using UMDS must be associated with the Update Manager server so that Update Manager can patch the hosts in your vSphere environment. For more information about associating the UMDS depot with the Update Manager server, see "Associating the UMDS Patchstore Depot with the Update Manager Server," on page 155.

2 Configure the Update Manager host and cluster settings.

  You can configure the Update Manager settings from the **Configuration** tab of the Update Manager Administration view. For more information and the detailed procedure about configuring host and cluster settings by using Update Manager, see "Configuring Host and Cluster Settings," on page 77.

3 Create fixed or dynamic patch baselines containing the third-party software patches that you downloaded to the Update Manager repository.

  You can create patch baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating fixed patch baselines, see "Create a Fixed Patch Baseline," on page 84. For detailed instructions about creating a dynamic patch baseline, see "Create a Dynamic Patch Baseline," on page 85.

4 Attach the patch baselines to a container object containing the hosts that you want to scan or remediate.

  The container object can be a folder, cluster, or datacenter. You can attach baselines and baseline groups to objects from the Update Manager Compliance view. For more information about attaching baselines and baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

5 Scan the container object.

  After you attach baselines 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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

  You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

6 Review the scan results displayed in the Update Manager Client Compliance view.

  For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

7 Remediate the container object.

Remediate the hosts that are in Non-Compliant state to make them compliant with the attached baselines. For more information about remediating hosts against patch or extension baselines, see "Remediate Hosts Against Patch or Extension Baselines," on page 117.

After remediation is completed, the compliance state of the hosts against the attached baseline is updated to Compliant.

Testing Patches or Extensions and Exporting Baselines to Another Update Manager Server

Before you apply patches or extensions to ESX/ESXi hosts, you might want to test the patches and extensions by applying them to hosts in a test environment. You can then use Update Manager PowerCLI to export the tested baselines to another Update Manager server instance and apply the patches and extensions to the other hosts.

Update Manager PowerCLI is a command-line and scripting tool built on Windows PowerShell, and provides a set of cmdlets for managing and automating Update Manager. For more information about installing and using Update Manager PowerCLI, see *vCenter Update Manager PowerCLI Installation and Administration Guide*.

This workflow describes how to test patches by using one Update Manager instance and how to export the patch baseline containing the tested patches to another Update Manager instance.

1 Create fixed host patch baselines.

   Create fixed patch baselines containing the patches that you want to test. Fixed patch baselines do not change their content when new patches are downloaded into the Update Manager patch repository. You can create a fixed patch baseline from the **Baselines and Groups** tab of the Update Manager Administration view. For more information and a detailed procedure, see "Create a Fixed Patch Baseline," on page 84.

2 Attach the patch baselines to a container object containing the hosts that you want to scan or remediate.

   The container object can be a folder, cluster, or datacenter. You can attach baselines and baseline groups to objects from the Update Manager Compliance view. For more information about attaching baselines and baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

3 Scan the container object.

   After you attach baselines 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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

   You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

4 Review the scan results displayed in the Update Manager Client Compliance view.

   For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

5 (Optional) Stage the patches in the attached baselines to the hosts that you want to update.

   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 host downtime during remediation. For a detailed procedure about staging patches and extensions to hosts, see "Stage Patches and Extensions to ESX/ESXi Hosts," on page 116.

6 Remediate the container object.

Remediate the hosts that are in Non-Compliant state to make them compliant with the attached baselines. For more information about remediating hosts against patch or extension baselines, see "Remediate Hosts Against Patch or Extension Baselines," on page 117.

7 Export the patch baselines from the Update Manager server that you used to test the patches, and import them to another Update Manager server.

You can export and import patch baselines from one Update Manager server to another by using an Update Manager PowerCLI script. The following example script creates a duplicate of the baseline *MyBaseline* on the *$destinationServer*.

NOTE The script works for fixed and dynamic patch baselines as well as for extension baselines.

```
# $destinationServer = Connect-VIServer <ip_address_of_the_destination_server>
# $sourceServer = Connect-VIServer <ip_address_of_the_source_server>
# $baselines = Get-PatchBaseline MyBaseline -Server $sourceServer
# ExportImportBaselines.ps1 $baselines $destinationServer
Param([VMware.VumAutomation.Types.Baseline[]] $baselines,
[VMware.VimAutomation.Types.VIServer[]]$destinationServers)

$ConfirmPreference = 'None'
$includePatches = @()
$excludePatches = @()

function ExtractPatchesFromServer([VMware.VumAutomation.Types.Patch[]]$patches,
[VMware.VimAutomation.Types.VIServer]$destinationServer){
    $result = @()
    if ($patches -ne $null){
        foreach($patch in $patches){
            $extractedPatches = Get-Patch -Server $destinationServer -SearchPhrase
$patch.Name
   if ($extractedPatches -eq $null){
    Write-Warning -Message "Patch '$($patch.Name)' is not available on the server
$destinationServer"
   } else {
    $isFound = $false
    foreach ($newPatch in $extractedPatches){
     if ($newPatch.IdByVendor -eq $patch.IdByVendor){
      $result += $newPatch
      $isFound = $true
              }
          }
    if ($isFound -eq $false) {
     Write-Warning -Message "Patch '$($patch.Name)' with VendorId '$($patch.IdByVendor)' is
not available on the server $destinationServer"
    }
   }
  }
 }
 return .$result;
}

function
CreateStaticBaseline([VMware.VumAutomation.Types.Baseline]$baseline,
[VMware.VimAutomation.Types.VIServer]$destinationServer){
 $includePatches = ExtractPatchesFromServer $baseline.CurrentPatches $destinationServer
```

```
 if ($includePatches.Count -lt 1){
  write-error "Static baseline '$($baseline.Name)' can't be imported. No one of the patches
it contains are available on the server $destinationServer"
 } else {
  $command = 'New-PatchBaseline -Server $destinationServer -Name $baseline.Name -Description
$baseline.Description -Static -TargetType $baseline.TargetType -IncludePatch $includePatches'
  if ($baseline.IsExtension) {
   $command += ' -Extension'
  }

  Invoke-Expression $command
 }
}

function
CreateDynamicBaseline([VMware.VumAutomation.Types.Baseline]$baseline,
[VMware.VimAutomation.Types.VIServer]$destinationServer)
{
 if ($baseline.BaselineContentType -eq 'Dynamic'){
  $command = 'New-PatchBaseline -Server $destinationServer -Name $baseline.Name -Description
$baseline.Description -TargetType $baseline.TargetType -Dynamic -SearchPatchStartDate
$baseline.SearchPatchStartDate - SearchPatchEndDate $baseline.SearchPatchEndDate -
SearchPatchProduct $baseline.SearchPatchProduct -SearchPatchSeverity
$baseline.SearchPatchSeverity -SearchPatchVendor $baseline.SearchPatchVendor'
 } elseif ($baseline.BaselineContentType -eq 'Both'){
        $includePatches = ExtractPatchesFromServer $baseline.InclPatches $destinationServer
     $excludePatches = ExtractPatchesFromServer $baseline.ExclPatches $destinationServer

  $command = 'New-PatchBaseline -Server $destinationServer -Name $baseline.Name -Description
$baseline.Description -TargetType $baseline.TargetType -Dynamic -SearchPatchStartDate
$baseline.SearchPatchStartDate -SearchPatchEndDate $baseline.SearchPatchEndDate -
SearchPatchProduct $baseline.SearchPatchProduct -SearchPatchSeverity
$baseline.SearchPatchSeverity -SearchPatchVendor $baseline.SearchPatchVendor'
  if ($includePatches.Count -gt 0){
   $command += ' -IncludePatch $includePatches'
  }

  if ($excludePatches.Count -gt 0){
  $command += ' -ExcludePatch $excludePatches'
  }
 }

 #check for null because there is known issue for creating baseline with null
SearchPatchPhrase
 if ($baseline.SearchPatchPhrase -ne $null){
  $command += ' -SearchPatchPhrase $baseline.SearchPatchPhrase'
 }

 Invoke-Expression $command
}

foreach ($destinationServer in $destinationServers) {
 if ($baselines -eq $null) {
  Write-Error "The baselines parameter is null"
 } else {
```

```
  foreach($baseline in $baselines){
   if ($baseline.GetType().FullName –eq 'VMware.VumAutomation.Types.PatchBaselineImpl'){
    Write–Host "Import '" $baseline.Name "' to the server $destinationServer"
    if($baseline.BaselineContentType –eq 'Static'){
     CreateStaticBaseline $baseline $destinationServer
    } else {
     CreateDynamicBaseline $baseline $destinationServer
    }
   } else {
    Write–Warning –Message "Baseline '$($baseline.Name)' is not patch baseline and will be
skipped."
   }
  }
 }
}
```

You have now exported the tested baseline to another Update Manager server.

8 Apply the patches to your ESX/ESXi hosts by using the Update Manager server instance to which you exported the tested patch baseline.

Applying Extensions to Hosts

With Update Manager you can apply extensions to ESX/ESXi hosts. An extension is any additional software that can be installed on the host or patched if the additional software already exists on the host.

To perform the initial installation of an extension, you must use an extension baseline. After the extension is installed on the host, you can update the extension module with either patch or extension baselines.

When applying extension baselines by using Update Manager, you must be aware of the functional implications of new modules to the host. Extension modules might alter the behavior of ESX/ESXi hosts. During installation of extensions, Update Manager only performs the checks and verifications expressed at the package level.

Some extensions might require that the host enters maintenance mode during remediation. To apply extensions at a cluster level, you should configure the cluster settings as well. Configure Update Manager to temporarily disable VMware DPM, HA admission control, FT, and to temporarily disconnect any removable media devices connected to the virtual machines on a host.

This workflow describes the overall process to apply extensions to the hosts in your vSphere inventory. You can apply extensions to hosts at a folder, cluster or datacenter level. You can also apply extensions to a single host. This workflow describes the proccess to apply extensions to multiple hosts in a container object.

1 Configure the Update Manager host and cluster settings.

  You can configure the Update Manager settings from the **Configuration** tab of the Update Manager Administration view. For more information and the detailed procedure about configuring host and cluster settings by using Update Manager, see “Configuring Host and Cluster Settings,” on page 77.

2 (Optional) Import an offline bundle to download extensions to the Update Manager server.

  Offline bundles might contain extensions that you download from the Internet or copy from a media drive. Offline bundles are ZIP files that can be located on a local or a shared network drive. You can import offline bundles from the **Configuration** tab of the Update Manager Administration view. For more information about importing offline bundles and for a detailed procedure on importing offline bundles, see “Import Patches Manually,” on page 73.

3 Create extension baselines.

You can create host extension baselines from the **Baselines and Groups** tab in the Update Manager Administration view. For a detailed procedure about creating extension baselines, see "Create a Host Extension Baseline," on page 86.

4 Attach the extension baselines to a container object containing the hosts that you want to remediate.

To scan and remediate hosts, attach the extensions baselines to a container object containing the hosts to which you want to apply the extensions. The container object can be a folder, cluster, or datacenter. You can attach baselines and baseline groups to objects from the Update Manager Compliance view. For more information about attaching baselines and baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

5 Scan the container object.

After you attach baselines 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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

6 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

7 (Optional) Stage the extensions from the attached baselines to the ESX/ESXi hosts.

You can stage the extensions and copy them from the Update Manager server to selected hosts before applying them. Staging extensions speeds up the remediation process and helps minimize host downtime during remediation. For a detailed procedure about staging patches and extensions to hosts, see "Stage Patches and Extensions to ESX/ESXi Hosts," on page 116.

8 Remediate the hosts in the container object against extension baselines.

You can remediate the container object of the hosts against the attached baselines. If hosts are in a Non-Compliant state, remediate the container object to make the hosts compliant with the attached baselines. You can start the remediation process manually or schedule a remediation task. See "Remediate Hosts Against Patch or Extension Baselines," on page 117 for a detailed procedure.

During staging extensions and extension remediation, Update Manager performs prescan and postscan operations. After remediation is completed, the compliance state of the hosts against the attached baselines is updated to Compliant.

Orchestrated Datacenter Upgrades

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 without powering the virtual machine off as long as VMware Distributed Resource Scheduler (DRS) is available for the cluster. To perform an orchestrated upgrade, you must first remediate a cluster against a host upgrade baseline, and then remediate the same cluster against a virtual machine upgrade baseline group containing the VM Hardware Upgrade to Match Host and VMware Tools Upgrade to Match Host baselines.

- Orchestrated Upgrade of Hosts on page 148

  You can use Update Manager to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory by using a single upgrade baseline.

- Orchestrated Upgrade of Virtual Machines on page 149

  An orchestrated upgrade allows you to upgrade VMware Tools and the virtual hardware for 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

You can use Update Manager to perform orchestrated upgrades of the ESX/ESXi hosts in your vSphere inventory by using a single upgrade baseline.

This workflow describes the overall process to perform an orchestrated upgrade of the hosts in your vSphere inventory. Update Manager supports host upgrades for hosts from ESX 3.0.0 and later as well as ESX 3i version 3.5 and later to ESX/ESXi versions 4.0.x and 4.1. You cannot upgrade ESX/ESXi 4.0 hosts to ESX/ESXi 4.0.x, because this operation is a patching process. The remediation for hosts from versions 4.0.x to version 4.1 is considered an upgrade.

NOTE You cannot upgrade ESX 3.0.x hosts directly to ESX 4.1. To upgrade ESX hosts of version 3.0.x to version 4.1 you must first upgrade them to version 4.0 or 4.0.x and then upgrade to 4.1.

Before you perform the upgrade, ensure that you configure Update Manager to temporarily disable VMware DPM, HA admission control, and FT. Update Manager does not remediate hosts in a cluster on which these features are enabled.

Ensure that you temporarily disconnect any removable devices connected to the virtual machines on a host.

You can perform orchestrated upgrades of hosts at the folder, cluster, or datacenter level.

1 Configure the Update Manager host and cluster settings.

  You can configure the Update Manager settings from the **Configuration** tab of the Update Manager Administration view. For more information and the detailed procedures about configuring host and cluster settings by using Update Manager, see "Configuring Host and Cluster Settings," on page 77.

2 Import a complete upgrade release bundle.

  Import a complete upgrade release bundle so that can upgrade all the hosts in your vSphere inventory. You can import upgrade release bundles from the **Host Upgrade Releases** tab of the Update Manager Administration view.

  For example, to upgrade all the ESX/ESXi hosts in your vSphere environment to version 4.1, you must upload all of the files required for this upgrade (three ZIP files and one ISO file):

  - `esx-DVD-4.1.0-`*`build_number`*`.iso` for ESX 3.x hosts
  - `upgrade-from-ESXi3.5-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 3.x hosts
  - `upgrade-from-ESX4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESX 4.0.x hosts
  - `upgrade-from-ESXi4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 4.0.x hosts

  Here *build_number* is the build number of the upgrade release.

  For the complete procedure about importing host upgrade releases, see "Import Host Upgrade Releases," on page 89.

3 Create a host upgrade baseline with the upgrade release bundle that you imported.

  You create host upgrade baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For a detailed procedure about creating host upgrade baselines, see "Create a Host Upgrade Baseline," on page 90.

4 Attach the host upgrade baseline to a container object containing the hosts that you want to upgrade.

You can attach baselines and baseline groups to objects from the Update Manager Compliance view. For more information about attaching baselines and baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

5 Scan the container object.

After you attach baselines 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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

6 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

7 Remediate the container object.

If hosts are in Non-Compliant 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. For more information about remediating hosts against an upgrade baseline and for a detailed procedure, see "Remediate Hosts Against an Upgrade Baseline," on page 119.

Hosts that are upgraded reboot and disconnect for some time during the remediation.

Orchestrated Upgrade of Virtual Machines

An orchestrated upgrade allows you to upgrade VMware Tools and the virtual hardware for 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 workflow describes the overall process to perform an orchestrated upgrade of the virtual machines in your vSphere inventory.

1 Create a virtual machine baseline group.

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. You can create baseline groups from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating baseline groups and for detailed instructions, see "Create a Virtual Machine and Virtual Appliance Baseline Group," on page 96.

2 Attach the baseline group to an object containing the virtual machines that you want to upgrade.

To scan and 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. For detailed instructions about attaching baselines and baseline groups to objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

3 Scan the container object.

You must scan it to view the compliance state of the virtual machines in the container. You can scan selected objects manually to start the scanning immediately. For detailed instructions on how to scan your virtual machines manually, see "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 102.

You can also scan the virtual machines in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

4 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

5 Remediate the non-compliant virtual machines in the container object to make them compliant with the attached baseline group.

If virtual machines are in a Non-Compliant 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. For more information about remediating virtual machines and for detailed instructions, see "Remediate Virtual Machines and Virtual Appliances," on page 125.

During an 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 is completed, Update Manager restarts the machine and restores the original power state of the virtual machine.

During a virtual machine hardware upgrade, the virtual machines must be shut down. After the remediation is completed, 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.

Upgrading and Applying Patches to Hosts Using Baseline Groups

You can use baseline groups to apply upgrade and patch baselines together for upgrading and updating hosts in a single remediation operation.

You can upgrade all ESX/ESXi hosts in your deployment system by using a single upgrade baseline. You can apply patches to the hosts at the same time by using a baseline group containing one upgrade baseline and multiple host patch baselines.

This workflow describes how to upgrade and patch the hosts in your vSphere inventory at the same time. You can upgrade hosts and apply patches to hosts at the folder, cluster or datacenter level. You can also upgrade and patch a single host. This workflow describes the process to patch and upgrade multiple hosts in a container object.

1 Configure the Update Manager host and cluster settings.

You can configure the Update Manager settings from the **Configuration** tab of the Update Manager Administration view. For more information and the detailed procedures about configuring host and cluster settings by using Update Manager, see "Configuring Host and Cluster Settings," on page 77.

2 Import a complete upgrade release bundle.

Import a complete upgrade release bundle, so that you can upgrade all the hosts in your vSphere inventory. You can import upgrade release bundles from the **Host Upgrade Releases** tab of the Update Manager Administration view.

For example, to upgrade all the ESX/ESXi hosts in your vSphere environment to version 4.1, you must upload all of the files required for this upgrade (three ZIP files and one ISO file):

- `esx-DVD-4.1.0-`*`build_number`*`.iso` for ESX 3.x hosts
- `upgrade-from-ESXi3.5-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 3.x hosts
- `upgrade-from-ESX4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESX 4.0.x hosts
- `upgrade-from-ESXi4.0-to-4.1.0-0.0.`*`build_number`*`-release.zip` for ESXi 4.0.x hosts

Here *build_number* is the build number of the upgrade release.

For a complete procedure about importing host upgrade releases, see "Import Host Upgrade Releases," on page 89.

3 Create a host upgrade baseline with the upgrade release bundle that you imported.

You create host upgrade baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For a detailed procedure about creating host upgrade baselines, see "Create a Host Upgrade Baseline," on page 90.

4 Create fixed or dynamic host patch baselines.

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.

You can create patch baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating fixed patch baselines see "Create a Fixed Patch Baseline," on page 84. The detailed instructions about creating a dynamic patch baseline are described in "Create a Dynamic Patch Baseline," on page 85.

5 Create a baseline group containing the patch baselines as well as the host upgrade baseline that you created.

You can create baseline groups from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating baseline groups for hosts, see "Create a Host Baseline Group," on page 95.

6 Attach the baseline group to a container object.

To scan and remediate the hosts in your environment, you must first attach the host baseline group to a container object containing the hosts that you want to remediate. You can attach baseline groups to objects from the Update Manager Compliance view. For more information about attaching baseline groups to vSphere objects, see "Attach Baselines and Baseline Groups to Objects," on page 98.

7 Scan the container object.

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 to start the scanning immediately. For detailed instructions on how to scan your hosts manually, see "Manually Initiate a Scan of ESX/ESXi Hosts," on page 101.

You can also scan the hosts in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

8 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

9 Remediate the container object.

Remediate the hosts that are in Non-Compliant state to make them compliant with the attached baseline group. For more information about remediating hosts against baseline groups containing patch, extension, and upgrade baselines, see "Remediate Hosts Against Baseline Groups," on page 121.

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 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.

Applying Patches to Virtual Machines

You can use Update Manager 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 workflow describes the overall process to apply patches to the virtual machines in your vSphere inventory. You can apply patches to virtual machines at a folder, cluster or datacenter level. You can also apply patches to a single virtual machine. This workflow describes the process to apply patches to multiple virtual machines in a container object.

1 Create fixed or dynamic patch baselines.

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.

You can create patch baselines from the **Baselines and Groups** tab of the Update Manager Administration view. For more information about creating fixed patch baselines, see "Create a Fixed Patch Baseline," on page 84. For detailed instructions about creating a dynamic patch baseline, see "Create a Dynamic Patch Baseline," on page 85.

2 (Optional) Create a baseline group.

You can combine multiple patch baselines in a baseline group. You can create patch baselines from the **Baselines and Groups** tab in the Update Manager Administration view. For more information about creating baseline groups, see "Create a Virtual Machine and Virtual Appliance Baseline Group," on page 96.

3 Attach the baselines or baseline groups to a container object containing the virtual machines that you want to remediate.

To remediate virtual machines, attach the patch baseline or baseline group to a virtual machine or a container object containing the virtual machines. The container object can be a folder or a datacenter. For a detailed description of the procedure, see "Attach Baselines and Baseline Groups to Objects," on page 98.

4 Scan the container object.

Before remediation, you should scan the virtual machine or container object for compliance with the attached baselines. You can start the scan operation either manually or as a scheduled task. For detailed descriptions of the procedures, see "Schedule a Scan," on page 102 and "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 102.

5 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

6 Remediate the container object.

If virtual machines are in a noncompliant state, remediate the container object to make them compliant with the attached baseline or baseline groups. You can start the remediation process manually or schedule a remediation task. For a detailed description of the procedure, see "Remediate Virtual Machines and Virtual Appliances," on page 125.

One or more patches might require the guest operating system to restart. If no users are logged in to the guest operating system, the virtual machine restarts immediately. Otherwise, a dialog box informs logged-in users of the upcoming shutdown.

The remediated virtual machines become compliant with the attached patch baselines or baseline groups.

Upgrading Virtual Appliances

An upgrade remediation of a virtual appliance upgrades the entire software stack in the virtual appliance, including the operating system and applications. To upgrade the virtual appliance to the latest released or latest critical version, you can use one of the Update Manager predefined upgrade baselines or create your own.

Virtual appliances must be powered on before scan and remediation operations. When you power on a virtual appliance for the first time, Update Manager discovers it as a virtual appliance. Because virtual appliances download the version information for the new virtual appliance or the new software package from the Internet, they must have Internet access.

Updates for a virtual appliance are downloaded by automatic updates, or during the remediation process. Update Manager controls only when and what to download. The download URL is set by the ISV providing the virtual appliance.

This workflow describes how to upgrade the virtual appliances in your vSphere inventory. You can upgrade virtual appliances at the folder, cluster or datacenter level. You can also upgrade a single virtual appliance. This workflow describes the process to upgrade multiple virtual appliances in a container object.

1 (Optional) Create a virtual appliance upgrade baseline.

You create virtual appliance baselines from the **Baselines and Groups** tab in the Update Manager Administration view. For a detailed description of the procedure, see "Create and Edit a Virtual Appliance Upgrade Baseline," on page 92.

2 Attach virtual appliance upgrade baselines to an object containing the virtual appliances that you want to upgrade.

To scan and upgrade virtual appliances, attach your virtual appliance upgrade baselines to a container object containing the virtual appliances that you want to upgrade. The container object can be a folder, vApp, or datacenter. For a detailed description of the procedure, see "Attach Baselines and Baseline Groups to Objects," on page 98.

3 Scan the container object.

After you attach the virtual appliance upgrade baselines 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 to start the scanning immediately. For detailed instructions on how to scan your virtual appliances manually, see "Manually Initiate a Scan of Virtual Machines and Virtual Appliances," on page 102.

You can also scan the virtual appliances in the container object at a time convenient for you by scheduling a scan task. For more information and detailed instructions about scheduling a scan, see "Schedule a Scan," on page 102.

4 Review the scan results displayed in the Update Manager Client Compliance view.

For a detailed procedure about viewing scan results and for more information about compliance states, see "Viewing Scan Results and Compliance States for vSphere Objects," on page 103.

5 Remediate the virtual appliances in the container object against the attached virtual appliance upgrade baselines.

If virtual appliances are in a Non-Compliant state, remediate the container object of the virtual appliances to make it compliant with the attached baselines. You can start the remediation process manually or schedule a remediation task. For a detailed description of the procedure, see "Remediate Virtual Machines and Virtual Appliances," on page 125.

Update Manager directs the virtual appliances to download the missing updates and controls the remediation process of when and how to remediate, but the virtual appliance downloads and installs the updates itself.

The remediated virtual appliances become compliant with the attached baselines.

Keeping the vSphere Inventory Up to Date

You can use Update Manager to keep your vSphere inventory updated with the most recent patches.

You can change the frequency of the checks for updates and patches, create dynamic patch baselines, attach the baselines to the objects in the inventory, and perform regular scans and scheduled remediation, to keep your vSphere inventory of hosts and virtual machines updated.

This workflow describes the overall process to keep the hosts and virtual machines in your vSphere inventory updated with the most recent patches.

1 Configure the patch download schedule.

Update Manager checks for patches at regular intervals. You can modify the schedule for checking and downloading patch data. For a detailed description of the procedure, see "Configure Checking for Patches," on page 74.

2 Create dynamic patch baselines.

The contents of dynamic patch baselines are updated when new patches that meet the criteria become available. For information about creating dynamic patch baselines, see "Create a Dynamic Patch Baseline," on page 85.

3 Attach the baselines to a container object.

To scan and remediate the objects in your vSphere inventory, attach the baselines to selected objects in the inventory. For a detailed description of the procedure, see "Attach Baselines and Baseline Groups to Objects," on page 98.

4 Schedule a scan.

You can schedule periodic scans of the hosts and virtual machines in your vSphere inventory. For a detailed description of the procedure, see "Schedule a Scan," on page 102.

5 Schedule remediation for hosts and virtual machines.

Schedule remediation tasks at times convenient for you for the hosts and virtual machines in your vSphere inventory. For more information about scheduling remediation, see "Scheduling Remediation for Hosts, Virtual Machines, and Virtual Appliances," on page 126.

Associating the UMDS Patchstore Depot with the Update Manager Server

UMDS is an optional module of Update Manager. UMDS downloads patch metadata and patch binaries when Update Manager is installed in an air-gap or semi-air-gap deployment system and has no access to the Internet. The patch metadata and patch binaries that you download using UMDS must be associated with the Update Manager server so that Update Manager can patch the hosts and virtual machines in your vSphere environment.

Before you associate the UMDS patchstore depot with the Update Manager server, set up UMDS and download patches. For more information about installing, setting up UMDS, and downloading patches, see Chapter 10, "Installing, Setting Up, and Using Update Manager Download Service," on page 59.

You can either use a portable media drive to transfer the downloads to the machine on which Update Manager is installed, or you can copy them to a Web server. You must then set up Update Manager to use a shared repository as a patch download source.

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:\`).

- Associate the UMDS Depot with the Update Manager Server Using a Portable Media Drive on page 155

  In an air-gap deployment system where the Update Manager server is installed on a computer with no access to the Internet or other networks, the patch metadata and patch binaries you download using UMDS must be transferred to the machine on which Update Manager is installed.

- Associate the UMDS Depot with Update Manager Server Using IIS on page 156

  In a semi-air-gap environment, you can set up Internet Information Services (IIS) on the machine on which UMDS is installed and configure Update Manager to use the downloaded patch binaries and patch metadata from the IIS Web server.

- Associate the UMDS Depot with Update Manager Server Using Apache on page 158

  In a semi-air-gap environment, you can set up an Apache Web server on the machine on which UMDS is installed and configure Update Manager to use the downloaded patch binaries and patch metadata from the Apache Web server.

Associate the UMDS Depot with the Update Manager Server Using a Portable Media Drive

In an air-gap deployment system where the Update Manager server is installed on a computer with no access to the Internet or other networks, the patch metadata and patch binaries you download using UMDS must be transferred to the machine on which Update Manager is installed.

Procedure

1. Connect a portable media drive to the computer on which you have installed UMDS and have downloaded the patch binaries and patch metadata.
2. Open a Command Prompt window and navigate to the folder in which UMDS is installed.
   - The default location in 32-bit Windows is `C:\Program Files\VMware\Infrastructure\Update Manager`
   - The default location in 64-bit Windows is `C:\Program Files (x86)\VMware\Infrastructure\Update Manager`

3 Export the downloaded patches to the portable media drive.

```
vmware-umds -E --export-store F:\
```

Here `F:\` is the path to the media drive, for example a USB flash drive.

4 Verify that all files are exported to the portable media drive, and then safely remove it and connect it to the machine on which the Update Manager server is installed.

5 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 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.

6 Click the **Configuration** tab in the Update Manager Administration view.

7 Under Settings, click **Patch Download Settings**.

8 Select the **Use a shared repository** radio button.

9 Enter the path to the portable media drive.

```
F:\
```

Here `F:\` is the path to the media drive, for example a USB flash drive.

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

Make sure that the validation is successful. If the validation fails, Update Manager reports the reason for the failure. You can use the path to the shared repository only if the validation succeeds.

11 Click **Apply** to apply the changes.

12 Click **Download Now** to download the patch metadata immediately.

Update Manager downloads patch binaries during staging and remediation.

The patch binaries and patch metadata downloaded using the UMDS are imported to the machine on which the Update Manager server is installed.

Associate the UMDS Depot with Update Manager Server Using IIS

In a semi-air-gap environment, you can set up Internet Information Services (IIS) on the machine on which UMDS is installed and configure Update Manager to use the downloaded patch binaries and patch metadata from the IIS Web server.

Use this approach when the Update Manager server is installed on a machine that is connected to the UMDS machine, but does not have direct Internet access.

NOTE The procedure uses IIS 6. Other versions of IIS can be configured similarly.

Prerequisites

Install and set up IIS on the machine on which UMDS is running. For information about setting up an IIS Web server, see the *Internet Information Services* documentation on the Microsoft Web site.

Procedure

1 Log in to the computer on which you have installed UMDS and download the patch binaries and patch metadata.

2 Create a directory for the patch data under the document root of the Web server.

For example, `C:\inetpub\wwwroot\UMDS`.

3 Export the downloaded metadata and binaries to the `UMDS` directory under the Web server root.

```
vmware-umds -E --export-store C:\inetpub\wwwroot\UMDS
```

4 Add `.vib`, `.sig`, and `.xml` as allowed MIME types for the Web server.

   a Click **Start > Programs > Administrative Tools > Internet Information Services (IIS) Manager**.

   b In the Internet Information Services (IIS) Manager window, select **IIS Manager Information > *Computer Name*(local computer) > Web Sites > Default Web Site**.

   Here *Computer Name* is the name of your machine.

   c Right click the `UMDS` folder where you exported the patch data and select **Properties**.

   d Click **HTTP Headers > MIME Types**.

   e Click **New** and add the new MIME types.

   In the **Extension** text field, enter `.vib`, `.sig`, and `.xml`. Enter one file extension for each MIME type entry. In the **MIME Type** field, enter **`application/octet-stream`** for `.vib` and `.sig`. For `.xml`, enter **`text/xml`** in the **MIME Type** field.

5 Set appropriate permissions for the `UMDS` folder in the Web server root.

   a Right-click the `UMDS` folder under **Default Web Site** in the Internet Information Services (IIS) Manager window, and select **Permissions**.

   b In the Advanced Security Settings dialog box, select the **Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here** and **Replace permission entries on all child objects with entries shown here that apply to child objects** check boxes.

   c Click **Apply**.

6 Restart the IIS Admin Service in the Services Control Manager.

7 (Optional) Verify that you can view the `UMDS` directory under the Web server root in a browser and download files.

8 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 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.

9 Click the **Configuration** tab in the Update Manager Administration view.

10 Select the **Use a shared repository** radio button.

11 Enter the URL of the folder on the Web server where you exported the patch binaries and patch metadata.

   For example, `http://`*`ip_address_or_hostname`*`/UMDS`

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

   Make sure that the validation is successful. If the validation fails, Update Manager reports the reason for the failure. You can use the path to the shared repository only if the validation succeeds.

13 Click **Apply** to apply the changes.

14 Click **Download Now** to download the patch metadata immediately.

   Update Manager downloads patch binaries during staging and remediation.

Update Manager is now configured to use the patch metadata and patch binaries downloaded through UMDS and hosted on the IIS Web server.

Associate the UMDS Depot with Update Manager Server Using Apache

In a semi-air-gap environment, you can set up an Apache Web server on the machine on which UMDS is installed and configure Update Manager to use the downloaded patch binaries and patch metadata from the Apache Web server.

Use this approach when the Update Manager server is installed on a machine that is connected to the UMDS machine, but does not have direct Internet access.

NOTE The procedure uses Apache 2.2.14. Other versions of Apache can be configured similarly.

Prerequisites

Set up Apache on the machine on which UMDS is running. For information about setting up an Apache Web server, see the documentation on the *Apache HTTP Server Project* Web site.

Procedure

1 Log in to the computer on which you have installed UMDS and download the patch binaries and patch metadata.

2 Create a directory for the patch data under the document root of the Web server.

For example, `C:\Program Files\Apache Software Foundation\Apache2.2\htdocs\UMDS`.

3 Export the downloaded patch metadata and patch binaries to the `UMDS` directory in the Web server root.

```
vmware-umds -E --export-store C:\Program Files\Apache Software
Foundation\Apache2.2\htdocs\UMDS
```

4 (Optional) Verify that you can view the `UMDS` directory under the Web server root in a browser and download files.

5 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 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.

6 Click the **Configuration** tab in the Update Manager Administration view.

7 Select the **Use a shared repository** radio button.

8 Enter the URL of the folder on the Web server where you exported the patch binaries and patch metadata.

For example, `http://`*`ip_address_or_hostname`*`/UMDS`

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

Make sure that the validation is successful. If the validation fails, Update Manager reports the reason for the failure. You can use the path to the shared repository only if the validation succeeds.

10 Click **Apply** to apply the changes.

11 Click **Download Now** to download the patch metadata immediately.

Update Manager downloads patch binaries during staging and remediation.

Update Manager is now configured to use the patch metadata and patch binaries downloaded through UMDS and hosted on the Apache Web server.

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, but 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, you can retrieve the ID of the objects that you want to access. 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 on page 159

  Using Microsoft Excel, you can connect to the Update Manager database and query the database views to generate a common report.

- Generate Common Reports Using Microsoft SQL Server Query on page 160

  Using a Microsoft SQL Server query, you can generate a common report from the Update Manager database.

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 can 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 the following 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 column to join the columns in the tables 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 are applicable to the scanned objects in the inventory.

18 Troubleshooting

If you encounter problems when running or 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 in a Single vCenter Server System

Because of loss of network connectivity or the restart of the servers, the connection between the Update Manager plug-in and the Update Manager server or vCenter Server system might get interrupted.

Problem

The connection between the Update Manager plug-in and the Update Manager server or vCenter Server system is interrupted, when the servers are restarting or are stopped. In such a case various symptoms are observed.

- Update Manager plug-in displays a reconnection dialog, and after 15-20 seconds, a failure message appears. The plug-in is disabled.
- Update Manager plug-in displays a reconnection dialog. Within 15-20 seconds, the dialog disappears, and the plug-in can be used.
- vSphere Client displays a reconnection dialog. After an interval, it displays the login form. To use Update Manager, you must re-enable the Update Manager plug-in.

Cause

- The Update Manager server stops and is not available for more than 15-20 seconds.
- The Update Manager server restarts, and the service becomes available within 15-20 seconds.
- vCenter Server stops.

Solution

- If the Update Manager server has stopped, start the Update Manager service and re-enable the Update Manager Client plug-in.
- If the Update Manager server has restarted, wait for it to become available.
- If the vCenter Server service has stopped, start the vCenter Server service and enable the Update Manager plug-in.

Connection Loss with Update Manager Server or vCenter Server in a Connected Group in vCenter Linked Mode

Because of loss of network connectivity or a server restart, the connection between the Update Manager plug-in and the Update Manager server or vCenter Server system might get interrupted.

Problem

The connection between the Update Manager plug-in and the Update Manager server or vCenter Server system is interrupted, when the servers are restarting or are stopped. In such a case various symptoms are observed.

- Update Manager 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.
- Update Manager plug-in displays a modal reconnection dialog. Within 15-20 seconds, the dialog disappears, and the plug-in can be used.
- 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.
- 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.

Cause

- The Update Manager server in use stops and is not available for more than 15-20 seconds.
- The Update Manager server in use restarts, and the service becomes available within 15-20 seconds.
- An Update Manager server that is not currently in use stops.
- vCenter Server stops.

Solution

- If the Update Manager server has stopped, start the Update Manager service.

  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.
- If the Update Manager server has restarted, wait for the Update Manager service to become available.
- If the Update Manager server has stopped, start the Update Manager service.
- If the vCenter Server service has stopped, start the vCenter Server service.

Gather Update Manager Log Bundles

You can gather information about recent events on the Update Manager server for diagnostic purposes. When Update Manager and vCenter Server are installed on the same machine, you can also gather the vCenter Server log bundle together with the Update Manager log bundle.

Procedure

1 Log in to the machine on which Update Manager is installed.

   To obtain the complete set of the logs, you should log in with the user name and password used for installing 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 Bundles

When the 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 as an administrator 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 Bundle Is Not Generated

Because of limitations in the ZIP utility used by Update Manager, the cumulative log bundle size cannot exceed 2GB, although the script seems to complete successfully.

Problem

Update Manager does not generate log bundle after the script is run.

Solution

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 (x86)\VMware\Infrastructure\Update Manager`.

3 To run the script and exclude the vCenter Server logs enter the following command:

```
cscript vum-support.wsf /n
```

The **/n** option lets the script skip the vCenter Server support bundle and collect only the Update Manager log bundle.

4 Press Enter.

The Update Manager log bundle is generated as a ZIP package successfully.

Host Extension Remediation or Staging Fails Due to Missing Prerequisites

Some host extension remediation or staging operations fail because Update Manager does not automatically download and install missing prerequisites.

Problem

Host extension remediation or staging might fail.

Cause

Update Manager skips the extensions with missing prerequisites and lists the missing prerequisites as events when it detects them during the staging and remediation operations. To proceed with staging and remediation, you must install the prerequisites.

Solution

1 To see which prerequisites are missing, in Compliance View select **Tasks & Events > Events**.

2 Add the missing prerequisites manually to either an extension or a patch baseline, depending on the type of the missing prerequisites.

3 (Optional) Create a baseline group that contains the new baseline as well as the original baseline.

4 Remediate the host against the two baselines.

No Baseline Updates Available

Baselines are based on metadata that Update Manager downloads from the Shavlik and VMware Web sites. Shavlik provides metadata for virtual machines and applications, while VMware provides metadata for ESX/ESXi hosts.

Problem

Updates for virtual machines and ESX/ESXi hosts might be unavailable.

Cause

- Misconfigured Web server proxy.
- Shavlik servers are unavailable.
- VMware update service is unavailable.
- Poor network connectivity.

Solution

- Check the connectivity settings. For more information, see "Configure Update Manager Network Connectivity Settings," on page 69.
- Check the Shavlik Web site (http://www.shavlik.com) to determine whether it is available.
- Check the VMware Web site (http://www.vmware.com) to determine whether it is available.
- 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 Displayed as Not Applicable

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.

Problem

A scan might result in all baselines being marked as Not Applicable.

Cause

This condition typically indicates an error in scanning.

Solution

1 Examine the server logs for scan tasks that are marked as failed.

2 Retry the scan operation.

All Updates in Compliance Reports Are Unknown

Scanning is the process in which you generate compliance information about vSphere objects against attached baselines and baseline groups. The compliance statuses of objects can be All Applicable, Non Compliant, Incompatible, Unknown, and Compliant.

Problem

All results of a scan might be listed as Unknown.

Cause

Such a condition typically indicates an error at the start of the scanning process. This might also indicate that no scan occurred.

Solution

Schedule a scan or manually start 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.

Problem

After remediation, the remediated virtual machines continue to be in the Not Compliant state.

Cause

- Insufficient disk space for Service Pack installation.
- Conflicts with running applications.

Solution

- Retry remediation after freeing up disk space.
- Reboot the virtual machine and then retry the remediation operation.

Patch Remediation of Virtual Machines Is Not Completed

In some instances, remediating virtual machines with the default patch baselines fails.

Problem

Virtual machine remediation with the default Critical VM Patches and Non-Critical VM Patches baselines might fail.

Cause

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.

Solution

1 End the patch process from the Task Manager in the guest.

2 To identify the patch that resulted in 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.

Patch Remediation of Virtual Machines Fails for Some Patches

In some cases, remediation of virtual machines with the default Critical VM Patches and Non-Critical VM Patches baselines fails.

Problem

Remediation of virtual machines fails for some patches.

Cause

Remediation might fail for some patches, if the 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.

Solution

Review the **Events** tab of the Update Manager plug-in to determine if patches were not downloaded.

Patch Remediation of Virtual Machines Succeeds but the Baseline Is Not Compliant

In some cases, remediation of virtual machines with the default Critical VM Patches and Non-Critical VM Patches baselines succeeds but the baseline is still marked Not Compliant.

Problem

Remediation is completed but the baseline is still noncompliant.

Cause

The baseline might be still noncompliant when you apply 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.

Solution

Repeat the remediation process.

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 a host of versions ESX/ESXi 4.0.x or ESX/ESXi 4.1.

Problem

You cannot upgrade VMware Tools because a virtual machine in incompatible compliance state cannot be remediated.

Cause

If no VMware Tools installation is detected on a virtual machine, a scan of the virtual machine against the VMware Tools Upgrade to Match Host baseline or a baseline group containing this baseline results in an incompatible compliance state of the virtual machine.

Solution

Install VMware Tools manually, or right-click the virtual machine in the vSphere Client Inventory and select **Guest > Install/Upgrade VMware Tools**.

ESX/ESXi Host Scanning Fails

Scanning is the process in which you generate compliance information about the vSphere objects against attached baselines and baseline groups. In some cases, the scan of ESX 4.0.x and ESXi 4.0.x hosts might fail.

Problem

The scan process of ESX/ESXi hosts might fail.

Cause

If the VMware vCenter Update Manager Update Download task is not completed successfully after you add a host to the vSphere inventory, no host patch metadata is downloaded.

Solution

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 81.

ESXi Host Upgrade Fails

The remediation process of an ESXi host against an upgrade baseline or a baseline group containing an upgrade baseline might fail.

Problem

An ESXi host might fail to upgrade.

Cause

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 completed successfully, the ESXi host is not upgraded.

Solution

1 If you see an Agent Deploy failure, make sure that the `/tmp` directory has at least 10MB of free space.

2 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 patch repository. Update Manager reports the type of conflict. 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 can take action to resolve the conflict.

Conflicting New Module The host update is a new module that provides software for the first time, but is in conflict with either an existing update on the host or another update in the Update Manager repository. Update Manager reports the type of conflict. 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.

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 if a 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.

Updates Are in Conflict or Conflicting New Module State

After you perform a successful scan, the compliance state of the attached baseline might be incompatible because of conflicting updates. The status of the update will be Conflict if the update is a patch, and Conflicting New Module, if the update is a new module.

Problem

The state of the attached baseline is incompatible because an update in the baseline is in conflict with either other updates in the Update Manager patch repository or an existing update on the host.

Cause

- The baseline contains a host update that conflicts with another update already installed on the host.
- The baseline contains a host update that conflicts with other updates in the Update Manager repository.
- The dynamic baseline criteria results in a conflicting set.

- The baseline is attached to a container object and conflicts with one or more inventory objects in the folder. This is an indirect conflict.

Solution

- Detach or remove the baseline containing the update that conflicts with another update already installed on the host.

  If Update Manager suggests a resolution for the conflicting update, add the resolution update into the baseline and retry the scan operation.
- Open the Patch Details or the Extension Details window to see details about the conflict and the other updates with which the selected update is in conflict.
  - If the conflicting updates are in the same baseline, remove the conflicting updates from the baseline and perform the scan again.
  - If the conflicting updates are not in the same baseline, ignore the conflict and proceed to install the updates by starting a remediation.
- Edit the dynamic baseline criteria or exclude the conflicting patches and scan again.

  If Update Manager suggests a resolution for the conflicting patch, add the resolution patches into the baseline and retry the scan operation.
- If the conflict is indirect, you can remediate the container object, but only the objects that are not in conflict are remediated. You should resolve the conflicts or move the inventory objects that are in conflict, and then remediate.

Updates Are in Missing Package State

The compliance state of the attached baseline might be incompatible because packages might be missing from updates.

Problem

When you perform a host upgrade scan, if the binary package for the host is missing or not uploaded, or if you upload the wrong binary package, the scan fails.

Solution

1 Edit the host upgrade baseline and import the required package.

2 Repeat the scan.

Updates Are in Not Installable State

After you perform a scan, the compliance state of the attached baseline might be displayed as incompatible because of updates that cannot be installed on the object.

Problem

The state of the attached baseline is incompatible because it contains updates that cannot be installed.

Cause

- A baseline containing Linux patches is attached to a Red Hat Linux virtual machine. If one or more updates are missing during the scan, they appear as Not Installable.
- A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine on which VMware Tools is not installed. The Upgrade Details window shows the actual reason for the Incompatible state.

- A VMware Tools Upgrade to Match Host baseline is attached to a virtual machine with VMware Tools not managed by the VMware vSphere platform. The Upgrade Details window shows the actual reason for the Incompatible state.

Solution

- No action is required. Update Manager does not support remediation of Linux virtual machines. You can detach the patch baseline.
- If VMware Tools is not installed on the virtual machine, install a version of VMware Tools and retry the scan operation.
- If VMware Tools on the virtual machine is not managed by the VMware vSphere platform, you should detach the baseline and perform the upgrade manually. For more information about upgrading VMware Tools when it is packaged and distributed as OSPs, see *VMware Tools Installation Guide Operating System Specific Packages*.

Updates Are in Unsupported Upgrade State

After you perform a successful scan, the compliance state of the attached baseline might be incompatible because of unsupported upgrade.

Problem

The state of the attached baseline is incompatible because of an unsupported upgrade.

Cause

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.

Solution

No workaround is available. See the upgrade details to check the current hardware version.

Database Views

19

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 19-1. 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 19-2. VUMV_UPDATES

Field	Notes
UPDATE_ID	Unique ID generated by 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: 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, VM_GENERAL, VM_TOOLS, VM_HARDWAREVERSION or VA_GENERAL
UPDATECATEGORY	Specifies whether the update is a patch or an upgrade.

VUMV_HOST_UPGRADES

This database view provides detailed information about the host upgrade packages.

Table 19-3. 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 19-4. 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 of 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 19-5. 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: 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 19-6. 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 19-6. VUMV_BASELINES (Continued)

Field	Notes
TARGET_COMPONENT	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, VM_HARDWAREVERSION, or VA_GENERAL
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 19-7. 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 time that the baseline group was updated

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 19-8. 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 that for operating systems and applications.

Table 19-9. 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 ESXi host, Installable ESXi host

VUMV_BASELINE_ENTITY

This database view contains the objects to which a particular baseline is attached.

Table 19-10. VUMV_BASELINE_ENTITY

Field	Notes
BASELINE_ID	Baseline ID (foreign key, VUMV_BASELINES)
ENTITY_UID	Unique 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 19-11. 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 is applicable.

Table 19-12. 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 scan operations.

Table 19-13. 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	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, VM_HARDWAREVERSION or VA_GENERAL

VUMV_ENTITY_REMEDIATION_HIST

This database view contains the history of remediation operations.

Table 19-14. 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 is applicable.

Table 19-15. VUMV_UPDATE_PRODUCT_DETAILS

Field	Notes
UPDATE_METAUID	Software update ID (foreign key, VUMV_UPDATES)
UPDATE_TITLE	Update title
UPDATE_SEVERITY	Update impact information: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
PRODUCT_NAME	Product name
PRODUCT_VERSION	Product version

VUMV_BASELINE_UPDATE_DETAILS

This database view contains information about the software updates that are part of a baseline.

Table 19-16. 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 19-16. VUMV_BASELINE_UPDATE_DETAILS (Continued)

Field	Notes
SEVERITY	Update severity: 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 19-17. 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: Not Applicable, Low, Moderate, Important, Critical, HostGeneral, and HostSecurity
ENTITY_STATUS	Status of the entity with regard to the update: 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 19-18. 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 the hardware version of a particular virtual machine.

Table 19-19. 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 19-19. 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 virtual appliances.

Table 19-20. 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	Free-form string for API feature compatibility
LASTGOODIP	Last known IP address that 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	Default software update URL of the virtual appliance

VUMV_VA_PRODUCTS

This database view contains information about the virtual appliance vendor.

Table 19-21. VUM_VA_PRODUCTS

Field	Notes
ID	Unique ID, a generated sequence number
VENDORNAME	Vendor name
VENDORUUID	Unique ID of the vendor
PRODUCTNAME	Product name (without 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