

Installing and Administering VMware vSphere Update Manager

Update 2
vSphere Update Manager 5.5

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-001542-01

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

Copyright © 2009–2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

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

Contents

About Installing and Administering VMware vSphere Update Manager	9
Updated Information	11
1 Understanding Update Manager	13
Update Manager Client Overview	14
Update Manager Web Client Overview	14
About the Update Manager Process	15
Configuring the Update Manager Download Source	16
Downloading Updates and Related Metadata	17
Importing ESXi Images	18
Creating Baselines and Baseline Groups	18
Attaching Baselines and Baseline Groups to vSphere Objects	20
Scanning Selected vSphere Objects	21
Reviewing Scan Results	21
Staging Patches and Extensions to Hosts	22
Remediating Selected vSphere Objects	22
2 System Requirements	25
Update Manager Hardware Requirements	25
Supported Operating Systems and Database Formats	26
Update Manager Compatibility with vCenter Server , vSphere Client and vSphere Web Client	26
Required Database Privileges	27
3 Preparing the Update Manager Database	29
Create a 32-Bit DSN on a 64-Bit Operating System	30
About the Bundled Microsoft SQL Server 2008 R2 Express Database Package	30
Maintaining Your Update Manager Database	30
Configure a Microsoft SQL Server Database Connection	30
Create a New Data Source (ODBC)	31
Identify the SQL Server Authentication Type	32
Configure an Oracle Database	32
Configure an Oracle Connection to Work Locally	33
Configure an Oracle Database to Work Remotely	33
4 Installing Update Manager	35
Prerequisites for Installing the Update Manager Server	36
Obtain the Update Manager Installer	37
Install the Update Manager Server	38
Install the Update Manager Client Plug-In	39
Enable the Update Manager Web Client Plug-In	40

5	Upgrading Update Manager	41
	Upgrade the Update Manager Server	42
	Upgrade the Update Manager Client Plug-In	43
	Upgrade the Update Manager Java Components	43
6	Best Practices and Recommendations for Update Manager Environment	45
	Update Manager Deployment Models	45
	Update Manager Deployment Models and Their Usage	47
7	Uninstalling Update Manager	49
	Uninstall the Update Manager Server	49
	Uninstall the Update Manager Client Plug-In	49
8	Installing, Setting Up, and Using Update Manager Download Service	51
	Installing UMDS	51
	Compatibility Between UMDS and the Update Manager Server	52
	Install UMDS	52
	Setting Up and Using UMDS	53
	Set Up the Data to Download with UMDS	54
	Change the UMDS Patch Repository Location	54
	Configure URL Addresses for Hosts and Virtual Appliances	55
	Download the Specified Data Using UMDS	56
	Export the Downloaded Data	56
9	Configuring Update Manager	59
	Update Manager Network Connectivity Settings	60
	Change the Update Manager Network Settings	61
	Configuring the Update Manager Download Sources	62
	Configure Update Manager to Use the Internet as a Download Source	63
	Add a New Download Source	64
	Use a Shared Repository as a Download Source	64
	Import Patches Manually	66
	Configure the Update Manager Proxy Settings	66
	Configure Checking for Updates	67
	Configuring and Viewing Notifications	68
	Configure Notifications Checks	68
	View Notifications and Run the Notification Checks Task Manually	69
	Types of Update Manager Notifications	70
	Take Snapshots Before Remediation	70
	Configuring Host and Cluster Settings	71
	Configure Host Maintenance Mode Settings	72
	Configure Cluster Settings	73
	Enable Remediation of PXE Booted ESXi 5.x Hosts	74
	Configure Smart Rebooting	75
	Configure the Update Manager Patch Repository Location	75
	Configure Mail Sender Settings	76
	Restart the Update Manager Service	76

Run the VMware vSphere Update Manager Update Download Task	76
Update Manager Privileges	77
10 Working with Baselines and Baseline Groups	79
Creating and Managing Baselines	80
Create and Edit Patch or Extension Baselines	80
Create and Edit Host Upgrade Baselines	84
Create and Edit a Virtual Appliance Upgrade Baseline	87
Delete Baselines	89
Creating and Managing Baseline Groups	89
Create a Host Baseline Group	90
Create a Virtual Machine and Virtual Appliance Baseline Group	91
Edit a Baseline Group	91
Add Baselines to a Baseline Group	92
Remove Baselines from a Baseline Group	92
Delete Baseline Groups	93
Attach Baselines and Baseline Groups to Objects	93
Attach Baselines and Baseline Groups to Objects in Update Manager Web Client	94
Filter the Baselines and Baseline Groups Attached to an Object	94
Detach Baselines and Baseline Groups from Objects	95
Detach Baselines and Baseline Groups from Objects in Update Manager Web Client	96
11 Scanning vSphere Objects and Viewing Scan Results	97
Manually Initiate a Scan of ESX/ESXi Hosts	97
Manually Initiate a Scan of ESX/ESXi Hosts in Update Manager Web Client	98
Manually Initiate a Scan of Virtual Machines and Virtual Appliances	98
Manually Initiate a Scan of Virtual Machines and Virtual Appliances in Update Manager Web Client	99
Manually Initiate a Scan of a Datacenter in Update Manager Web Client	99
Schedule a Scan	100
Viewing Scan Results and Compliance States for vSphere Objects	100
View Compliance Information for vSphere Objects	101
Review Compliance with Individual vSphere Objects	101
Compliance View	102
Compliance States for Updates	104
Baseline and Baseline Group Compliance States	105
Viewing Patch Details	106
Viewing Extension Details	107
Viewing Upgrade Details	107
Host Upgrade Scan Messages in Update Manager	109
Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present	111
VMware Tools Status	112
12 Remediating vSphere Objects	115
Orchestrated Upgrades of Hosts and Virtual Machines	115
Remediating Hosts	116
Remediation Specifics of ESX Hosts	118
Remediation Specifics of ESXi Hosts	118

	Remediation Specifics of ESXi 5.x Hosts	119
	Remediation Specifics of Hosts That Are Part of a Virtual SAN Cluster	120
	Remediating Hosts That Contain Third-Party Software	121
	Stage Patches and Extensions to ESX/ESXi Hosts	121
	Remediate Hosts Against Patch or Extension Baselines	122
	Remediate Hosts Against an Upgrade Baseline	125
	Remediate Hosts Against Baseline Groups	127
	Cluster Remediation Options Report	130
	Remediating Virtual Machines and Virtual Appliances	131
	Rolling Back to a Previous Version	131
	Remediate Virtual Machines and Virtual Appliances	131
	Upgrade VMware Tools on Power Cycle	132
	Scheduling Remediation for Hosts, Virtual Machines, and Virtual Appliances	133
13	View Update Manager Events	135
	View Tasks and Events for a Selected Object	135
	Update Manager Events	136
14	Patch Repository and Virtual Appliance Upgrades	147
	View Available Patches and Extensions	147
	Add and Remove Patches or Extensions from a Baseline	148
	Host Patch Severity and Host Patch Category	148
	Severity and Category Values in Different vSphere Releases	148
	Search for Patches or Extensions in the Patch Repository	150
	View Available Virtual Appliance Upgrades and Accept EULAs	151
15	Common User Goals	153
	Applying Patches to Hosts	154
	Applying Third-Party Patches to Hosts	155
	Testing Patches or Extensions and Exporting Baselines to Another Update Manager Server	157
	Applying Extensions to Hosts	160
	Orchestrated Datacenter Upgrades	161
	Orchestrated Upgrade of Hosts	162
	Orchestrated Upgrade of Virtual Machines	163
	Upgrading and Patching Hosts Using Baseline Groups	164
	Upgrading Virtual Appliances	165
	Keeping the Hosts Compliant With the Most Recent Patches	166
	Associating the UMDS Patchstore Depot with the Update Manager Server	167
	Associate the UMDS Depot with the Update Manager Server Using a Portable Media Drive	168
	Associate the UMDS Depot with Update Manager Server Using IIS	169
	Associate the UMDS Depot with Update Manager Server Using Apache	170
	Generating Common Database Reports	171
	Generate Common Reports Using Microsoft Office Excel 2003	171
	Generate Common Reports Using Microsoft SQL Server Query	172
	Setting a Bandwidth Limit for Downloading of ESXi 5.x Patches	173
	Limit the Update Download Bandwidth by Using the vSphere Client	173
	Limit the Update Download Bandwidth by Running an esxcli Command	174

16	Troubleshooting	175
	Update Manager Web Client Remains Visible in the vSphere Web Client After Uninstalling Update Manager Server	176
	Connection Loss with Update Manager Server or vCenter Server in a Single vCenter Server System	176
	Connection Loss with Update Manager Server or vCenter Server in a Connected Group in vCenter Linked Mode	177
	Gather Update Manager Log Bundles	178
	Gather Update Manager and vCenter Server Log Bundles	178
	Log Bundle Is Not Generated	178
	Host Extension Remediation or Staging Fails Due to Missing Prerequisites	179
	No Baseline Updates Available	179
	All Updates in Compliance Reports Are Displayed as Not Applicable	180
	All Updates in Compliance Reports Are Unknown	180
	VMware Tools Upgrade Fails if VMware Tools Is Not Installed	180
	ESX/ESXi Host Scanning Fails	181
	ESXi Host Upgrade Fails	181
	The Update Manager Repository Cannot Be Deleted	181
	Incompatible Compliance State	182
	Updates Are in Conflict or Conflicting New Module State	183
	Updates Are in Missing Package State	183
	Updates Are in Not Installable State	184
	Updates Are in Unsupported Upgrade State	184
17	Database Views	185
	VUMV_VERSION	186
	VUMV_UPDATES	186
	VUMV_HOST_UPGRADES	186
	VUMV_VA_UPGRADES	187
	VUMV_PATCHES	187
	VUMV_BASELINES	187
	VUMV_BASELINE_GROUPS	188
	VUMV_BASELINE_GROUP_MEMBERS	188
	VUMV_PRODUCTS	188
	VUMV_BASELINE_ENTITY	189
	VUMV_UPDATE_PATCHES	189
	VUMV_UPDATE_PRODUCT	189
	VUMV_ENTITY_SCAN_HISTORY	189
	VUMV_ENTITY_REMEDIATION_HIST	190
	VUMV_UPDATE_PRODUCT_DETAILS	190
	VUMV_BASELINE_UPDATE_DETAILS	190
	VUMV_ENTITY_SCAN_RESULTS	191
	VUMV_VMTOOLS_SCAN_RESULTS	191
	VUMV_VMHW_SCAN_RESULTS	191
	VUMV_VA_APPLIANCE	192
	VUMV_VA_PRODUCTS	192
	Index	193

About Installing and Administering VMware vSphere Update Manager

Installing and Administering VMware vSphere Update Manager provides information about installing, configuring, and using VMware® vSphere Update Manager to scan and remediate the objects in your vSphere environment. It also describes the tasks that you can perform to update your vSphere inventory objects and make them compliant against attached baselines and baseline groups.

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

- 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/ESXi 4.0 and later.
- For ESX/ESXi host upgrade and migration operations, Update Manager works with ESX/ESXi 4.0 and later.

NOTE Update Manager 5.x does not support virtual machine patch operations.

Intended Audience

This information is intended for anyone who wants to install, upgrade, or use Update Manager. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Updated Information

This *About Installing and Administering VMware vSphere Update Manager* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *About Installing and Administering VMware vSphere Update Manager* documentation.

Revision	Description
EN-001542-01	■ Added a new topic: “Obtain the Update Manager Installer,” on page 37. The new topic provides a more thorough procedure and clearly states that the Update Manager installer is an integral part of the vCenter Server installer.
EN-001542-00	Initial release.

Understanding Update Manager

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.

With Update Manager, you can perform the following tasks:

- Upgrade and patch ESX/ESXi hosts.
- Install and update third-party software on hosts.
- Upgrade virtual machine hardware, VMware Tools, and virtual appliances.

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 server component, which you can install either on the same computer as the vCenter Server system or on a different computer, and of client components. There is an Update Manager Client that runs on the vSphere Client, and an Update Manager Web Client that runs on the vSphere Web Client. You can use Update Manager Web Client to view scan results and compliance states for vSphere inventory objects, and use the Update Manager Client to perform patch and version management of the vSphere inventory.

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.

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

This chapter includes the following topics:

- [“Update Manager Client Overview,”](#) on page 14
- [“Update Manager Web Client Overview,”](#) on page 14
- [“About the Update Manager Process,”](#) on page 15

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 and available virtual appliance upgrades
- Review and check notifications
- Import ESXi images

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.

Update Manager Web Client Overview

Starting with Update Manager 5.1 Update 1, a new Update Manager Web Client plug-in for the vSphere Web Client is provided. If vSphere Web Client is the primary client that you use to manage your vSphere inventory, you can use the Update Manager Web Client to view scan results and compliance states for vSphere inventory objects, and later remediate them from the Update Manager Client plug-in in the vSphere Client.

Update Manager Web Client is enabled by default in the vSphere Web Client, after you install the Update Manager server component. The Update Manager Web Client appears as an **Update Manager** tab under the **Monitor** tab in vSphere Web Client.

To be able to see the Update Manager Web Client in vSphere Web Client you must have the **View Compliance Status** privilege.

By using Update Manager Web Client, you can perform the following tasks:

- Attach and detach baselines and baseline groups from a selected inventory object

- View compliance and scan results for each selected inventory object
- Scan a selected inventory object

Operations such as creating baselines and baseline groups, importing ESXi images, staging, and remediation are available only from the Update Manager Client plug-in in the vSphere Client.

In Update Manager Web Client, you can initiate scans on a datacenters and datacenter folders.

Except from the **Update Manager** tab, compliance information for an inventory object is also available from the **Summary** tab of the vSphere Web Client, in the **Update Manager Compliance** portlet. You can initiate a scan from the summary page of an object, but for a detailed status of the scan operation, you have to go to the **Update Manager** tab.

About the Update Manager Process

Upgrading vSphere objects and applying patches or 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, extensions, and virtual appliance upgrades. 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 Download Source](#) on page 16
You can configure the Update Manager server to download patches, extensions, and virtual appliance upgrades either from the Internet or from a shared repository. You can also import patches and extensions manually from a ZIP file.
- [Downloading Updates and Related Metadata](#) on page 17
Downloading virtual appliance upgrades, host patches, extensions, and related metadata is a predefined automatic process that you can modify. By default, at regular configurable intervals, Update Manager contacts VMware or third-party sources to gather the latest information (metadata) about available upgrades, patches, or extensions.
- [Importing ESXi Images](#) on page 18
You can upgrade or migrate the hosts in your environment to ESXi 5.5 by using host upgrade baselines. To create a host upgrade baseline, you must first upload at least one ESXi 5.5 .iso image 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 patch, extension, or upgrade baselines. Baseline groups are assembled from existing baselines.
- [Attaching Baselines and Baseline Groups to vSphere Objects](#) on page 20
To use baselines and baseline groups, you must attach them to selected inventory objects such as container objects, virtual machines, virtual appliances, or hosts. You can attach baselines and baseline groups to vSphere objects from both the Update Manager Client and the Update Manager Web Client.

- [Scanning Selected vSphere Objects](#) on page 21

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 21

Update Manager scans vSphere objects to determine how they comply with baselines and baseline groups that you attach. You can filter scan results by text search, group selection, baseline selection, and compliance status selection.

- [Staging Patches and Extensions to Hosts](#) on page 22

You can stage 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 that can reduce the time during which hosts are in maintenance mode.

- [Remediating Selected vSphere Objects](#) on page 22

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.

Configuring the Update Manager Download Source

You can configure the Update Manager server to download patches, extensions, and virtual appliance upgrades either from the Internet or from a shared repository. You can also import patches and extensions manually from a ZIP file.

Configuring the Update Manager 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 upgrades, patches, and extensions to the Update Manager repository. You can also add URL addresses to download virtual appliance upgrades or third-party patches and extensions. Third-party patches and extensions are applicable only to hosts that are running ESX/ESXi 4.0 and later.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see [Chapter 8, “Installing, Setting Up, and Using Update Manager Download Service,”](#) on page 51.

With Update Manager, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. Import of offline bundles is supported only for hosts that are running ESX/ESXi 4.0 and later. You download the offline bundle ZIP files from the Internet or copy them from a media drive, and save them on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later. You can download offline bundles from the VMware Web site or from the Web sites of third-party vendors.

NOTE You can use offline bundles for host patching operations only. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESX/ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5.

For detailed descriptions of the procedures, see [“Configuring the Update Manager Download Sources,”](#) on page 62.

Downloading Updates and Related Metadata

Downloading virtual appliance upgrades, host patches, extensions, and related metadata is a predefined automatic process that you can modify. By default, at regular configurable intervals, Update Manager contacts VMware or third-party sources to gather the latest information (metadata) about available upgrades, patches, or extensions.

VMware provides information about patches for ESX/ESXi hosts and virtual appliance upgrades.

Update Manager downloads the following types of information:

- Metadata about all ESX/ESXi 4.x and ESXi 5.x patches regardless of whether you have hosts of such versions in your environment.
- Metadata about ESX/ESXi 4.x and ESXi 5.x patches as well as about extensions from third-party vendor URL addresses.
- Notifications, alerts, and patch recalls for ESX/ESXi 4.x and ESXi 5.x hosts.
- Metadata about upgrades for virtual appliances.

Downloading information about all updates is a relatively low-cost operation in terms of disk space and network bandwidth. The availability of regularly updated metadata lets you add scanning tasks for hosts or appliances at any time.

Update Manager supports the recall of patches for hosts that are running ESX/ESXi 4.0 or later. 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 to 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.

If Update Manager cannot download upgrades, patches, or extensions—for example, if it is deployed on an internal network segment that does not have Internet access—you must use UMDS to download and store the data on the machine on which UMDS is installed. The Update Manager server can use the upgrades, patches, and extensions that UMDS downloaded after you export them.

For more information about UMDS, see [Chapter 8, “Installing, Setting Up, and Using Update Manager Download Service,”](#) on page 51.

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

You can change the time intervals at which Update Manager downloads updates or checks for notifications. For detailed descriptions of the procedures, see [“Configure Checking for Updates,”](#) on page 67 and [“Configure Notifications Checks,”](#) on page 68.

Types of Software Updates and Related Terms

Update Manager downloads software updates and metadata from Internet depots or UMDS-created shared repositories. You can import offline bundles and host upgrade images from a local storage device into the local Update Manager repository.

Bulletin	A grouping of one or more VIBs. Bulletins are defined within metadata.
Depot	A logical grouping of VIBs and associated metadata that is published online.
Host upgrade image	An ESXi image that you can import in the Update Manager repository and use for upgrading ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 hosts to ESXi 5.5.

Extension	A bulletin that defines a group of VIBs for adding an optional component to a ESX host. An extension is usually provided by a third party that is also responsible for patches or updates to the extension.
Metadata	Extra data that defines dependency information, textual descriptions, system requirements, and bulletins.
Offline bundle ZIP	An archive that encapsulates VIBs and corresponding metadata in a self-contained package that is useful for offline patching. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 hosts to ESXi 5.5.
Patch	A bulletin that groups one or more VIBs together to address a particular issue or enhancement.
Roll-up	A collection of patches that is grouped for ease of download and deployment.
VA upgrade	Updates for a virtual appliance, which the vendor considers an upgrade.
VIB	A VIB is a single software package.

Importing ESXi Images

You can upgrade or migrate the hosts in your environment to ESXi 5.5 by using host upgrade baselines. To create a host upgrade baseline, you must first upload at least one ESXi 5.5 .iso image to the Update Manager repository.

With Update Manager 5.5 you can upgrade or migrate hosts that are running ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 to ESXi 5.5. Host upgrades to ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 are not supported.

Before uploading ESXi images, obtain the image files from the VMware Web site or another source. You can create custom ESXi images that contain third-party VIBs by using ESXi Image Builder CLI. For more information, see *Using vSphere ESXi Image Builder CLI*.

You can upload and manage ESXi images from the **ESXi Images** tab of the Update Manager Administration view.

ESXi images that you import are kept in the Update Manager repository. You can include ESXi images in host upgrade baselines. To delete an ESXi image from the Update Manager repository, first you must delete the upgrade baseline that contains it. After you delete the baseline, you can delete the image from the **ESXi Images** tab.

For more information about importing ESXi images and creating host upgrade baselines, see [“Create a Host Upgrade Baseline,”](#) on page 86.

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 patch, extension, or upgrade baselines. Baseline groups are assembled from existing baselines.

Host baseline groups can contain a single upgrade baseline, as well as a number of patch and extension baselines.

Virtual machine and virtual appliance baseline groups can contain up to three upgrade baselines: one VMware Tools upgrade baseline, one virtual machine hardware upgrade baseline, and one virtual appliance upgrade baseline.

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 two predefined patch baselines and three predefined upgrade baselines. You cannot edit or delete the three predefined virtual machine and virtual appliance upgrade baselines. You can use the predefined baselines, or create patch, extension, and upgrade baselines that meet your criteria. Baselines you create, as well as predefined baselines, can be combined in baseline groups. For more information about creating and managing baselines and baseline groups, see [Chapter 10, “Working with Baselines and Baseline Groups,”](#) on page 79.

Baseline Types

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

Update Manager provides upgrade, patch, and extension baselines.

Upgrade Baselines

Baseline	Description
Host Upgrade Baseline	Defines to which version to upgrade or migrate the hosts in your environment. With Update Manager, you can upgrade or migrate ESX/ESXi hosts from version 4.x and ESXi hosts from version 5.0 and 5.1 to ESXi 5.5.
Virtual Appliance Upgrade Baseline	Defines to which version to upgrade a selected virtual appliance. For example, you can upgrade to the latest released virtual appliance version by using the predefined VA Upgrade to Latest (Predefined) baseline.
Virtual Machine Upgrade Baseline	Defines to which version to upgrade virtual hardware or VMware Tools. With Update Manager 5.5 you can upgrade to hardware version vmx-10 and to the latest VMware Tools version on hosts that are running ESXi 5.5.

Patch Baselines

Patch baselines define a number of patches that must be applied to a given host. Patch baselines can be either dynamic or fixed.

Baseline	Description
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	You manually specify which patches to include in the fixed patch baseline from the total set of patches available in the Update Manager repository.

Extension Baselines

Baseline	Description
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.

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 the hosts in your environment are updated with the latest patches, or whether the virtual appliances and virtual machines are upgraded to the latest version.

Critical Host Patches (Predefined)	Checks ESX/ESXi hosts for compliance with all critical patches.
Non-Critical Host Patches (Predefined)	Checks ESX/ESXi hosts for compliance with all optional patches.
VMware Tools Upgrade to Match Host (Predefined)	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 (Predefined)	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 vmx-10 on hosts that are running ESXi 5.5.
VA Upgrade to Latest (Predefined)	Checks virtual appliance compliance with the latest released virtual appliance version.

Baseline Groups

Baseline groups can contain patch, extension, and upgrade baselines. The baselines that you add to a baseline group must be non-conflicting.

A baseline group is limited to a combination of patches, extensions, and upgrades. The following are valid combinations of baselines that can make up a baseline group:

- Multiple host patch and extension baselines.
- One upgrade baseline, multiple patch and 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. You cannot create a baseline group containing two virtual appliance upgrade baselines.

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. You can attach baselines and baseline groups to vSphere objects from both the Update Manager Client and the Update Manager Web Client.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and datacenters. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

For a detailed description of the procedure, see [“Attach Baselines and Baseline Groups to Objects,”](#) on page 93 for Update Manager Client or [“Attach Baselines and Baseline Groups to Objects in Update Manager Web Client,”](#) on page 94.

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 it is up to date with the latest virtual hardware or VMware Tools version.

Update Manager supports the following types of scan:

Host patch scan	You can perform patch scans on ESX/ESXi 4.0 and later.
Host extensions scan	You can scan ESX/ESXi 4.0 and later for extensions (additional software modules).
Host upgrade scan	You can scan ESX/ESXi 4.x, ESXi 5.0 and ESXi 5.1 for upgrading to ESXi 5.5.
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.

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 11, “Scanning vSphere Objects and Viewing Scan Results,”](#) on page 97.

Reviewing Scan Results

Update Manager scans vSphere objects to determine how they comply with baselines and baseline groups that you attach. You can filter scan results by text search, group selection, baseline selection, and compliance status selection.

When you select a container object, you view the overall compliance status of the container against the attached baselines as a group. You also see the individual compliance statuses of the objects in the selected container against all baselines. If you select an individual baseline attached to the container object, you see the compliance status of the container against the selected 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 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 100.

Staging Patches and Extensions to Hosts

You can stage 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 that can reduce the time during which hosts are in maintenance mode.

Staging patches and extensions to hosts that are running ESX/ESXi 4.0 or later lets you 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 4.x hosts. Update Manager can stage patches to PXE booted ESXi 5.x hosts.

For more information about staging patches, see [“Stage Patches and Extensions to ESX/ESXi Hosts,”](#) on page 121.

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 makes the selected vSphere objects compliant with patch, extension, and upgrade baselines.

As with scanning, you can remediate single hosts, virtual machines, or virtual appliances, and you can also initiate remediation on the folder, cluster, or datacenter level, as well as on all objects in your virtual infrastructure.

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 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.

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 12, “Remediating vSphere Objects,”](#) on page 115.

Remediating Hosts

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

IMPORTANT Update Manager neither upgrades nor patches PXE booted ESXi hosts of version 4.x and skips them when you remediate hosts in a container object. You can patch PXE booted ESXi 5.x hosts if you enable the setting from the **ESX Host/Cluster Settings** page of the **Configuration** tab or from the Remediate wizard.

After you upload ESXi images, upgrades for ESX/ESXi hosts are managed through baselines and baseline groups.

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.

IMPORTANT After you have upgraded or migrated your host to ESXi 5.5, you cannot roll back to your version ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software. Back up your host configuration before performing an upgrade or migration. If the upgrade or migration fails, you can reinstall the ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software that you upgraded or migrated from, and restore your host configuration. For more information about backing up and restoring your ESX/ESXi configuration, see *vSphere Upgrade*.

Remediating Virtual Machines and Virtual Appliances

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.

NOTE Update Manager 5.x does not support virtual machine patch baselines.

Orchestrated Upgrades

With Update Manager, you can perform orchestrated upgrades of hosts and virtual machines. Orchestrated upgrades allow you to upgrade hosts and virtual machines in your vSphere inventory by using baseline groups.

You can perform an orchestrated upgrade of hosts by using a baseline group that contains a single host upgrade baseline and multiple patch or extension baselines. Update Manager first upgrades the hosts and then applies the patch or extension baselines.

You can perform an orchestrated upgrade of virtual machines by using a virtual machine baseline group that contains the following baselines:

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

You can use orchestrated upgrades to upgrade the virtual hardware and VMware Tools of virtual machines in the inventory at the same time. The VMware Tools upgrade baseline runs first, followed by the virtual machine hardware upgrade baseline.

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

System Requirements

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 2008 R2 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,”](#) on page 25
- [“Supported Operating Systems and Database Formats,”](#) on page 26
- [“Update Manager Compatibility with vCenter Server, vSphere Client and vSphere Web Client,”](#) on page 26
- [“Required Database Privileges,”](#) on page 27

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, verify that your system meets the minimum hardware requirements.

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 vSphere Update Manager Sizing Estimator*. You can find the *VMware vSphere Update Manager Sizing Estimator* on the [vSphere Update Manager Documentation](#) page. Use the drop-down menu on the page to select the respective release version of the sizing estimator you need.

Supported Operating Systems and Database Formats

Update Manager works with specific databases and operating systems.

The Update Manager server requires a 64-bit Windows system.

NOTE Make sure the system on which you are installing the Update Manager server is not an Active Directory domain controller.

The Update Manager plug-in requires the vSphere Client, and works with the same operating systems as the vSphere Client.

Update Manager scans and remediates Windows and Linux virtual machines for VMware Tools and virtual hardware upgrades.

The Update Manager server requires SQL Server or Oracle database. Update Manager can handle small-scale environments using the bundled SQL Server 2008 R2 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.

To see a list of operating systems on which you can install the Update Manager server and the UMDS, see [Supported host operating systems for VMware vCenter Server installation](#). The supported host operating systems for vCenter Server installation listed in the article also apply for installation of the respective versions of the Update Manager server and the UMDS.

To see a list of database formats that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Update Manager Compatibility with vCenter Server , vSphere Client and vSphere Web Client

Update Manager and vCenter Server must be of compatible versions. The Update Manager Client plug-in can be installed and enabled only on vSphere Client of a compatible version. The Update Manager Web Client is automatically enabled on a vSphere Web Client of a compatible version after installation of the Update Manager server.

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

Update Manager 5.5 is compatible only with vCenter Server 5.5. Although multiple versions of the Update Manager Client plug-in might coexist on the same computer, the Update Manager Client plug-in of version 5.5 can be installed and enabled only on vSphere Client 5.5.

During installation you connect the Update Manager 5.5 server to a vCenter Server 5.5 system. After the installation, the Update Manager Web Client 5.5 is automatically enabled on the vSphere Web Client 5.5 that you use to connect to this vCenter Server system.

To see more information about the Update Manager compatibility with vCenter Server, vSphere Client and vSphere Web Client, select the **Solution Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Required Database Privileges

The set of database privileges needed for the Update Manager installation and upgrade differs from the set of privileges needed for the Update Manager administration.

Before installing or upgrading Update Manager, you must grant adequate privileges to the database user.

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

Database	Privileges
Oracle	<p>Either assign the DBA role, or grant the following set of privileges to the Update Manager Oracle database user.</p> <ul style="list-style-type: none"> ■ 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	<p>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.</p>

To run Update Manager, you must grant a set of minimum privileges to the database user.

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

Database	Privileges
Oracle	<p>The minimum required privileges of the Oracle database user are the following:</p> <ul style="list-style-type: none"> ■ create session ■ create any table ■ drop any table
Microsoft SQL Server	<p>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.</p>

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 2008 R2 Express (64-bit).

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 2008 R2 Express, you can install and configure the database when you install Update Manager. Microsoft SQL Server 2008 R2 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. If the database user name and password change after you install the Update Manager server or UMDS, you can reconfigure Update Manager and UMDS without the need to reinstall them. See *Reconfiguring VMware vSphere Update Manager*.

Before you begin the database setup, review the supported databases. If you create an ODBC connection to a database server that is not supported, a DSN for the unsupported database might be displayed in the drop-down menu of the Update Manager installation wizard. For more information about the supported database patches, see *VMware Product Interoperability 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,”](#) on page 30
- [“About the Bundled Microsoft SQL Server 2008 R2 Express Database Package,”](#) on page 30
- [“Maintaining Your Update Manager Database,”](#) on page 30
- [“Configure a Microsoft SQL Server Database Connection,”](#) on page 30
- [“Configure an Oracle Database,”](#) on page 32

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 2008 R2 Express Database Package

The Microsoft SQL Server 2008 R2 Express database package is installed and configured when you select Microsoft SQL Server 2008 R2 Express as your database during the 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	<ol style="list-style-type: none"> a Click Add. b For Microsoft SQL Server 2008, Microsoft SQL Server 2008 R2 Express, Microsoft SQL Server 2012, or Microsoft SQL Server 2014 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.

To see a detailed list of all Microsoft SQL Server database versions that are compatible with the Update Manager server and the UMDS, select the **Solution/Database Interoperability** option from the *VMware Product Interoperability Matrixes* at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- 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.

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 11g or Oracle 12c 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.

NOTE For Oracle database servers of version 11.2.0.3 or 11.2.0.4, use Oracle Instant Client Package - ODBC of version 11.2.0.2 for 32-bit Microsoft Windows.

- 3 Install the corresponding Oracle ODBC driver through the Oracle Universal Installer.
- 4 Increase the number of open cursors for the database.

Add the entry **open_cursors = 300** to the *ORACLE_BASE\ADMIN\VUM\pfile\init.ora* file.

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

Verify that the ODBC data source that you use is a 32-bit system DSN. See [“Create a 32-Bit DSN on a 64-Bit Operating System,”](#) on page 30.

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

- Verify that the ODBC data source that you use is a 32-bit system DSN. See [“Create a 32-Bit DSN on a 64-Bit Operating System,”](#) on page 30.
- Set up a 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

Update Manager consists of a server component and a plug-in component. 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. To improve performance, especially in large-scale environments, install the Update Manager server component on a different computer. After you install the Update Manager server component, to use the Update Manager application, you must install the Update Manager Client plug-in and enable it on the vSphere Client.

Update Manager 5.1 Update 1 provides an Update Manager Web Client plug-in for vSphere Web Client. After you install the Update Manager server component, the Update Manager Web Client plug-in is automatically enabled on vSphere Web Client. The Update Manager Web Client plug-in appears as an **Update Manager** tab under the **Monitor** tab in vSphere Web Client.

You can use Update Manager with a Update Manager instance installed on a Windows machine or with the VMware vCenter Server Appliance.

The Update Manager 5.5 installer generates a 2048-bit key and self-signed certificate. To replace the self-signed SSL certificate after installation, you can use the Update Manager Utility.

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.

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

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 run Update Manager in deployments that you protect using SRM. Use caution before connecting the Update Manager server to a vCenter Server instance to which the SRM server is connected. Connecting the Update Manager server to the same vCenter Server instance as SRM might cause problems when you upgrade SRM or vSphere, and when you perform daily tasks. Check the compatibility and interoperability of Update Manager with SRM before you deploy.

This chapter includes the following topics:

- [“Prerequisites for Installing the Update Manager Server,”](#) on page 36
- [“Obtain the Update Manager Installer,”](#) on page 37
- [“Install the Update Manager Server,”](#) on page 38

- [“Install the Update Manager Client Plug-In,”](#) on page 39
- [“Enable the Update Manager Web Client Plug-In,”](#) on page 40

Prerequisites for Installing the Update Manager Server

Before you install the Update Manager server, review the installation prerequisites.

Update Manager Database Requirements

Update Manager requires an Oracle or SQL Server database. Update Manager can handle small-scale environments using the bundled SQL Server 2008 R2 Express. For environments with more than 5 hosts and 50 virtual machines, you must create either an Oracle or SQL Server database. For large-scale environments, set up the database on a machine different than the machines on which the Update Manager server is installed and the vCenter Server database is located.

For more information about setting up the Update Manager database, see [Chapter 3, “Preparing the Update Manager Database,”](#) on page 29.

- Create a database and 32-bit DSN, unless you are using the bundled SQL Server 2008 R2 Express.
- Make sure that if the Update Manager database is located on a remote machine, the database and the system DSN use SQL Server authentication.

Update Manager does not support Windows authentication of the database when the database is located on a different machine because of local system account problems.

- If you plan to use the bundled Microsoft SQL Server 2008 R2 Express database, make sure that you install Microsoft Windows Installer version 4.5 (MSI 4.5) on your system. You can download MSI 4.5 from the vSphere installer.
- Make sure that the database privileges meet the requirements listed in [“Required Database Privileges,”](#) on page 27.
- Create the 32-bit ODBC connection to a supported database server version by using a supported database client version.

If you create an ODBC connection to a database server that is of an unsupported version, and your database client is of a supported version, a DSN for the unsupported database might be displayed in the drop-down menu of the Update Manager installation wizard.

vCenter Server Installation

- Install vCenter Server.

If prompted, you must restart the machine on which vCenter Server is installed. Otherwise, you might not be able to register Update Manager with vCenter Server, and the Update Manager installation might fail.

For more information about installing vCenter Server, see *vSphere Installation and Setup*.

- Gather the following networking information for the vCenter Server system.

- User name and password for the vCenter Server system.

During the Update Manager installation process, you must register the Update Manager server with the vCenter Server system. 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 *vCenter Server and Host Management*.

- Port numbers. In most cases, the default Web service port 80 is used.

- IP address.

If the IP address of the vCenter Server system or Update Manager changes, you can re-register the Update Manager server with the vCenter Server system. For more information about configuring the Update Manager server after installation, see *Reconfiguring VMware vSphere Update Manager*.

Update Manager System Requirements

- Make sure that your system meets the requirements specified in [Chapter 2, “System Requirements,”](#) on page 25.

IMPORTANT You can install the Update Manager 5.5 server component only on a 64-bit machine. Make sure the system on which you are installing the Update Manager server is not an Active Directory domain controller.

- Log in as a local Administrator or a domain user that is member of the Administrators group.

Obtain the Update Manager Installer

You install the Update Manager components from the vCenter Server installer for Windows.

Update Manager can only run on a 64-bit Windows operating system. If you want to use a vCenter Server Appliance to manage your virtual environment, you still need to obtain the vCenter Server installer for Windows to install the Update Manager server or the UMDS on a Windows host machine of a supported version.

Prerequisites

Create a My VMware account at <https://my.vmware.com/web/vmware/>.

Procedure

- 1 Download the vCenter Server installer from the VMware Web site at <https://my.vmware.com/web/vmware/downloads>.

vCenter Server is part of VMware vCloud Suite and of VMware vSphere, listed under Datacenter & Cloud Infrastructure.
 - a Under Datacenter & Cloud Infrastructure, select VMware vCloud Suite or VMware vSphere, and click **Download Product**.
 - b Select a version from the **Select Version** drop-down menu to switch to the product version you need.
 - c Find VMware vCenter Server on that page, and select **Go to Downloads**.
 - d Download the .iso file of the VMware vCenter Server *<product version>* and Modules for Windows.
- 2 Confirm that the md5sum is correct.

See the VMware Web site topic Using MD5 Checksums at <http://www.vmware.com/download/md5.html>.
- 3 Mount the ISO image to the Windows virtual machine or physical server on which you want to install the Update Manager server or the UMDS.

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

See installation prerequisites in [“Prerequisites for Installing the Update Manager Server,”](#) on page 36.

Check the compatibility and interoperability of the vCenter Server server with SRM. You should use caution when connecting the Update Manager server to a vCenter Server instance to which the SRM server is connected. Connecting the Update Manager server to the same vCenter Server instance as SRM might cause problems when you upgrade SRM or vSphere, and when you perform daily operations.

Procedure

- 1 In the software installer directory, double-click the `autorun.exe` file and select **vSphere Update Manager**.

If you cannot run `autorun.exe`, browse to the `UpdateManager` folder 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 Review the support information, select whether to download updates from the default download sources immediately after installation, and click **Next**.

If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click the **Download Now** button on the Download Settings page. You can modify the default download schedule after the installation is complete.

If you deselect **Download updates from default sources immediately after installation**, the update download task runs after installation, but it does not download any updates.

- 7 Type 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**.
- 8 Select the type of database that you want to use.

- If you do not have an existing database, select **Install a Microsoft SQL Server 2008 R2 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, type the user name and password for the DSN and click **Next**.

IMPORTANT The DSN must be a 32-bit DSN.

- 9 (Optional) Select the database options.
 - If the system DSN you specify points to an existing Update Manager database with the current schema, you can either retain your existing database or replace it with an empty one.
 - If the system DSN you specify points to an existing Update Manager database with different 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**.

- 10 From the drop-down menu, select the IP address or the host name of your Update Manager instance.

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, you must select the correct IP address or use a DNS name. The DNS name must be resolved from all hosts that this Update Manager instance will manage.

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

NOTE Use caution when you specify the Update Manager port settings, as you cannot modify them after installation.

For the SOAP port, you have no limitations to the range of ports used, as long as there are no conflicts.

For the Server port, you can use the following range: 80, 9000-9100. Update Manager automatically opens ESX/ESXi firewall ports in this range to allow outbound HTTP traffic to the patch store.

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

- 13 Select the Update Manager 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.

- 14 (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 120GB free space.

- 15 Click **Install** to begin the installation.

- 16 Click **Finish**.

The Update Manager server component is installed, and the client component appears as an available plug-in in the Plug-in Manager of the vSphere Client.

What to do next

In the vSphere Client, select **Plug-ins > Manage Plug-ins** to install and enable the Update Manager Client plug-in.

Install the Update Manager Client Plug-In

To use Update Manager, you must install the Update Manager Client plug-in, 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

- Install the Update Manager server.
- Install Microsoft.NET Framework 3.5 SP1. You can download it from the vSphere installer.

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 Plug-in Manager window, click **Download and install** for the VMware vSphere Update Manager extension.
- 4 Select a language for the installer and 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 Click **Install**.
- 9 Complete the Update Manager Client installation, and click **Finish**.
The status for the Update Manager extension is displayed as Enabled.
- 10 Click **Ignore** if a security warning appears.
The security warning appears when the vSphere client detects a certificate that is not added in the Trusted Root Certification Authorities store. This is usually the case with the self-signed certificate used by ESX/ESXi hosts by default. For highly secure environments, you must set up a trusted third-party certificate later.
- 11 Click **Close** to close the Plug-in Manager window.

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

Enable the Update Manager Web Client Plug-In

You can use the Update Manager Web Client plug-in to use some of the Update Manager features from the vSphere Web Client.

Prerequisites

Verify you have the **View Compliance Status** privilege, otherwise you cannot see and use the Update Manager Web Client in vSphere Web Client.

The Update Manager Web Client plug-in is automatically enabled in the vSphere Web Client after you install the Update Manager server.

The Update Manager Web Client plug-in appears as an **Update Manager** tab under the **Monitor** tab in vSphere Web Client.

Upgrading Update Manager

You can upgrade to Update Manager 5.5 from Update Manager version 4.x, Update Manager 5.0 and Update Manager 5.1 that are installed on a 64-bit operating system. Direct upgrades from Update Manager 1.0 Update 6 and earlier, and Update Manager systems that are installed on a 32-bit platform are not supported.

If you are running an earlier version of Update Manager on a 32-bit platform, you cannot perform an in-place upgrade to Update Manager 5.5. You must use the data migration tool that is provided with Update Manager 5.0 installation media to move your Update Manager system from 32-bit operating system to Update Manager 5.0 on a 64-bit operating system, and then perform an in-place upgrade from version 5.0 to version 5.5. For detailed information how to use the data migration tool, see the *Installing and Administering VMware vSphere Update Manager* documentation for Update Manager 5.0.

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.

Previous versions of Update Manager use a 512-bit key and self-signed certificate and these are not replaced during upgrade. If you require a more secure 2048-bit key, you can either perform a fresh installation of Update Manager 5.5, or use the Update Manager Utility to replace the existing certificate.

Scheduled tasks for virtual machine patch scan and remediation are not removed during the upgrade. After the upgrade, you can edit and remove scheduled scan tasks that exist from previous releases. You can remove existing scheduled remediation tasks but you cannot edit them.

Virtual machine patch baselines are removed during the upgrade. Existing scheduled tasks that contain them run normally and ignore only the scanning and remediation operations that use virtual machine patch baselines.

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.

The Java Components (JRE) required by Update Manager are installed or upgraded silently on the system when you install or upgrade Update Manager. Starting with Update Manager 5.5 update 1, you can upgrade the Java Components separately to a version that is released asynchronously from Update Manager releases.

This chapter includes the following topics:

- [“Upgrade the Update Manager Server,”](#) on page 42
- [“Upgrade the Update Manager Client Plug-In,”](#) on page 43
- [“Upgrade the Update Manager Java Components,”](#) on page 43

Upgrade the Update Manager Server

To upgrade an instance of Update Manager that is installed on a 64-bit machine, you must first upgrade vCenter Server to a compatible version.

The Update Manager 5.5 release allows upgrades from Update Manager 1.0 Update 6, Update Manager 4.x, Update Manager 5.0, and Update Manager 5.1.

Prerequisites

- Grant the database user the required set of privileges. For more information, see [Chapter 3, “Preparing the Update Manager Database,”](#) on page 29.
- 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 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.

If prompted, you must restart the machine that is running vCenter Server. Otherwise, you might not be able to upgrade Update Manager.

- 2 In the software installer directory, double-click the `autorun.exe` file at `C:\installer_location`, and select **vSphere Update Manager**.

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

- 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 Review the support information, select whether to delete old upgrade files, select whether to download updates from the default download sources immediately after installation, and click **Next**.

If you deselect **Delete the old host upgrade files from the repository**, you retain files that you cannot use with Update Manager 5.5.

If you deselect **Download updates from default sources immediately after installation**, Update Manager downloads updates once daily according to the default download schedule or immediately after you click **Download Now** on the Download Settings page. You can modify the default download schedule after the installation is complete.

- 9 Type 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.

- 10 Type 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.

- 11 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 (Optional) On the Database re-initialization warning page, select to keep your existing remote database if it is already upgraded to the latest schema.
If you replace your existing database with an empty one, you lose all of your existing data.
- 13 Specify 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.
- 14 (Optional) Provide information about the proxy server and port, specify whether the proxy should be authenticated, and click **Next**.
- 15 Click **Install** to begin the upgrade.
- 16 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

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 Plug-in Manager window, click **Download and install** for the VMware vSphere Update Manager extension.
- 4 Complete the Update Manager Client installation, and click **Finish**.
The status for the Update Manager extension is displayed as Enabled.
- 5 Click **Close** to close the Plug-in Manager window.

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

Upgrade the Update Manager Java Components

The required Update Manager Java Components (JRE) are installed or upgraded silently when you install or upgrade Update Manager. By using a vCenter Server Java components patch, you can also upgrade Update Manager Java Components separately from Update Manager installer.

By using the separate installer, you can upgrade JRE to a version that is released asynchronously from Update Manager releases. If an earlier version of JRE is present on the system, this procedure upgrades it.

When Update Manager runs on the same system as the vCenter Server, if an earlier version of vCenter Server tc Server is present on that system, this procedure also upgrades the vCenter Server tc Server component.

During the patch process, the Update Manager undergoes a downtime as the vCenter Server Java Components patch restarts the Update Manager service.

Prerequisites

- Download the vCenter Server Java Components patch from VMware downloads page at <https://my.vmware.com/web/vmware/downloads>. The name format is `VMware-VIMPatch-5.5.0-build_number-YYYYMMDD.iso`
- Stop any running Update Manager operations, such as scanning, staging, or remediation.

Procedure

- 1 On the system where Update Manager is installed, mount the ISO of the vCenter Server Java Components patch.
- 2 In Windows Explorer, double-click the file `ISO_mount_directory/autorun.exe`.

A vCenter Server Java Components Update wizard opens.

- 3 Click **Patch All**.

If the Java components on the Update Manager system are up to date, a status message that confirms that is displayed.

If the Java components on the Update Manager system are not up to date, they are silently upgraded.

When clicking the **Patch All** button, if vCenter Server, vCenter Single Sign-On, vCenter Inventory Service or vSphere Web Client are also installed on the system where Update Manager is installed, the Java components for all of these are also silently upgraded.

The Java components are upgraded on the Update Manager system.

Best Practices and Recommendations for Update Manager Environment

6

You can install Update Manager on the server on which vCenter server runs or on a different server.

The Update Manager server and client plug-ins must be the same version. Update Manager, vCenter Server, and the vSphere Client must be of a compatible version. For more information about compatibility, see [“Update Manager Compatibility with vCenter Server, vSphere Client and vSphere Web Client,”](#) on page 26.

Update Manager has two deployment models:

Internet-connected model

The Update Manager server is connected to the VMware patch repository, and third-party patch repositories (for ESX/ESXi 4.x, ESXi 5.x hosts, as well as for virtual appliances). Update Manager works with vCenter Server to scan and remediate the virtual machines, appliances, hosts, and templates.

Air-gap model

Update Manager has no connection to the Internet and cannot download patch metadata. In this model, you can use UMDS to download and store patch metadata and patch binaries in a shared repository. To scan and remediate inventory objects, you must configure the Update Manager server to use a shared repository of UMDS data as a patch datastore. For more information about using UMDS, see [Chapter 8, “Installing, Setting Up, and Using Update Manager Download Service,”](#) on page 51.

Outside of DRS clusters, you might not be able to remediate the host running the Update Manager or vCenter Server virtual machines by using the same vCenter Server instance, because the virtual machines cannot be suspended or shut down during remediation. You can remediate such a host by using separate vCenter Server and Update Manager instances on another host. Inside DRS clusters, if you start a remediation task on the host running the vCenter Server or Update Manager virtual machines, DRS attempts to migrate the virtual machines 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 also fails if you have selected the option to power off or suspend the virtual machines before remediation.

This chapter includes the following topics:

- [“Update Manager Deployment Models,”](#) on page 45
- [“Update Manager Deployment Models and Their Usage,”](#) on page 47

Update Manager Deployment Models

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

Update Manager deployment configurations might vary depending on your environment.

Table 6-1. 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.

You can use one of several common host-deployment models for Update Manager server:

All-in-one model	vCenter Server and Update Manager server are installed on one host and their database instances are on the same host. This model is most reliable when your system is relatively small.
Medium deployment model	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.
Large deployment model	vCenter Server and Update Manager server run on different hosts, each with its dedicated database server. This model is recommended for large deployments when the datacenters contain more than 1,000 virtual machines or 100 hosts.

For best practices and recommendations, see *VMware vSphere Update Manager Performance and Best Practices*.

Uninstalling Update Manager

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

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

The Update Manager Web Client is automatically removed from the vSphere Web Client, after you uninstall the Update Manager server.

This chapter includes the following topics:

- [“Uninstall the Update Manager Server,”](#) on page 49
- [“Uninstall the Update Manager Client Plug-In,”](#) on page 49

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 vSphere 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.

The Update Manager Web Client is automatically removed from the vSphere Web Client.

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.

Prerequisites

Check if you have McAfee software installed on the system the Update Manager plug-in runs on. In case McAfee software runs in the same system as Update Manager, you cannot uninstall the Update Manager plug-in. To successfully uninstall the Update Manager plug-in, first disable all McAfee services, then uninstall the Update Manager plug-in and enable the McAfee services again.

Procedure

- 1 From the Windows **Start** menu, select **Settings > Control Panel > Add or Remove Programs**.
- 2 Select **VMware vSphere Update Manager Client 5.5** 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

8

VMware vSphere Update Manager Download Service (UMDS) is an optional module of Update Manager. UMDS downloads upgrades for virtual appliances, 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 a secured network that is disconnected from other local networks and the Internet. Update Manager requires access to patch information to function properly. In such an environment, you can install UMDS on a computer that has Internet access to download upgrades, 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 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 5.5 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 and Viewing Notifications,”](#) on page 68.

This chapter includes the following topics:

- [“Installing UMDS,”](#) on page 51
- [“Setting Up and Using UMDS,”](#) on page 53

Installing UMDS

You can install and use UMDS to download virtual appliance upgrades, 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.

NOTE You cannot upgrade UMDS 4.x to UMDS 5.5, but under certain conditions you can perform a fresh installation of UMDS 5.5 and use an existing patch store from UMDS 4.x. You can install UMDS only on 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 2008 R2 Express, you can install and configure the database when you install UMDS.

Installing UMDS 5.5 in an Environment with Update Manager 5.5 Instances Only

In the UMDS 5.5 installation wizard, you can select the patch store to be an existing download directory from an earlier UMDS 4.x installation and reuse the applicable downloaded updates in UMDS 5.5. You should uninstall existing UMDS 4.x instances before reusing the patch store. Once you associate an existing download directory with UMDS 5.5, you cannot use it with earlier UMDS versions.

If you install UMDS with an existing download directory, make sure that you perform at least one download by using UMDS 5.5 before you export updates.

Installing UMDS 5.5 in an Environment with both Update Manager 4.x and Update Manager 5.x Instances

You should not install UMDS 5.5 with an existing UMDS 4.x download directory if your environment contains both Update Manager 4.x and Update Manager 5.x instances. In such a case, you need a UMDS 4.x and a UMDS 5.x installation on two separate machines, in order to export updates for the respective Update Manager versions.

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.

Because Update Manager 5.x does not support guest operating system patching and vCenter Server 5.5 does not support ESX/ESXi 3.5 host operations, UMDS 5.5 does not download patches for guest operating systems and ESX/ESXi 3.5 hosts. UMDS 5.5 is compatible and can work with Update Manager 5.0, Update Manager 5.1, Update Manager 5.5 and their respective update releases.

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 upgrades, patch metadata and patch binaries.
- Uninstall UMDS 1.0.x or UMDS 4.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.
- To ensure optimal performance, install UMDS on a system with requirements same as the ones for the Update Manager server listed in [Chapter 2, “System Requirements,”](#) on page 25.

Procedure

- 1 Insert the VMware vSphere 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 (Optional) If the wizard prompts you, install the required items such as Windows Installer 4.5.

This step is required only if Windows Installer 4.5 is not present on your machine and you must perform it the first time you install a vSphere 5.x product. After the system restarts, the installer launches again.

- 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 Select the database options and click **Next**.
 - If you do not have an existing database, select **Install a Microsoft SQL Server 2008 R2 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**.
- 9 Enter the Update Manager Download Service proxy settings and click **Next**.
- 10 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. You can select the patch store to be an existing download directory from a previous UMDS 4.x installation and reuse the applicable downloaded updates in UMDS 5.5. After you associate an existing download directory with UMDS 5.5, you cannot use it with earlier UMDS versions.
- 11 (Optional) In the warning message about the disk free space, click **OK**.
- 12 Click **Install** to begin the installation.
- 13 Click **OK** in the Warning message notifying you that .NET Framework 3.5 SP1 is not installed.

The UMDS installer installs the prerequisite before the actual product installation.
- 14 Click **Finish**.

UMDS is installed.

Setting Up and Using UMDS

You can set up UMDS to download upgrades for virtual appliances, or patches and notifications for ESX/ESXi hosts. You can also set up UMDS to download ESX/ESXi 4.x and ESXi 5.x patch binaries, patch metadata, and notifications from third-party portals.

After you download the upgrades, 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.

You can also set up UMDS to download ESX/ESXi 4.x and ESXi 5.x 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 data you want, you can copy it 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 upgrades and patches automatically.

Set Up the Data 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 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 and all virtual appliance upgrades, run the following command:

```
vmware-umds -S --enable-host --enable-va
```

- To set up a download of all ESX/ESXi host updates and disable the download of virtual appliance upgrades, run the following command:

```
vmware-umds -S --enable-host --disable-va
```

- To set up a download of all virtual appliance upgrades and disable the download of host updates, run the following command:

```
vmware-umds -S --disable-host --enable-va
```

- To set up a download of only ESX 4.0 and ESXi 4.0 host updates, run the following commands:

```
vmware-umds -S --disable-host
vmware-umds -S -e esx-4.0.0 embeddedEsx-4.0.0
```

- To set up a download of all ESXi 5.x updates, and to disable downloading of only ESX 4.0 and ESXi 4.0 host updates, run the following commands:

```
vmware-umds -S --enable-host
vmware-umds -S -d esx-4.0.0 embeddedEsx-4.0.0
```

What to do next

Download the selected data.

Change the UMDS Patch Repository Location

UMDS downloads upgrades, 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 data after you install UMDS.

If you have already downloaded any virtual appliances upgrades, or host updates, 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 64-bit Windows is C:\Program Files (x86)\VMware\Infrastructure\Update Manager.

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

```
vmware-umds -S --patch-store your_new_patchstore_folder
```

In this example, *your_new_patchstore_folder* is the path to the new folder in 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 data using UMDS.

Configure URL Addresses for Hosts and Virtual Appliances

You can configure UMDS to connect to the Web sites of third-party vendors to download ESX/ESXi 4.x and ESXi 5.x host patches and notifications. You can also configure the URL addresses from which UMDS downloads virtual appliance upgrades.

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 64-bit Windows is C:\Program Files (x86)\VMware\Infrastructure\Update Manager.

- 3 Configure UMDS to download data from the new URL address.

- To add a new URL address for downloading patches and notifications for ESX/ESXi 4.x or ESXi 5.x hosts, run the following command:

```
vmware-umds -S --add-url https://host_URL/index.xml --url-type HOST
```

- To add a URL address for downloading virtual appliance upgrades, run the following command:

```
vmware-umds -S --add-url https://virtual_appliance_URL/index.xml --url-type VA
```

- 4 (Optional) Remove a URL address, so that UMDS will not download data from it anymore.

Downloaded data is retained and can be exported.

```
vmware-umds.exe -S --remove-url https://URL_to_remove/index.xml
```

UMDS is configured to download host patches and notifications, as well as virtual appliance upgrades from specific URL addresses.

What to do next

Download the patches and notifications using UMDS.

Download the Specified Data Using UMDS

After you set up UMDS, you can download upgrades, 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 64-bit Windows is C:\Program Files (x86)\VMware\Infrastructure\Update Manager.

- 3 Download the selected updates.

vmware-umds -D

This command downloads all the upgrades, 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 upgrades, patches, and notifications and want to download them again, you can include the start and end times to restrict the data 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 upgrades, patches and notifications that were downloaded in November 2010, for example, run the following command:

vmware-umds -R --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59

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

What to do next

Export the downloaded upgrades, patches, and notifications.

Export the Downloaded Data

You can export downloaded upgrades, 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.

Prerequisites

If you installed UMDS with an existing download directory, make sure that you perform at least one download by using UMDS 5.5 before you export updates.

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 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 deployment in which the Update Manager server is installed on a machine connected to the machine on which UMDS is installed, *repository_path* can be the path to the folder on the Web server that serves as a shared repository.

If the Update Manager server is installed on a machine in an isolated and secure environment, *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 ESX/ESXi patches that you downloaded during a specified time window.

For example, to export the patches downloaded in November 2010, run the following command:

```
vmware-umds -E --export-store repository-path --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
```

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 Download Source,”](#) on page 64.

Configuring Update Manager

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 *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

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,”](#) on page 60
- [“Change the Update Manager Network Settings,”](#) on page 61
- [“Configuring the Update Manager Download Sources,”](#) on page 62
- [“Configure the Update Manager Proxy Settings,”](#) on page 66
- [“Configure Checking for Updates,”](#) on page 67
- [“Configuring and Viewing Notifications,”](#) on page 68
- [“Take Snapshots Before Remediation,”](#) on page 70
- [“Configuring Host and Cluster Settings,”](#) on page 71
- [“Configure Smart Rebooting,”](#) on page 75
- [“Configure the Update Manager Patch Repository Location,”](#) on page 75
- [“Configure Mail Sender Settings,”](#) on page 76
- [“Restart the Update Manager Service,”](#) on page 76
- [“Run the VMware vSphere Update Manager Update Download Task,”](#) on page 76
- [“Update Manager Privileges,”](#) on page 77

Update Manager Network Connectivity Settings

The port, IP, and DNS settings are configured during the installation of Update Manager and do not depend on your deployment model.

Default Network Ports

The network port settings are configured during installation but you can change them later to avoid conflicts with other programs installed on the same machine.

Table 9-1. Update Manager Default Network Ports

TCP Port Number	Description
80	The port used by Update Manager to connect to vCenter Server.
9084	The port used by ESX/ESXi hosts to access host patch downloads over HTTP.
902	The port used by Update Manager to push host upgrade files.
8084	The port used by Update Manager client plug-in to connect to the Update Manager SOAP server.
9087	The HTTPS port used by Update Manager Client plug-in to upload host upgrade files.

IP Address and DNS Name

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 address 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 To avoid any potential DNS resolution problems, use an IP address whenever possible. 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 as well as by vCenter Server.

Update Manager supports Internet Protocol version 6 (IPv6) environments for scanning and remediating hosts running ESX/ESXi 4.0 and later. Update Manager does not support IPv6 for scanning and remediation of virtual machines and virtual appliances.

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. To be able to scan and remediate ESX 3.x hosts, you should install Update Manager on a computer with IPv4 enabled.

vCenter Server, Update Manager, and your ESX/ESXi hosts might exist in a heterogeneous IPv6 and IPv4 network environment. In such an environment, if you use IP addresses, and no dual stack IPv4 or IPv6 DNS servers exist, 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 only by 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.

Table 9-2. Update Manager Configuration

Host IP Version	Action
IPv4	Configure Update Manager to use either an IPv4 address or a host name. Using a host name lets all hosts rely on the DNS server to resolve to an IPv4 address.
IPv6	Configure Update Manager to use either an IPv6 address or a host name. Using a host name lets hosts rely on the DNS server to resolve to an IPv6 address.
IPv4 and IPv6	Configure Update Manager to use either IPv4 or IPv6.

Change the Update Manager Network Settings

The network ports are configured during installation. You can modify the IP address or host name for the patch store in the Update Manager network connectivity settings.

Prerequisites

- 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 requires outbound ports 80 and 443.

Procedure

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

You can see information about the network connectivity settings.

Option	Description
SOAP port	Update Manager Client uses this port to communicate with the Update Manager server.
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.
IP address or host name for the patch store	The IP address or name of the host in which patches are downloaded and stored.

- 2 Edit the IP address or host name for the patch store.
- 3 Click **Apply**.

What to do next

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

Configuring the Update Manager Download Sources

You can configure the Update Manager server to download patches and extensions for ESX/ESXi hosts or upgrades for virtual appliances either from the Internet or from a shared repository of UMDS data. You can also import patches and extensions for ESX/ESXi hosts manually from a ZIP file.

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

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 upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see [Chapter 8, “Installing, Setting Up, and Using Update Manager Download Service,”](#) on page 51.

Changing the 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 updates from the Internet and a shared repository at the same time. To download new data, you must run the VMware vSphere Update Manager Download task. You can start the task by clicking the **Download Now** button at the bottom of the Download Sources pane.

If the VMware vSphere 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, you can import both VMware and third-party patches or extensions manually from a ZIP file, also called an offline bundle. Import of offline bundles is supported only for hosts that are running ESX/ESXi 4.0 and later. You download the offline bundle ZIP files from the Internet or copy them from a media drive, and save them on a local or a shared network drive. You can import the patches or extensions to the Update Manager patch repository later. You can download offline bundles from the VMware Web site or from the Web sites of third-party vendors.

NOTE You can use offline bundles for host patching operations only. You cannot use third-party offline bundles or offline bundles that you generated from custom VIB sets for host upgrade from ESX/ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5.

Offline bundles contain one `metadata.zip` file, one or more VIB files, and optionally two `.xml` files, `index.xml` and `vendor-index.xml`. 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` file, the VIBs, and the `.xml` files, if available, into the Update Manager patch repository.

- [Configure Update Manager to Use the Internet as a Download Source](#) on page 63
If your deployment system is connected to the Internet, you can directly download ESX/ESXi patches and extensions, as well as virtual appliance upgrades.
- [Add a New Download Source](#) on page 64
If you use the Internet as a download source for updates, you can add a third-party URL address to download virtual appliance upgrades, as well as patches and extensions for hosts that are running ESX/ESXi 4.0 and later.
- [Use a Shared Repository as a Download Source](#) on page 64
You can configure Update Manager to use a shared repository as a source for downloading virtual appliance upgrades, as well as ESX/ESXi patches, extensions, and notifications.
- [Import Patches Manually](#) on page 66
Instead of using a shared repository or the Internet as a download source for patches and extensions, you can import patches and extensions manually by using an offline bundle.

Configure Update Manager to Use the Internet as a Download Source

If your deployment system is connected to the Internet, you can directly download ESX/ESXi patches and extensions, as well as virtual appliance upgrades.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Settings**.
- 2 In the Download Sources pane, select **Direct connection to Internet**.
- 3 Choose the type of updates to download by selecting or deselecting the check box next to the type of update.

You can choose whether to download virtual appliance upgrades and host patches and extensions. You cannot edit the download source location of the default ESX/ESXi patches and extensions. You can only enable or disable downloading.
- 4 (Optional) Add an additional third-party download source for virtual appliances or hosts that are running ESX/ESXi 4.0 and later.
- 5 Click **Apply**.
- 6 Click **Download Now** to run the VMware vSphere Update Manager Update Download task.

All notifications and updates are downloaded immediately even if the **Enable scheduled download** checkbox is not selected in **Configuration > Notification Check Schedule** or **Configuration > Download Schedule**, respectively.

Add a New Download Source

If you use the Internet as a download source for updates, you can add a third-party URL address to download virtual appliance upgrades, as well as patches and extensions for hosts that are running ESX/ESXi 4.0 and later.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Settings**.
- 2 In the Download Sources pane, select **Direct connection to Internet**.
- 3 Click **Add Download Source**.
- 4 In the Add Download Source window, type the new download source URL.

Update Manager supports both HTTP and HTTPS URL addresses. You should specify HTTPS URL addresses, so that the data is downloaded securely. The URL addresses that you add 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 URL addresses too. You can configure the proxy settings from the Proxy Settings pane.

- 5 (Optional) Type 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 vSphere Update Manager Update Download task.

All notifications and updates are downloaded immediately even if the **Enable scheduled download** checkbox is not selected in **Configuration > Notification Check Schedule** or **Configuration > Download Schedule**, respectively.

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

Use a Shared Repository as a Download Source

You can configure Update Manager to use a shared repository as a source for downloading virtual appliance upgrades, as well as ESX/ESXi patches, extensions, and notifications.

Prerequisites

You must create the shared repository using UMDS and host it on a Web server or a local disk. The UMDS version you use must be of a version compatible with your Update Manager installation.

For more information about the compatibility, see [“Compatibility Between UMDS and the Update Manager Server,”](#) on page 52. You can find the detailed procedure about exporting the upgrades, patch binaries, patch metadata, and notifications in [“Export the Downloaded Data,”](#) on page 56.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Settings**.
- 2 In the 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 downloaded upgrades, patches, extensions, and notifications. In an 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 specify 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 updates 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 updates 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.

You must 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 vSphere Update Manager Update Download task and to download the updates immediately.

The shared repository is used as a source for downloading upgrades, 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 on 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 download source for patches and extensions, 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 *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Settings**.
- 2 Click **Import Patches** at the bottom of the Download Sources pane.
- 3 On the Select Patches File 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.

After a successful upload, the Confirm Import page appears.

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 On the Confirm Import page of the Import Patches wizard, review the patches that you have selected to import into the Update Manager repository.
- 6 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 the Update Manager Proxy Settings

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

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Settings**.

- 2 In the Proxy Settings pane, select **Use proxy** and change the proxy information.
- 3 (Optional) If the proxy requires authentication, select **Proxy requires authentication** and provide a user name and password.
- 4 (Optional) Click **Test Connection** at any time to test that you can connect to the Internet through the proxy.
- 5 Click **Apply**.

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

Configure Checking for Updates

Update Manager checks for virtual appliance upgrades, host patches, and extensions 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.

In some cases you might want to decrease the duration between checks for updates. If you are not concerned about the latest updates and want to reduce network traffic, or if you cannot access the update servers, you can increase the duration between checks for updates.

By default the task to download update metadata and binaries is enabled and is called VMware vSphere Update Manager Update Download task. By modifying this task, you can configure checking for updates. You can modify the VMware vSphere 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 update 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 **Download Schedule**.
- 2 Make sure that the **Enable scheduled download** check box is selected.

NOTE If you deselect the check box, the scheduled task that checks for updates is disabled. However, you can still force a check and download updates by clicking **Download Now** in **Download Settings** on the **Configuration** tab.

- 3 Click **Edit Download Schedule** 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 update download, and click **Next**.
- 6 (Optional) Specify one or more email addresses to be notified when the new updates are downloaded, and click **Next**.

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

- 7 On the Ready to Complete page, click **Finish**.

The task runs according to the time you specified.

Configuring and Viewing Notifications

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

In case patches with issues or potential issues are released, the patch metadata is updated, and Update Manager marks the patches 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. Update Manager notifies you if a recalled patch is already installed on certain hosts. Update Manager also deletes all the recalled patches from the patch repository.

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

Update Manager supports patch recalls for offline bundles that you have imported. Patches from an imported offline bundle are recalled 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 fixes, Update Manager notifies you about the fixes and sends email notifications if you have enabled them.

If you use a shared repository as a source for downloading patches and notifications, Update Manager downloads recall notifications from the shared repository to the Update Manager patch repository, but does not send recall email alerts. For more information about using a shared repository, see [“Use a Shared Repository as a Download Source,”](#) on page 64.

Note After a download of patch recall notifications, Update Manager flags recalled patches but their compliance state does not refresh automatically. You must perform a scan to view the updated compliance state of patches affected by the recall.

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 vSphere Update Manager Check Notification task. By modifying this task, you can configure the time and frequency at which 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 vSphere 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 **Enable scheduled download** check box is selected.

NOTE If you deselect the check box, the scheduled task that checks for notifications is disabled. However, you can still force a check and download notifications by clicking the **Check Notifications** link on the **Notifications** tab or the **Download Now** button in **Download Settings** on the **Configuration** tab.

- 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 On the Ready to Complete page, 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 on the Home page, click **Update Manager** under Solutions and Applications. 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.

Any new notifications that are available on the VMware Web site are immediately downloaded even if the **Enable scheduled download** checkbox is not selected in **Configuration > Notification Check Schedule**.

Types of Update Manager Notifications

Update Manager downloads all notifications that are available on the VMware Web site. Some notifications can trigger an alarm. By using the Alarm Settings wizard, you can specify automated actions to be taken when an alarm is triggered.

Information notifications	Information notifications appear in the Update Manager Notifications tab. They do not trigger an alarm. Clicking an information notification opens the Notification Details window.
Warning notifications	Warning notifications appear in the Update Manager Notifications tab and trigger an alarm, which appears in the vSphere Client Alarms tab. Warning notifications are typically fixes for patch recalls. Clicking a warning notification opens the Patch Recall Details window.
Alert notifications	Alert notifications appear in the Update Manager Notifications tab and trigger an alarm, which appears in the vSphere Client Alarms tab. Alert notifications are typically patch recalls. Clicking an alert notification opens the Patch Recall Details window.

Take Snapshots Before Remediation

By default, Update Manager is configured to take snapshots of virtual machines before applying updates. If the remediation fails, you can use the snapshot to return the virtual machine to the state before the remediation.

Update Manager does not take snapshots of fault tolerant virtual machines and virtual machines that are running virtual machine hardware version 3. If you decide to take snapshots of such virtual machines, the remediation might fail.

You can choose to keep 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 **Take a snapshot of 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 can choose to 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.

Updates might require that the host enters maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, vCenter Server can migrate 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. Use of EVC prevents migrations with vMotion from failing because of incompatible CPUs. EVC can only be enabled in a cluster where host CPUs meet the compatibility requirements. For more information about EVC and the requirements that the hosts in an EVC cluster must meet, see *vCenter Server and Host Management*.

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 and staging complete successfully, Update Manager disables VMware DPM during these operations. To ensure successful remediation, you should allow Update Manager to disable VMware DPM and HA admission control before the remediation operation. After the operation completes, Update Manager restores VMware DPM and HA admission control. Update Manager disables HA admission control before staging and remediation but not before scanning.

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 VMware 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 or power on the hosts.

Within a cluster, you should select to temporarily disable HA admission control to allow vMotion to proceed, in order to prevent 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 select to 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.

There are some specifics about remediating hosts that are part of a Virtual SAN cluster:

- The host remediation process might take extensive amount of time to complete.
- By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time.
- Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.

- If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

Configure Host Maintenance Mode Settings

ESX/ESXi host updates 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 updates. You can configure how Update Manager responds if the host fails to enter 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.

Hosts that are part of a Virtual SAN cluster can enter maintenance mode only one at a time. This is specificity of the Virtual SAN clusters.

If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **VM Power state** drop-down menu to determine the change of the power state of the virtual machines and appliances that are running on the host to be remediated.

Option	Description
Power Off virtual machines	Powers off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspends all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leaves virtual machines and virtual appliances in their current power state. This is the default setting.

- 3 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the retry delay, and the number of retries.

If a host fails to enter maintenance mode before remediation, Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

- 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 have 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.

After remediation, Update Manager reconnects the removable media devices if they are still available.

- 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 can run either in a sequence or in parallel. 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.

NOTE Remediating hosts in parallel can improve performance significantly by reducing the time required for cluster remediation. Update Manager remediates hosts in parallel without disrupting the cluster resource constraints set by DRS. Avoid remediating hosts in parallel if the hosts are part of a Virtual SAN cluster. Due to the specifics of the Virtual SAN cluster, a host cannot enter maintenance mode while other hosts in the cluster are currently in maintenance mode.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 for features that you want to disable or enable.

Option	Description
Distributed Power Management (DPM)	<p>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.</p> <p>If you do not choose to disable DPM, Update Manager skips the cluster on which VMware DPM is enabled. If you choose to temporarily disable VMware DPM, Update Manager disables DPM on the cluster, remediates the hosts in the cluster, and re-enables VMware DPM after remediation is complete.</p>
High Availability (HA) admission control	<p>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.</p> <p>If you do not choose to disable HA admission control, Update Manager skips the cluster on which HA admission control is enabled. If you choose 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.</p>

Option	Description
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 you do not choose to turn off FT for the virtual machines on a host, Update Manager does not remediate that host.
Enable parallel remediation for hosts in cluster	Update Manager can remediate hosts in clusters in a parallel manner. Update Manager continuously evaluates the maximum number of hosts it can remediate in parallel without disrupting DRS settings. If you do not select the option, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can select to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

- 3 Click **Apply**.

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

Enable Remediation of PXE Booted ESXi 5.x Hosts

You can configure Update Manager to let other software initiate remediation of PXE booted ESXi 5.x hosts. The remediation installs patches and software modules on the hosts, but typically the host updates are lost after a reboot.

The global setting in the Update Manager **Configuration** tab enables solutions such as ESX Agent Manager or Cisco Nexus 1000V to initiate remediation of PXE booted ESXi 5.x hosts. In contrast, the **Enable patch remediation of powered on PXE booted ESXi hosts** setting in the Remediate wizard enables Update Manager to patch PXE booted hosts.

To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with Update Manager, so that the updates are not lost because of a reboot. Update Manager itself does not reboot the hosts because it does not install updates requiring a reboot on PXE booted ESXi 5.x hosts.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 To enable installation of software for solutions on PXE booted ESXi 5.x hosts, select **Allow installation of additional software on PXE booted ESXi 5.x hosts**.
- 3 Click **Apply**.

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 on the Home page, click **Update Manager** under Solutions and Applications. 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 the 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 the 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 vSphere 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 vSphere Update Manager Service** in the Computer Management window and selecting **Start**.

Configure Mail Sender Settings

You must configure the email sender account to enable vCenter Server to send 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 view the vCenter Server Settings dialog box.
- 3 In the navigation pane, select **Mail**.
- 4 Specify 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 vSphere Update Manager Service** and select **Restart**.

The service restarts on the local computer.

Run the VMware vSphere Update Manager Update Download Task

If you change the patch download source settings, you must run the VMware vSphere 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 vSphere 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 cover distinct functionalities.

Table 9-3. 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 upgrade images and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see *vSphere Security*.

Working with Baselines and Baseline Groups

10

Baselines can be upgrade, extension, or patch baselines. Baselines contain a collection of one or more patches, extensions, or upgrades.

Baseline groups are assembled from existing baselines, and might contain one upgrade baseline per type of upgrade baseline and one or more patch and extension baselines, or might contain 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 *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

Update Manager includes two default dynamic patch baselines and three upgrade baselines.

Critical Host Patches (Predefined)	Checks ESX/ESXi hosts for compliance with all critical patches.
Non-Critical Host Patches (Predefined)	Checks ESX/ESXi hosts for compliance with all optional patches.
VMware Tools Upgrade to Match Host (Predefined)	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 (Predefined)	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 vmx-10 on hosts that are running ESXi 5.5.
VA Upgrade to Latest (Predefined)	Checks virtual appliance compliance with the latest released 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 inventory objects 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,”](#) on page 80
- [“Creating and Managing Baseline Groups,”](#) on page 89
- [“Attach Baselines and Baseline Groups to Objects,”](#) on page 93
- [“Attach Baselines and Baseline Groups to Objects in Update Manager Web Client,”](#) on page 94
- [“Filter the Baselines and Baseline Groups Attached to an Object,”](#) on page 94
- [“Detach Baselines and Baseline Groups from Objects,”](#) on page 95
- [“Detach Baselines and Baseline Groups from Objects in Update Manager Web Client,”](#) on page 96

Creating and Managing Baselines

You can create custom patches, extensions, and upgrade baselines to meet the needs of your specific deployment by using the New Baseline wizard. You create and manage baselines in the Update Manager Client Administration view.

Create and Edit Patch or Extension Baselines

You can remediate hosts against baselines that contain patches or extensions. Depending on the patch criteria you select, patch baselines can be either dynamic or fixed.

Dynamic patch baselines contain a set of patches, which updates automatically according to patch availability and the criteria that you specify. Fixed baselines contain only patches that you select, regardless of new patch downloads.

Extension baselines contain additional software modules for ESX/ESXi hosts. This additional software might be VMware software or third-party software. You can install additional modules by using extension baselines, and update the installed modules by using patch baselines.

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 that 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

Ensure that you have the **Manage Baseline** privilege.

- [Create a Fixed Patch Baseline](#) on page 81
Fixed baselines consist of a specific set of patches that do not change as patch availability changes.
- [Create a Dynamic Patch Baseline](#) on page 81
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.
- [Create a Host Extension Baseline](#) on page 82
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.
- [Filter Patches or Extensions in the New Baseline Wizard](#) on page 83
When you create a patch or extension baseline, you can filter the patches and extensions available in the Update Manager repository to find specific patches and extensions to exclude or include in the baseline.

- [Edit a Patch Baseline](#) on page 84

You can edit an existing host patch baseline.

- [Edit a Host Extension Baseline](#) on page 84

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

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 on the Home page, click **Update Manager** under Solutions and Applications. 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.
- 2 Type a name, and optionally, a description of the baseline.
- 3 Under Baseline Type, select **Host Patch**, and click **Next**.
- 4 Select **Fixed** for the type of baseline and click **Next**.
- 5 Select individual patches to include and click the down arrow to add them to the Fixed Patches to Add list.
- 6 (Optional) Click **Advanced** to find specific patches to include in the baseline.
- 7 Click **Next**.
- 8 On the Ready to Complete page, click **Finish**.

The new 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 on the Home page, click **Update Manager** under Solutions and Applications. 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.
- 2 Type a name, and optionally, a description of the baseline.
- 3 Under Baseline Type select **Host Patch**, and click **Next**.
- 4 Select **Dynamic** as the type of baseline, and click **Next**.

- 5 On the Dynamic Baseline Criteria page, specify 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.
Category	Specifies the category of patches to include.
Release 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 ones that are applicable for the selected product and are of the specified severity level.

- 6 (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.
- 7 (Optional) Click **Advanced** to search for specific patches to exclude from the baseline.
- 8 Click **Next**.
- 9 (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.
- 10 (Optional) Click **Advanced** to search for specific patches to include in the baseline.
- 11 Click **Next**.
- 12 On the Ready to Complete page, click **Finish**.

The new 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.

NOTE 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 on the Home page, click **Update Manager** under Solutions and Applications. 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.
- 2 Type a name, and optionally, a description of the baseline.
- 3 Under Baseline Type, select **Host Extension** and click **Next**.
- 4 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.
- 5 (Optional) Click **Advanced** to filter the extensions to include specific extensions in the baseline.
- 6 Click **Next**.
- 7 On the Ready to Complete page, click **Finish**.

The new 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 available in the Update Manager repository 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, click **Advanced**.
 - If you are creating a dynamic patch baseline, on the Patches to Exclude or Additional Patches page, click **Advanced**.
 - If you are creating a host extension baseline, on the Extensions page, click **Advanced**.
- 2 On the Filter Patches or Filter Extensions page, specify 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.
Category	Specifies the category of patches or extensions to include.
Release 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 specified.

Edit a Patch Baseline

You can edit an existing host patch baseline.

You edit patch baselines from the Update Manager Client Administration view.

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Hosts**.
- 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, and select patches to include or exclude.
- 5 On the Ready to Complete page, click **Finish**.

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

Ensure that you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 On the Ready to Complete page, click **Finish**.

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 ESXi 5.5 images.

You can upload and manage ESXi images from the **ESXi Images** tab of the Update Manager Administration view.

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

Before uploading ESXi images, obtain the image files from the VMware Web site or another source. You can create custom ESXi images that contain third-party VIBs by using ESXi Image Builder CLI. For more information, see *Using vSphere ESXi Image Builder CLI*.

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 Images and Create Host Upgrade Baselines](#) on page 85
You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.5 images that you import to the Update Manager repository.
- [Create a Host Upgrade Baseline](#) on page 86
To upgrade or migrate the hosts in your vSphere environment, you must create host upgrade baselines.
- [Edit a Host Upgrade Baseline](#) on page 87
You can change the name, description, and upgrade options of an existing host upgrade baseline. You cannot delete a host upgrade image by editing the host upgrade baseline.
- [Delete ESXi Images](#) on page 87
You can delete ESXi images from the Update Manager repository if you no longer need them.

Import Host Upgrade Images and Create Host Upgrade Baselines

You can create upgrade baselines for ESX/ESXi hosts with ESXi 5.5 images that you import to the Update Manager repository.

You can use ESXi .iso images to upgrade ESXi 4.x, ESXi 5.0 and ESXi 5.1 hosts to ESXi 5.5 or migrate ESX 4.x hosts to ESXi 5.5.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.5.0-build_number.x86_64.iso` or a custom image created by using Image Builder.

Prerequisites

Ensure that you have the **Upload File** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **ESXi Images** tab click **Import ESXi Image** on the upper-right side.
- 2 On the Select ESXi Image page of the Import ESXi Image wizard, browse to and select the ESXi image that you want to upload.

- 3 Click **Next**.



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

- 4 (Optional) In the Security Warning window, select an option to handle the certificate 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	Action
Ignore	Click Ignore to continue using the current SSL certificate and start the upload process.
Cancel	Click Cancel to close the window and stop the upload process.
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 is uploaded, click **Next**.
- 6 (Optional) Create a host upgrade baseline.
 - a Leave the **Create a baseline using the ESXi image** selected.
 - b Specify a name, and optionally, a description for the host upgrade baseline.
- 7 Click **Finish**.

The ESXi image that you uploaded appears in the Imported ESXi Images pane. You can see more information about the software packages that are included in the ESXi image in the Software Packages pane.

If you also created a host upgrade baseline, the new baseline is displayed in the Baselines pane of the **Baselines and Groups** tab.

What to do next

To upgrade or migrate the hosts in your environment, you must create a host upgrade baseline if you have not already done so.

Create a Host Upgrade Baseline

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

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 ESXi image.

Procedure

- 1 On the **Baselines and Groups** tab, click **Create** above the Baselines pane.
- 2 Under Baseline Type, select **Host Upgrade** and click **Next**.
- 3 On the ESXi Image page, select a host upgrade image and click **Next**.
- 4 Review the Ready to Complete page and click **Finish**.

The new 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 a host upgrade image by editing the host upgrade baseline.

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

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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.
- 5 On the Ready to Complete page, click **Finish**.

Delete ESXi Images

You can delete ESXi images from the Update Manager repository if you no longer need them.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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

Verify that the ESXi images are not included in baselines. You cannot delete images that are included in a baseline.

Procedure

- 1 In the Update Manager Administration view, click the **ESXi Images** tab.
- 2 Under Imported ESXi Images, select the file you want to delete and click **Delete**.
- 3 Click **Yes** to confirm the deletion.

The ESXi image is deleted and no longer available under Imported ESXi Images.

Create and Edit a Virtual Appliance Upgrade Baseline

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

Virtual appliance baselines let you upgrade virtual appliances either to the latest available version or to a specific version number.

- [Create a Virtual Appliance Upgrade Baseline](#) on page 88

You upgrade virtual appliances by using a virtual appliance upgrade baseline. You can either use the predefined virtual appliance upgrade baseline, or create custom virtual appliance upgrade baselines.

- [Edit a Virtual Appliance Upgrade Baseline](#) on page 89

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

Create a Virtual Appliance Upgrade Baseline

You upgrade virtual appliances by using a virtual appliance upgrade baseline. You can either use the predefined virtual appliance upgrade baseline, or create custom virtual appliance upgrade baselines.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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.
- 2 Type a name, and optionally, a description of the baseline.
- 3 Under Baseline Type, select **VA Upgrade**, and click **Next**.
- 4 On the Upgrade Options page, select **Vendor** and **Appliance** options from the respective drop-down menus.

The options listed in these menus depend on the virtual appliance upgrades that are downloaded in the Update Manager repository. If no upgrades are downloaded in the repository, the available options are **All Vendors** and **All Products**, respectively.

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

Option	Description
Latest	Upgrades the virtual appliance to the latest version.
A specific version number	Upgrades the virtual appliance to a specific version. This option is available when you select a specific vendor and appliance name.
Do Not Upgrade	Does not upgrade the virtual appliance.

- 6 Click **Add Rule**.
- 7 (Optional) Add multiple rules.
 - a Click **Add Multiple Rules**.
 - b Select one or all vendors.
 - c Select one or all 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.

- 8 (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**.

- 9 Click **Next**.
- 10 On the Ready to Complete page, click **Finish**.

The new 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

Ensure that you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **VMs/VAs**.
- 2 Select an existing 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 On the Ready to Complete page, click **Finish**.

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 on the Home page, click **Update Manager** under Solutions and Applications. 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 perform an orchestrated upgrade of hosts by using a baseline group that contains a single host upgrade baseline and multiple patch or extension 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 a 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 a 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 a new Extension Baseline** at the bottom of the Patches page and complete the New Baseline wizard.
- 12 On the Ready to Complete page, 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 baselines in a virtual machine and virtual appliance 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 on the Home page, click **Update Manager** under Solutions and Applications. 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**.
- 3 Enter a name for the baseline group and click **Next**.
- 4 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 decide to remediate only virtual appliances, the upgrades for virtual machines are ignored, and the reverse. If a folder contains both virtual machines and virtual appliances, the appropriate upgrades are applied to each type of object.

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

After you complete the New Baseline wizard, you return to the New Baseline Group wizard.

- 6 Click **Next**.
- 7 On the Ready to Complete page, click **Finish**.

The new 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 (Optional) Change the included upgrade baselines (if any).
- 5 (Optional) Change the included patch baselines (if any).
- 6 (Optional) 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, extension, or upgrade baseline to an existing baseline group.

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

Prerequisites

Ensure that you have the **Manage Baseline** privilege.

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 **Hosts** or **VMs/VAs**, 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 included baselines.
- 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 individual baselines from existing baseline groups.

You can edit the contents of 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 on the Home page, click **Update Manager** under Solutions and Applications. 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 **Hosts** or **VMs/VAs**, 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 included baselines.
- 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 on the Home page, click **Update Manager** under Solutions and Applications. 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, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and datacenters. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

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 attach are specific for the Update Manager instance that is registered with the vCenter Server system.

Prerequisites

Ensure that you 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 complete the remaining steps in 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.

Attach Baselines and Baseline Groups to Objects in Update Manager Web Client

To view compliance information and remediate objects in the inventory against baselines and baseline groups, you must first attach existing baselines and baseline groups to these objects. You can attach baselines and baseline groups to object from the Update Manager Web Client in the vSphere Web Client.

You cannot create baselines and baseline groups from the Update Manager Web Client interface. To attach a different baseline or baseline group than the ones you see in the Attach Baseline or Group dialog of the Update Manager Web Client, you must first create them in Update Manager Client plug-in for the vSphere Client.

Prerequisites

- Verify that you have the **Attach Baseline** privilege.
- Verify that all the baselines or baseline groups that you want to use are already created. You can create baselines and baseline groups only from the Update Manager Client plug-in for the vSphere Client.

Procedure

- 1 Start the vSphere Web Client, and log in to the vCenter Server system.
- 2 Select an appropriate object in the vSphere Web Client object navigator.
- 3 Click the **Monitor** tab, and click **Update Manager**.
- 4 Click **Attach**, and select the types of baselines you want to attach.
 - a In the Individual Baselines pane, select one or more baselines to attach to the object.
 - b In the Baseline Groups pane, select one or more baseline groups to attach to the object.
- 5 Click **OK**.

What to do next

Scan the selected object against the attached baselines.

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 virtual machine, a virtual 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 Type 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

Ensure that you 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.

Detach Baselines and Baseline Groups from Objects in Update Manager Web Client

You can detach baselines and baseline groups from objects to which the baselines or baseline groups are 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.

Prerequisites

Ensure that you have the **Attach Baseline** privilege.

Procedure

- 1 Start the vSphere Web Client, and log in to the vCenter Server system.
- 2 Select an appropriate object in the vSphere Web Client object navigator.
- 3 Click the **Monitor** tab, and click **Update Manager**.
- 4 Remove a baseline or a baseline group that you no longer need.
 - a To remove a baseline, select the baseline and click **Detach** on the upper left corner of the Attached Baselines pane.
 - b To remove a baseline group, select the baseline group from the **Attached Baseline Groups** drop-down menu, and click **Detach** at the upper right corner of the **Attached Baseline Groups** drop-down menu.
- 5 In the Detach Baseline Group dialog box, select the entities that you want to detach the baseline or the baseline group from.
- 6 Click **OK**.

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

Scanning vSphere Objects and Viewing Scan Results

11

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

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

To initiate or schedule scans, you must have the **Scan for Applicable Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

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

This chapter includes the following topics:

- [“Manually Initiate a Scan of ESX/ESXi Hosts,”](#) on page 97
- [“Manually Initiate a Scan of ESX/ESXi Hosts in Update Manager Web Client,”](#) on page 98
- [“Manually Initiate a Scan of Virtual Machines and Virtual Appliances,”](#) on page 98
- [“Manually Initiate a Scan of Virtual Machines and Virtual Appliances in Update Manager Web Client,”](#) on page 99
- [“Manually Initiate a Scan of a Datacenter in Update Manager Web Client,”](#) on page 99
- [“Schedule a Scan,”](#) on page 100
- [“Viewing Scan Results and Compliance States for vSphere Objects,”](#) on page 100

Manually Initiate a Scan of ESX/ESXi Hosts

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. To run a scan of hosts in the vSphere inventory immediately, initiate a scan manually.

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**.
- 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 and all child objects are scanned against all patches, extensions, and upgrades in the attached baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

Manually Initiate a Scan of ESX/ESXi Hosts in Update Manager Web Client

Before remediation, you should scan the vSphere objects against the attached baselines and baseline groups. You can run a scan of hosts in the vSphere inventory immediately by initiating a scan from the Update Manager Web Client, and later perform staging and remediation from the Update Manager Client plug-in for the vSphere Client.

Procedure

- 1 Start the vSphere Web Client, and log in to the vCenter Server system.
- 2 In the vSphere Web Client object navigator, select an ESX/ESXi host, or a host folder.
- 3 Click the **Monitor** tab, and click **Update Manager**.
- 4 Click **Scan** and select the types of updates to scan for.

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

- 5 Click **OK**.

The selected host, or the container object is scanned against all patches, extensions, and upgrades in the attached baselines.

What to do next

Stage and remediate the scanned inventory object in Update Manager Client plug-in for the vSphere Client.

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**.
- 3 Select the types of updates to scan for.

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

- 4 Click **Scan**.

The virtual machines and appliances that you select are scanned against the attached baselines, depending on the options that you select. All child objects 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.

Manually Initiate a Scan of Virtual Machines and Virtual Appliances in Update Manager Web Client

You can scan virtual machines and virtual appliances in the vSphere inventory against attached baselines and baseline groups from the vSphere Web Client by using the Update Manager Web Client. You can later perform staging and remediation from the Update Manager Client plug-in for the vSphere Client.

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

Procedure

- 1 Start the vSphere Web Client, and log in to the vCenter Server system.
- 2 In the vSphere Web Client object navigator, select a virtual machine, virtual appliance, or a folder of virtual machines and appliances.
- 3 Click the **Monitor** tab, and click **Update Manager**.
- 4 Click **Scan** and select the types of updates to scan for.

You can scan for **Virtual appliance upgrades**, **VMware Tools upgrades**, and **VM Hardware upgrades**.

- 5 Click **OK**.

The virtual machines and appliances are scanned against the attached baselines, depending on the options that you selected.

What to do next

Stage and remediate the scanned inventory object in Update Manager Client plug-in for the vSphere Client.

Manually Initiate a Scan of a Datacenter in Update Manager Web Client

To start a simultaneous scan of hosts, virtual machines, and virtual appliances that are part of a datacenter or a datacenter folder from the vSphere inventory, you can initiate a scan against attached baselines and baseline groups from the Update Manager Web Client. If you are using vCenter Linked Mode, you can scan a vCenter instance.

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

Procedure

- 1 Start the vSphere Web Client, and log in to the vCenter Server system.
- 2 In the vSphere Web Client object navigator, select a datacenter or a datacenter folder.
- 3 Click the **Monitor** tab, and click **Update Manager**.
- 4 Click **Scan** and select the types of updates to scan for.

For the ESX/ESXi hosts in the datacenter, you can scan for **Patches and Extensions** and **Upgrades**.

For virtual machines and virtual appliances in the datacenter, you can scan for **Virtual appliance upgrades**, **VMware Tools upgrades**, and **VM Hardware upgrades**.

- 5 Click **OK**.

The selected inventory object and all child objects are scanned against the attached baselines, depending on the options that you selected. The larger the virtual infrastructure and the higher up in the object hierarchy you initiate the scan, the longer the scan takes.

What to do next

Stage and remediate the scanned inventory object in Update Manager Client plug-in for the vSphere Client.

Schedule a Scan

You can configure the vSphere Client to scan virtual machines, virtual appliances, and ESX/ESXi hosts 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**.
- 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:

- Objects must have an attached baseline or baseline group to be examined for compliance information.
- 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.

- 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 77. For more information about managing users, groups, roles and permissions, see *vCenter Server and Host Management*.

In the vSphere infrastructure hierarchy, 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 subfolders), 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 noncompliant 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 incompatible with B, the overall status of the folder is incompatible.

NOTE After a download of patch recall notifications, Update Manager flags recalled patches but their compliance state does not refresh automatically. You must perform a scan to view the updated compliance state of patches affected by the recall.

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 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 about the degree of compliance with attached baselines and baseline groups. You can view information about individual vSphere objects and about the patches, extensions, and upgrades included in a baseline or a baseline group.

The following information is included in the scan results:

- The last time that a scan was completed at this level.

- The total number of noncompliant, incompatible, unknown, and compliant updates.
- 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 updates that are applicable to particular virtual machines, appliances, or hosts.

Procedure

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

- 2 Select the type of object for which you want to view 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 a number link in the bottom pane of the Update Manager tab to see more details about updates.

Column	Description
Patches	The link indicates the number of patches in the selected compliance state and opens the Patch Details window.
Upgrades	The link indicates the number of upgrades in the selected compliance state and opens the Upgrade Details window.
Extensions	The link indicates the number of extensions in the selected compliance state and opens the Extension Details window.
Change log	The link is available only if the upgrade in the baseline is applicable to the selected virtual appliance. The link opens the Virtual Appliance Change Log Details window.

Compliance View

Information about the compliance states of selected vSphere inventory objects against baselines and baseline groups you attach is displayed in the Update Manager Client Compliance view.

The information is displayed in four panes.

Table 11-1. 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 11-1. Update Manager Tab Panes (Continued)

Pane	Description
Compliance	<p data-bbox="687 258 1422 384">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.</p> <p data-bbox="687 394 1422 443">If you select an individual host, virtual machine, or appliance, the color of the graph is solid and represents a single compliance state.</p> <p data-bbox="687 453 1299 474">Above the graph, the following compliance states are displayed:</p> <div data-bbox="687 499 1422 1409"> <div data-bbox="687 499 1422 831"> <p data-bbox="687 499 831 520">All Applicable</p> <p data-bbox="906 499 1422 632">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.</p> <p data-bbox="906 646 1422 831">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.</p> </div> <div data-bbox="687 852 1422 957"> <p data-bbox="687 852 844 873">Non-Compliant</p> <p data-bbox="906 852 1422 957">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 baselines or baseline groups.</p> </div> <div data-bbox="687 978 1422 1188"> <p data-bbox="687 978 823 999">Incompatible</p> <p data-bbox="906 978 1422 1188">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.</p> </div> <div data-bbox="687 1209 1422 1335"> <p data-bbox="687 1209 788 1230">Unknown</p> <p data-bbox="906 1209 1422 1335">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.</p> </div> <div data-bbox="687 1356 1422 1409"> <p data-bbox="687 1356 796 1377">Compliant</p> <p data-bbox="906 1356 1422 1409">Number of compliant virtual machines, appliances, or hosts in the selected container object.</p> </div> </div>
Bottom pane	<p data-bbox="687 1444 1422 1493">The information in this pane depends on whether you select an individual object or a container object.</p> <p data-bbox="687 1503 1422 1551">If you select a container object, the bottom pane of the Update Manager tab displays the following information:</p> <ul data-bbox="687 1562 1422 1698" style="list-style-type: none"> <li data-bbox="687 1562 1422 1635">■ A list of virtual machines, appliances, or hosts that meet the selections from the Attached Baseline Groups, Attached Baselines and Compliance panes. <li data-bbox="687 1646 1422 1698">■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups. <p data-bbox="687 1709 1422 1778">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:</p> <ul data-bbox="687 1789 1422 1927" style="list-style-type: none"> <li data-bbox="687 1789 1422 1837">■ The number of patches, extensions, or upgrades included in the baseline or baseline group that you select. <li data-bbox="687 1848 1235 1869">■ The number of staged patches or extensions to a host. <li data-bbox="687 1879 1422 1927">■ The overall compliance of the objects against the patches, extensions, or upgrades included in the selected baselines and baseline groups.

Table 11-1. Update Manager Tab Panes (Continued)

Pane	Description
	<ul style="list-style-type: none"> ■ The vendor, product, version, compliance, release date as well as change log for the selected virtual appliance against the attached upgrade baseline.

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 of the target object.

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.
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.
Installed	Installed compliance state indicates that the update is installed on the target object, and no further user action is required.
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.
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.
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.

Not Applicable	<p>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:</p> <ul style="list-style-type: none"> ■ There are other patches in the Update Manager patch repository that obsolete this patch. ■ The update does not apply to the target object.
Not Installable	The update cannot be installed. The scan operation might succeed on the target object, but remediation cannot be performed.
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.
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.
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.
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.

Baseline and Baseline Group Compliance States

Compliance states are computed after you scan the objects in your inventory against attached baselines or baseline groups. Update Manager computes the compliance state based on the applicability of the patches, extensions, and upgrades contained in the attached baselines or baseline groups.

Compliant

Compliant state indicates that a vSphere object is compliant with all baselines in an attached baseline group or with all patches, extensions, and upgrades in an attached baseline. 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. Compliant are also hosts with attached patch baselines containing extensions or patches in Obsoleted By Host state.

Compliant state occurs under the following conditions:

- Target objects are compliant with the baselines and baseline groups 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.

Non-Compliant

Non-compliant state indicates 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 vSphere object against 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 182.

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 any of the patches are in the 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.

Table 11-2. Patch Details Window

Option	Description
Patch 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.
Patch 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.
Category	Category of the update. The category might be Security, Enhancement, Recall, Info, Other, and so on.
Impact	The action that you must take to apply the update. This action might include rebooting the system or putting the host into maintenance mode.
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.

Table 11-3. Extension Details Window

Option	Description
Patch 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.
Patch 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.
Category	Category of the update. The category might be Security, Enhancement, Recall, Info, Other, and so on.
Impact	The action that you must take to apply the update. This action might include rebooting the system or putting the host into maintenance mode.
Release Date	Release date of the update.

Viewing Upgrade Details

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

Table 11-4. Host Upgrade Details Window

Option	Description
Baseline Name	Name of the upgrade baseline.
Baseline Type	The baseline type is host upgrade.
Baseline Description	Description of the baseline. If the baseline has no description, it is not displayed.
Compliance State	Compliance status for the upgrade. It represents a comparison between the state of the selected object and the upgrade baseline.
ESXi image	Displays the ESXi image included in the baseline.
Product	Displays the release version of the upgrade.
Version	Target version of the upgrade baseline.

Table 11-4. Host Upgrade Details Window (Continued)

Option	Description
Vendor	Vendor that provided the ESXi image.
Acceptance level	<p>Acceptance level of the ESXi image and included software packages. ESXi images can be either Signed or Unsigned, indicating their level of acceptance by VMware. Software packages included in ESXi images have the following acceptance levels:</p> <p>VMware Certified The package has gone through a rigorous certification program that verifies the functionality of the feature, and is signed by VMware with a private key. VMware provides customer support for these packages.</p> <p>VMware Accepted The package has gone through a less rigorous acceptance test program that only verifies that the package does not destabilize the system, and is signed by VMware with a private key. The test regimen does not validate the proper functioning of the feature. VMware support will hand off support calls directly to the partner.</p> <p>Partner Supported The partner has signed an agreement with VMware and has demonstrated a sound test methodology. VMware provides a signed private/public key pair to the partner to use for self-signing their packages. VMware support will hand off support calls directly to the partner.</p> <p>Community Supported The package is either unsigned, or signed by a key that is not cross-signed by VMware. VMware does not provide support for the package. For support, customers must either utilize the community or contact the author of the package.</p>

Table 11-5. 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	Compliance status for the upgrade. It represents a comparison between the state of the selected object and the upgrade baseline.
VMware 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.

Table 11-6. Virtual Appliance Change Log Details Window

Option	Description
Name	Name of the change.
Category	Type of the change. For example, bug fix or feature.
Severity	Severity of the change. For example, critical or moderate.
Reference ID	Unique ID in the reference file domain.
Reference Type	Reference type of the change.

Table 11-6. Virtual Appliance Change Log Details Window (Continued)

Option	Description
Reference URL	URL location that provides a detailed description of the change, such as a link to a knowledge base article.
Introduced in	Version of the virtual appliance in which the change was introduced.

Host Upgrade Scan Messages in Update Manager

When you scan ESX/ESXi hosts against an upgrade baseline, Update Manager runs a precheck script and provides informative messages in the Upgrade Details window for each host. The messages notify you about potential problems with hardware, third-party software on the host, and configuration issues, which might prevent a successful upgrade or migration to ESXi 5.5.

Messages that Update Manager provides correspond to error or warning codes from running the host upgrade precheck script.

For interactive installations, upgrades, and migrations performed by using the ESXi installer, the errors or warnings from the precheck script are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations, upgrades, or migrations, the errors or warnings are written to the installation log.

Update Manager provides scan result messages in the Upgrade Details window for errors or warnings from the precheck script. To see the original errors and warnings returned by the precheck script during an Update Manager host upgrade scan operation, review the Update Manager log file `C:\Documents and Settings\All Users\Application Data\VMware\VMware Update Manager\Logs\vmware-vum-server-log4cpp.log`.

Table 11-7. Scan Result Messages and Corresponding Error and Warning Codes

Scan Result Message in Update Manager	Description
Host CPU is unsupported. New ESXi version requires a 64-bit CPU with support for LAHF/SAHF instructions in long mode.	This message appears if the host processor is 32-bit and does not support required features. The corresponding error code is <code>64BIT_LONGMODESTATUS</code> .
Trusted boot is enabled on the host but the upgrade does not contain the software package <code>esx-tboot</code> . Upgrading the host will remove the trusted boot feature.	This message indicates that the host upgrade scan did not locate the <code>esx-tboot</code> VIB on the upgrade ISO. The corresponding error code is <code>TBOOT_REQUIRED</code>
The root password is not using MD5 hashing, causing it to be authenticated up to only 8 characters. For instructions on how to correct this, see VMware KB 1024500 at http://kb.vmware.com/kb/1024500 .	This message applies only to migrations from ESX to ESXi. This test checks whether the root password is encoded by using the MD5 algorithm. On ESX 4.1 hosts, passwords encrypted by using the DES algorithm are limited to eight symbols. For improved security, you should configure your hosts to use longer passwords. The corresponding error code is <code>MD5_ROOT_PASSWORD</code> .
VMkernel and Service Console network interfaces are sharing the same subnet <i>subnet_name</i> . This configuration is not supported after upgrade. Only one interface should connect to subnet <i>subnet_name</i> .	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning will be output for each such occurrence. The corresponding error code is <code>COS_NETWORKING</code> .
New ESXi version requires a minimum of <i>core_count</i> processor cores.	The host must have at least two cores. The corresponding error code is <code>CPU_CORES</code> .

Table 11-7. Scan Result Messages and Corresponding Error and Warning Codes (Continued)

Scan Result Message in Update Manager	Description
Processor does not support hardware virtualization or it is disabled in BIOS. Virtual machine performance may be slow.	Host performance might be impaired if the host processor does not support hardware virtualization or if hardware virtualization is not turned on in the host BIOS. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation. The corresponding error code is <code>HARDWARE_VIRTUALIZATION</code> .
Insufficient memory, minimum <i>size_in_MB</i> required for upgrade.	The host requires the specified amount of memory to upgrade. The corresponding error code is <code>MEMORY_SIZE</code> .
Host upgrade validity checks for <i>file_name</i> are not successful.	This test checks whether the precheck script itself can be run. The corresponding error code is <code>PRECHECK_INITIALIZE</code> .
The host partition layout is not suitable for upgrade.	Upgrading or migration is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition starts after sector 1843200. The corresponding error code is <code>PARTITION_LAYOUT</code> .
Unsupported configuration.	The file <code>/etc/vmware/esx.conf</code> must exist on the host. This message indicates that the file <code>/etc/vmware/esx.conf</code> is either missing, or the file data cannot be retrieved or read correctly. The corresponding error code is <code>SANE_ESX_CONF</code> .
The host does not have sufficient space on boot partition to store the upgrade image. A minimum of <i>size_in_MB</i> is required. Retry after freeing up sufficient space or perform a CD-based installation.	The ESX host disk must have enough free space to store the contents of the installer DVD. The corresponding error code is <code>SPACE_AVAIL_ISO</code> .
Cannot create a ramdisk of size <i>size_in_MB</i> to store the upgrade image. Check if the host has sufficient memory.	The ESXi host disk must have enough free space to store the contents of the installer DVD. The corresponding error code is <code>SPACE_AVAIL_ISO</code> .
The host does not have sufficient free space on a local VMFS datastore to back up current host configuration. A minimum of <i>size_in_MB</i> is required.	The host disk must have enough free space to store the ESX/ESXi 4.x configuration between reboots. The corresponding error code is <code>SPACE_AVAIL_CONFIG</code> .
The upgrade is not supported for current host version.	Upgrading or migration to ESXi 5.5 is possible only from ESX/ESXi 4.x, ESXi 5.0 and ESXi 5.1 hosts. The corresponding error code is <code>SUPPORTED_ESX_VERSION</code> .
Unsupported devices <i>device_name</i> found on the host.	The script checks for unsupported devices. Some PCI devices are not supported with ESXi 5.5. The corresponding error code is <code>UNSUPPORTED_DEVICES</code> .
Host software configuration requires a reboot. Reboot the host and try upgrade again.	To ensure a good bootbank for the upgrade, you must reboot the hosts before remediation. The corresponding error code is <code>UPDATE_PENDING</code> .

Table 11-7. Scan Result Messages and Corresponding Error and Warning Codes (Continued)

Scan Result Message in Update Manager	Description
In an environment with Cisco Nexus 1000V Distributed Virtual Switch, Update Manager displays different messages in different situations. For details, see “Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present,” on page 111.	<p>If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the precheck script checks if the software is part of the upgrade as well, and that the VEM supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the script returns a warning and the scan result indicates the version of the VEM software that was expected on the upgrade ISO, and the version, if any, that was found on the ISO.</p> <p>The corresponding error code is DISTRIBUTED_VIRTUAL_SWITCH.</p>
The host uses an EMC PowerPath multipathing module <i>file_name</i> to access storage. The host will not be able to access such storage after upgrade.	<p>The script checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the script verifies that matching components (CIM, VMkernel module) also exist in the upgrade. If they do not, the script returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found.</p> <p>The corresponding error code is POWERPATH.</p>

Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present

When you scan a host that is managed by the Cisco Nexus 1000V virtual switch, host upgrade scan messages provide information about problems with compliance between the VEM modules installed on the host and the modules available on the ESXi 5.5 image.

Update Manager supports Cisco Nexus 1000V, a virtual access software switch that works with VMware vSphere and consists of two components.

Virtual Supervisor Module (VSM) The control plane of the switch and a virtual machine that runs NX-OS.

Virtual Ethernet Module (VEM) A virtual line card embedded in ESX/ESXi hosts.

Update Manager determines whether a host is managed by Cisco Nexus 1000V. Update Manager verifies whether Cisco Nexus 1000V VEM VIBs in the ESXi upgrade image are compatible with the Cisco Nexus 1000V VSM managing the host.

By using vSphere ESXi Image Builder, you can create custom ESXi images, which contain third-party VIBs that are required for a successful remediation operation.

Table 11-8. Host Upgrade Scan Messages for the Cisco Nexus 1000V network switch

Host Upgrade Scan Message	Description
The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V software package on the host. Upgrading the host will remove the feature from the host.	A VEM VIB is not available on the ESXi 5.5 upgrade image.
The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade contains a Cisco Nexus 1000V software package <i>VIB_name</i> that is incompatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.	The VEM VIB on the ESXi 5.5 upgrade image is not compatible with the version of the VSM.

Table 11-8. Host Upgrade Scan Messages for the Cisco Nexus 1000V network switch (Continued)

Host Upgrade Scan Message	Description
The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.	The host and the image do not contain VEM VIBs, but the host is still listed in vCenter Server as managed by Cisco Nexus 1000V.
Cannot determine whether the upgrade breaks Cisco Nexus 1000V virtual network switch feature on the host. If the host does not have the feature, you can ignore this warning.	There was a problem with determining compatibility between the VEM VIB on the ESXi 5.5 upgrade image and the VSM. Check whether the version of the VSM managing the host is certified as being compatible with vCenter Server 5.5 and ESXi 5.5.

VMware Tools Status

For VMware Tools, the Upgrade Details window provides information about both compliance state and status. The status indicates whether the current version of VMware Tools is installed or supported and whether upgrades are available.

Table 11-9. VMware Tools Status

VMware Tools Status	Description	Compliance State
VMware Tools version is compliant.	The VMware Tools version is recent and supported. Remediation is not required.	Compliant
VMware Tools is installed, supported, and newer than the version available on the host.	VMware Tools is installed on a machine that is running on an earlier ESX/ESXi version. Remediation is not required.	Compliant
VMware Tools is installed and supported, but a newer version is available on the host.	An earlier supported version of VMware Tools is installed on the virtual machine. You can upgrade VMware Tools, but the existing earlier version is also supported.	Non-Compliant
VMware Tools is installed, but the installed version has a known issue and should be immediately upgraded.	A serious issue is present in the VMware Tools version that is installed on the machine. You must remediate the virtual machine against a VMware Tools upgrade baseline.	Non-Compliant
VMware Tools is installed, but the version is too new to work correctly with this virtual machine.	The existing newer version might cause problems on the virtual machine. You must remediate the virtual machine against a VMware Tools upgrade baseline, to downgrade to a supported version.	Non-Compliant
VMware Tools is installed, but the version is too old.	The VMware Tools version is no longer supported. You must remediate the virtual machine against a VMware Tools upgrade baseline.	Non-Compliant
VMware Tools is not installed.	VMware Tools is not present on the virtual machine. You must install VMware Tools by using the vSphere Client.	Incompatible

Table 11-9. VMware Tools Status (Continued)

VMware Tools Status	Description	Compliance State
VMware Tools is not managed by vSphere.	VMware Tools is installed by using operating system specific packages that cannot be upgraded with Update Manager. To upgrade VMware Tools by using Update Manager, you must install VMware Tools from the vSphere Client.	Incompatible
Status is empty.	The virtual machine has not been scanned.	Unknown

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 *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

This chapter includes the following topics:

- [“Orchestrated Upgrades of Hosts and Virtual Machines,”](#) on page 115
- [“Remediating Hosts,”](#) on page 116
- [“Remediating Virtual Machines and Virtual Appliances,”](#) on page 131
- [“Scheduling Remediation for Hosts, Virtual Machines, and Virtual Appliances,”](#) on page 133

Orchestrated Upgrades of Hosts and Virtual Machines

You can perform orchestrated upgrades of hosts or virtual machines in your vSphere inventory by using baseline groups. Baseline groups contain baselines for either hosts or virtual machines.

You can perform an orchestrated upgrade at the level of a container object or an individual object.

Orchestrated Upgrade of Hosts

Orchestrated upgrades let you apply upgrades, patches, and extensions to hosts in your inventory by using a single host baseline group.

If the baseline group contains an upgrade baseline, Update Manager first upgrades the hosts and then applies the patch or extension baselines. Because the upgrade runs first and patches are applicable to a specific host version, the orchestrated workflow ensures that patches are not lost during the upgrade.

Orchestrated Upgrade of Virtual Machines

You can use an 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

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. You cannot upgrade the virtual hardware of the virtual machines if VMware Tools is not installed, is out of date, or is managed by third-party tools.

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 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 by default. With Update Manager 5.5 you can select to run host remediation in parallel.

When you remediate a cluster of hosts sequentially and one of the hosts fails to enter maintenance mode, Update Manager reports an error, and the process stops and fails. The hosts in the cluster that are remediated stay at the updated level. The ones that 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 should 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 has the cluster features enabled. For more information, see [“Cluster Remediation Options Report,”](#) on page 130.

When you remediate a cluster of hosts in parallel, Update Manager remediates multiple hosts concurrently. During parallel remediation, if Update Manager encounters an error when remediating a host, it ignores the host and the remediation process continues for the other hosts in the cluster. Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.

Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. The reason is that by design only one host from a Virtual SAN cluster can be in a maintenance mode at any time.

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 Remediation

When you upgrade or migrate hosts by using a typical ESXi image that does not contain third-party software, no third-party modules are preserved after the upgrade.

You can upgrade or migrate hosts by using custom ESXi images that contain third-party modules for ESXi 5.5. In such a case, third-party modules that are compatible with ESXi 5.5 are available on the upgraded host.

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.

IMPORTANT After you have upgraded or migrated your host to ESXi 5.5, you cannot roll back to your version ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software. Back up your host configuration before performing an upgrade or migration. If the upgrade or migration fails, you can reinstall the ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software that you upgraded or migrated from, and restore your host configuration. For more information about backing up and restoring your ESX/ESXi configuration, see *vSphere Upgrade*.

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

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 5.5, you can remediate hosts of version ESX/ESXi 4.x and ESXi 5.x against offline bundles that you have imported manually.

You can stage patches before remediation to reduce host downtime.

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 179.

Remediation of PXE Booted ESXi Hosts

Update Manager 5.5 lets you to remediate PXE booted ESXi 5.x hosts. Update Manager does not apply patches that require a reboot to PXE booted ESXi hosts.

If there is any additional software installed on the PXE booted ESXi host, the software might be lost if the host restarts. You should update your image profile with the additional software so that it will be present after the reboot.

IMPORTANT Update Manager does not remediate PXE booted ESXi hosts of version 4.x.

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

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

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

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 5.5 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 5.5 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 5.5 host stores up to two builds, one boot build and one standby build.

Remediation of ESXi 4.0, 4.1, 5.0, and 5.1 hosts to their respective ESXi update releases is a patching process, while the remediation from version 4.x, 5.0 and 5.1 to 5.5 is considered an upgrade.

Remediation Specifics of ESXi 5.x Hosts

Since Update Manager 5.1 release, ESXi 5.x host upgrades are handled in a different way than earlier Update Manager instances.

When you perform a host scan, the target host is scanned against a set of VIBs from the upgrade image. In Update Manager 5.0 and earlier, when you scan hosts against an upgrade baseline that contains an ISO image of the same version as the target host, Update Manager displays Incompatible compliance state and remediation is not possible. In Update Manager 5.5, if you scan an ESXi 5.5 host against a base ESXi 5.5 image distributed by VMware or against a custom ESXi 5.5 image that contains the same set of VIBs as the ones already installed on the target host, Update Manager displays Compliant scan result. Update Manager 5.5 supports use of ESXi 5.5 ISO images for upgrade of an ESXi 5.5 host to ESXi 5.5 that contains additional or custom VIBs.

You might have several set of situations where you scan and remediate ESXi 5.x hosts against an ESXi 5.5 image. All 5.x versions of the ESXi hosts are binary compatible. Any third-party software modules on ESXi 5.x host will remain intact after upgrade to ESXi 5.5, regardless of whether you select the option to remove third-party modules. As different ESXi 5.x hosts are binary compatible, scanning and remediation operations to ESXi 5.5 return identical results.

The remediation process of ESXi 5.0 and ESXi 5.1 host to ESXi 5.5 image is an upgrade process. The remediation process of ESXi 5.5 host by using ESXi 5.5 image with additional VIBs is equivalent to a patching process.

Table 12-1. Scan and Remediation Situations for ESXi 5.x Hosts Against ESXi 5.5 Images

Action	Description
Scan and remediation of ESXi 5.x hosts against ESXi 5.5 image that contains additional non-conflicting and non-obsolete VIBs with the target host.	Update Manager displays Non-Compliant scan result. Remediation succeeds. All VIBs on the target host before remediation remain on the host. All VIBs from the upgrade image that are not present on the target host before remediation are added to the host.
Scan and remediation of ESXi 5.x hosts against ESXi 5.5 image that contains VIBs of later version than the same VIBs on the target host.	Update Manager displays Non-Compliant scan result. Remediation succeeds. VIBs on the target host are updated to the later version.
Scan and remediation of ESXi 5.x hosts against ESXi 5.5 image that contains conflicting VIBs with the target host.	Update Manager displays Incompatible scan result. Remediation fails. The host remains intact.

Table 12-1. Scan and Remediation Situations for ESXi 5.x Hosts Against ESXi 5.5 Images (Continued)

Action	Description
Scan and remediation of ESXi 5.x hosts against ESXi 5.5 image that contains vendor-tagged VIBs.	<ul style="list-style-type: none"> ■ If the vendor-tagged VIBs do not match the host hardware, Update Manager displays Incompatible scan result. Remediation fails. ■ If the vendor-tagged VIBs match the host hardware, Update Manager displays Non-Compliant scan result and remediation succeeds.
Scan and remediation of ESXi 5.x hosts against an ESXi 5.5 image that contains VIBs that obsolete the VIBs installed on the host.	Remediation succeeds. All VIBs that have been installed on the target host before remediation are replaced by the newer VIBs from the ESXi image.

Remediation Specifics of Hosts That Are Part of a Virtual SAN Cluster

There are some specifics about remediating hosts that are part of a Virtual SAN cluster.

By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Because of that the host remediation process might take extensive amount of time to complete since Update Manager must handle the remediation of the hosts sequentially. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.

You have several ways to handle remediation of a host that is part of a Virtual SAN cluster, depending on how you want the virtual machines handled on the host:

- You can put the host in maintenance mode from the vSphere Web Client, and remediate the host by using Update Manager.
- You can put the host in maintenance mode from the vSphere Client, and remediate the host by using Update Manager.
- You can have a host entering maintenance mode during the Update Manager remediation process.

From the vSphere Web Client you can select between multiple options when putting a host from a Virtual SAN cluster in maintenance mode: Ensure accessibility, Full data evacuation, and No data evacuation. The Ensure accessibility option is the default option, and means that when you put a host in maintenance mode, the Virtual SAN ensures that all accessible virtual machines on this host remain accessible. To learn more about each of the options, see the *Place a Member of Virtual SAN Cluster in Maintenance Mode* topic from *vSphere Storage* guide.

When you put a host from a Virtual SAN cluster into maintenance mode from the vSphere Client, you must confirm a maintenance mode warning message. Before confirming the message, you can select to move powered off and suspended virtual machines to other hosts in the cluster, but you have no options on how to handle the powered on virtual machines on the host. The powered on virtual machines are automatically handled equivalently to the default Ensure accessibility option.

When you use the Update Manager, the remediation process might put the host from the Virtual SAN cluster in maintenance mode, which would handle the virtual machines on the host in the manner of the default Ensure accessibility option.

If a host is a member of a Virtual SAN cluster, and any virtual machine on the host uses a VM storage policy with a setting for "Number of failures to tolerate=0", the host might experience unusual delays when entering maintenance mode. The delay occurs because Virtual SAN has to migrate the virtual machine data from one disk to another in the Virtual SAN datastore cluster. Delays might take up to hours. You can workaround this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files in the Virtual SAN datastore.

Remediating Hosts That Contain Third-Party Software

Hosts might contain third-party software, such as Cisco Nexus 1000V VEMs or EMC PowerPath modules. To upgrade or migrate such hosts successfully, you must either use a custom ESXi image or delete the third-party modules during remediation.

You cannot directly migrate third-party solutions as part of a host upgrade. Architectural changes between ESX/ESXi 4.x and ESXi 5.x and VIB forward incompatibility result in the loss of third-party components and possible system instability. To accomplish such migrations, you can create a custom ISO file with ESXi Image Builder CLI. For information about upgrading with third-party customizations, see the *vSphere Upgrade* documentation. For information about using ESXi Image Builder CLI to make a custom ISO, see the *vSphere Installation and Setup* documentation.

You can remove installed third-party solutions by using the Update Manager Remediate wizard.

ESXi 5.0, ESXi 5.1 hosts and ESXi 5.5 hosts are binary compatible. Any third-party software modules on ESXi 5.0 and ESXi 5.1 hosts will remain intact after upgrade to ESXi 5.5, regardless of whether you chose to remove third-party modules.

If you are upgrading an ESXi 5.0 or ESXi 5.1 host to ESXi 5.5 host, supported custom VIBs on the host that are not included in the ESXi installer ISO are migrated. If the host or the upgrade ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the conflicting VIB. You can remove the VIB and retry the upgrade, or use ESXi Image Builder CLI to create a custom .iso that resolves the conflict.

To discover potential problems with third-party software before an upgrade or migration operation, scan the hosts against an upgrade baseline and review the scan messages in the Update Manager Compliance view. See [“Host Upgrade Scan Messages in Update Manager,”](#) on page 109 and [“Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present,”](#) on page 111.

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 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 can stage patches to PXE booted ESXi 5.x hosts, but if the host is restarted prior to remediation, the staged patches will be lost and you will have to stage them again.

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 *vCenter Server and Host Management*. For a list of Update Manager privileges and their descriptions, see [“Update Manager Privileges,”](#) on page 77.

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 127.

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 instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- 1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.
- 2 Right-click the inventory object you want to remediate and select **Remediate**.
If you select a container object, all hosts under the selected object are remediated.
- 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 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 Schedule page, specify a unique name and an optional description for the task.
- 8 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.
- 9 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

- 10 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

- 11 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

- 12 (Optional) Select the check box under ESXi 5.x Patch Settings to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

- 13 Click **Next**.

- 14 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. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. NOTE Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the Power State menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

- 15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.
- 16 On the Ready to Complete page, 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 or migrate all hosts in your vSphere inventory by using a single upgrade baseline containing an ESXi 5.5 image.

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

To upgrade or migrate hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-5.5.0-build_number.x86_64.iso` or a custom image created by using Image Builder.

NOTE In case of an unsuccessful upgrade or migration from ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 to ESXi 5.5, you cannot roll back to your previous ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 instance.

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 instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

To remediate a host against an upgrade baseline, attach the baseline to the host.

Review any scan messages in the Upgrade Details window for potential problems with hardware, third-party software, and configuration issues that might prevent a successful upgrade or migration to ESXi 5.1. See [“Host Upgrade Scan Messages in Update Manager,”](#) on page 109 and [“Host Upgrade Scan Messages When Cisco Nexus 1000V Is Present,”](#) on page 111.

Procedure

- 1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.
- 2 Right-click the inventory object you want to remediate and select **Remediate**.
If you select a container object, all hosts under the selected object are remediated.
- 3 On the Remediation Selection page of the Remediate wizard, select the upgrade baseline to apply.
- 4 (Optional) Select the hosts that you 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**.

- 6 (Optional) On the ESXi 5.5 Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and ignore warnings about unsupported devices on the host in order to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.5 your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

NOTE ESXi 5.0, ESXi 5.1 and ESXi 5.5 hosts are binary compatible. Any hardware or third-party software modules on a ESXi 5.0 or a ESXi 5.1 host will remain intact after upgrade to ESXi 5.5.

- 7 Click **Next**.
- 8 On the Schedule page, specify a unique name and an optional description for the task.

- 9 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.
- 10 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

- 11 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

- 12 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

- 13 Click **Next**.

- 14 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.

Option	Details
Disable Fault Tolerance (FT) if it is enabled for the VMs on the selected hosts.	<p>If FT is turned on for any of the virtual machines on a host, Update Manager does not remediate that host.</p> <p>For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.</p>
Enable parallel remediation for the hosts in the selected clusters.	<p>Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially.</p> <p>By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel.</p> <p>By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number.</p> <p>NOTE Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the Power State menu in the Maintenance Mode Settings pane on the Host Remediation Options page.</p>
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	<p>Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.</p>

- 15 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.
- 16 On the Ready to Complete page, click **Finish**.

NOTE In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

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.

You can perform an orchestrated upgrade by using a host baseline group. The upgrade baseline in the baseline group runs first, followed by patch and extension baselines.

Prerequisites

Ensure that at least one 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 instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- 1 On the **Home** page of the vSphere Client, select **Hosts and Clusters** and click the **Update Manager** tab.
- 2 Right-click the inventory object you want to remediate and select **Remediate**.
If you select a container object, all hosts under the selected object are remediated.
- 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 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**.
- 6 (Optional) On the ESXi 5.5 Upgrade page, select the option to remove any installed third-party software modules that are incompatible with the upgrade and ignore warnings about unsupported devices on the host in order to continue with the remediation.

In case any additional third-party modules installed on the hosts are incompatible with the upgrade, the upgrade remediation does not succeed. To proceed and upgrade to ESXi 5.5 your ESX/ESXi hosts that contain third-party modules by using an ESXi image without the corresponding VIBs, you must choose to remove the third-party software on the hosts.

NOTE ESXi 5.0, ESXi 5.1 and ESXi 5.5 hosts are binary compatible. Any hardware or third-party software modules on a ESXi 5.0 or a ESXi 5.1 host will remain intact after upgrade to ESXi 5.5.

- 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 Schedule page, specify a unique name and an optional description for the task.
- 11 Select **Immediately** to begin the process immediately after you complete the wizard, or specify a time for the remediation process to begin, and click **Next**.
- 12 On the Host Remediation Options page, from the **Power state** drop-down menu, you can select the change in the power state of the virtual machines and virtual appliances that are running on the hosts to be remediated.

Option	Description
Power Off virtual machines	Power off all virtual machines and virtual appliances before remediation.
Suspend virtual machines	Suspend all running virtual machines and virtual appliances before remediation.
Do Not Change VM Power State	Leave virtual machines and virtual appliances in their current power state. A host cannot enter maintenance mode until virtual machines on the host are powered off, suspended, or migrated with vMotion to other hosts in a DRS cluster.

Some updates require that a host enters maintenance mode before remediation. Virtual machines and appliances cannot run when a host is in maintenance mode.

To reduce the host remediation downtime at the expense of virtual machine availability, you can choose to shut down or suspend virtual machines and virtual appliances before remediation. In a DRS cluster, if you do not power off the virtual machines, the remediation takes longer but the virtual machines are available during the entire remediation process, because they are migrated with vMotion to other hosts.

- 13 (Optional) Select **Retry entering maintenance mode in case of failure**, specify the number of retries, and specify the time to wait between retries.

Update Manager waits for the retry delay period and retries putting the host into maintenance mode as many times as you indicate in **Number of retries** field.

- 14 (Optional) Select **Disable any removable media devices connected to the virtual machine on the host**.

Update Manager does not remediate hosts on which virtual machines have connected CD, DVD, or floppy drives. In cluster environments, connected media devices might prevent vMotion if the destination host does not have an identical device or mounted ISO image, which in turn prevents the source host from entering maintenance mode.

After remediation, Update Manager reconnects the removable media devices if they are still available.

- 15 (Optional) Select the check box under ESXi 5.x Patch Settings to enable Update Manager to patch powered on PXE booted ESXi hosts.

This option appears only when you remediate hosts against patch or extension baselines.

- 16 Click **Next**.

- 17 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. For FT to be enabled, the hosts on which the Primary and Secondary virtual machines run must be of the same version and must have the same patches installed. If you apply different patches to these hosts, FT cannot be re-enabled.
Enable parallel remediation for the hosts in the selected clusters.	Remediate hosts in clusters in a parallel manner. If the setting is not selected, Update Manager remediates the hosts in a cluster sequentially. By design only one host from a Virtual SAN cluster can be in a maintenance mode at any time. Update Manager remediates hosts that are part of a Virtual SAN cluster sequentially even if you select the option to remediate them in parallel. By default, Update Manager continuously evaluates the maximum number of hosts it can remediate concurrently without disrupting DRS settings. You can limit the number of concurrently remediated hosts to a specific number. NOTE Update Manager remediates concurrently only the hosts on which virtual machines are powered off or suspended. You can choose to power off or suspend virtual machines from the Power State menu in the Maintenance Mode Settings pane on the Host Remediation Options page.
Migrate powered off and suspended virtual machines to other hosts in the cluster, if a host must enter maintenance mode.	Update Manager migrates the suspended and powered off virtual machines from hosts that must enter maintenance mode to other hosts in the cluster. You can choose to power off or suspend virtual machines before remediation in the Maintenance Mode Settings pane.

- 18 (Optional) Generate a cluster remediation options report by clicking **Generate Report** on the Cluster Remediation Options page and click **Next**.

19 On the Ready to Complete page, click **Finish**.

Note In the Recent Tasks pane, the remediation task is displayed and will remain at about 22 percent for most of the process. The process is still running and will take approximately 15 minutes to complete.

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.

You can generate a cluster remediation report when you create a remediation task for hosts that are contained in a cluster. You generate the report from the Cluster Remediation Options page of the Remediate wizard.

Table 12-2. 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.
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 upgrade baselines. You can also schedule a remediation operation at a time that is convenient for you.

NOTE Update Manager 5.x supports remediation of virtual appliances and vApps created with VMware Studio 2.0 and later.

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.

During remediation, virtual appliances must be able to connect to the Update Manager server. Ensure that the proxy configuration of virtual appliances lets them connect to the Update Manager server.

With Update Manager you can remediate templates. A template is a master copy of a virtual machine that can be used to create and provision new virtual machines.

You can set up automatic upgrades of VMware Tools on power cycle for virtual machines. For more information, see [“Upgrade VMware Tools on Power Cycle,”](#) on page 132.

NOTE Update Manager 5.x does not support virtual machine patch baselines.

If a host is connected to vCenter Server by using an IPv6 address, you cannot scan and remediate virtual machines and virtual appliances that run on the host.

Remediation of VMware vCenter Server Appliance is not supported. For more information about upgrading the virtual appliance, see the vCenter Server upgrade documentation.

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.

NOTE When you upgrade VMware Tools on power cycle in selected virtual machines, Update Manager does not take a snapshot of the virtual machines before remediation and you cannot roll back. Update Manager does not take snapshots of fault tolerant virtual machines.

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.

You can perform an orchestrated upgrade by using a virtual machine baseline group. The VMware Tools upgrade baseline runs first, followed by the virtual machine hardware upgrade baseline.

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 instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- 1 On the **Home** page of the vSphere Client , select **VMs and Templates** and click the **Update Manager** tab.
- 2 Right-click a container object from the inventory and select **Remediate**.
All virtual machines and appliances in the container are also remediated.
- 3 On the Remediation Selection page of the Remediate wizard, select the baseline group and upgrade baselines to apply.
- 4 Select the virtual machines and appliances that you want to remediate and click **Next**.
- 5 On the Schedule page, specify a name and an optional description for the task.
- 6 Select **Immediately** to begin the remediation process immediately after you complete the wizard, or enter specific times for powered on, powered off, or suspended virtual machines.
- 7 (Optional) Choose whether to upgrade VMware Tools on power cycle.

This option is active only when you perform an upgrade against a single Upgrade VMware Tools to Match Host baseline. You can only enable VMware Tools upgrade on power cycle from the Remediate wizard, but you cannot disable it. You can disable the setting by clicking the **VMware Tools upgrade settings** button in the Update Manager Compliance view and deselecting the check box of a virtual machine in the Edit VMware Tools upgrade settings window.

- 8 (Optional) Specify the rollback options.

This option is not available if you selected to upgrade VMware Tools on power cycle.

- a On the Rollback Options page of the Remediate wizard, select **Take a snapshot of 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.

Update Manager does not take snapshots of fault tolerant virtual machines.

If you perform a VMware Tools upgrade and select to upgrade VMware Tools on power cycle, Update Manager takes no snapshots of the selected virtual machines before remediation.

- 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 **Take a snapshot of the memory for the virtual machine** check box.
- 9 Click **Next**.
 - 10 Review the Ready to Complete page, and click **Finish**.

Upgrade VMware Tools on Power Cycle

You can automate the process to upgrade VMware Tools for the virtual machines in your inventory.

You can set up Update Manager to perform a check of the VMware Tools version when a machine is powered on or restarted. If necessary, Update Manager upgrades VMware Tools to the latest version supported by the host that is running the virtual machine.

When you perform a VMware Tools upgrade on power cycle, Update Manager does not take a snapshot of the virtual machine, and you cannot roll back to the previous version.

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 instance by selecting the name of the corresponding vCenter Server system in the navigation bar.

Procedure

- ◆ To enable upgrading of VMware Tools on power cycle, use one of the following options.

Option	Action
VMware Tools upgrade settings	<ol style="list-style-type: none"> a On the Home page of the vSphere Client , select VMs and Templates and click the Update Manager tab. b Select a virtual machine or a container object from the inventory. c Click VMware Tools upgrade settings. d In the Edit VMware Tools upgrade settings window, select the check boxes of the virtual machines for which you want to enable VMware Tools upgrade on power cycle. e Click Apply.
Check and update Tools during power cycle	<ol style="list-style-type: none"> a Right-click an object in the vSphere inventory and select Edit Settings. b On the Options tab, click VMware Tools. c In the Advanced section, select the Check and upgrade Tools during power cycling checkbox. d Click OK.

The next time the virtual machines are restarted or powered on, Update Manager checks the version of VMware Tools installed in the machines and performs an upgrade, if necessary.

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 specify a time for the remediation process on the Schedule page of the Remediate wizard.

You cannot edit existing scheduled remediation tasks. You can remove a scheduled remediation task and create a new one in its place.

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.

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.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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

- ◆ In the Update Manager Administration view, click the **Events** tab to get information about recent events.

This chapter includes the following topics:

- [“View Tasks and Events for a Selected Object,”](#) on page 135
- [“Update Manager Events,”](#) on page 136

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 In the vSphere Client 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 13-1. Update Manager Events

Type	Message Text	Action
Info	Successfully downloaded host patch definitions. New patches: <i>number_of_patches</i> .	
Error	Could not download host patch definitions.	Check your network connection to make sure that your metadata source is reachable.
Info	Successfully downloaded host patch packages. New packages: <i>number_of_packages</i> .	
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: <i>number_of_notifications</i> .	
Error	Could not download notifications.	Check your network connection.
Info	Successfully scanned <i>vSphere_object_name</i> .	
Info	Scanning object <i>vSphere_object_name</i> .	
Error	Scanning of <i>vSphere_object_name</i> is canceled by user.	
Error	Could not scan <i>vSphere_object_name</i> .	Check the Update Manager log (<code>vmware-vum-server-log4cpp.log</code>) for scan errors.
Warning	Found a missing patch: <i>patch_name</i> when scanning <i>vSphere_object_name</i> . Re-downloading patch definitions might resolve this problem.	
Info	Successfully scanned <i>virtual_appliance_name</i> for VA upgrades.	
Error	Could not scan <i>virtual_appliance_name</i> for VA upgrades.	
Info	Successfully scanned <i>vSphere_object_name</i> for VMware Tools upgrades.	
Error	Could not scan <i>vSphere_object_name</i> for VMware Tools upgrades.	
Warning	VMware Tools is not installed on <i>vSphere_object_name</i> . VMware vSphere Update Manager supports upgrading only an existing VMware Tools installation.	
Warning	VMware Tools upgrade scan was not performed on <i>virtual_machine_name</i> . VMware Tools upgrade scan is supported only for VMs that run on ESX/ESXi 4.0 and higher. VMware Tools upgrade scan is not supported for virtual appliances.	
Warning	VMware Tools upgrade was not performed on <i>virtual_machine_name</i> . VMware Tools upgrade is supported only for VMs that run on ESX/ESXi 4.0 and higher. VMware Tools upgrade is not supported for virtual appliances.	
Error	Could not scan <i>virtual_machine_name</i> because the virtual machine has an invalid connection state: <i>virtual_machine_connection_state</i> .	Check the state of the virtual machine. Reboot the virtual machine to facilitate scanning.

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not scan <i>host_name</i> because the host has an invalid connection state: <i>host_connection_state</i> .	Check the state of the host. Reboot the host to facilitate scanning.
Info	Remediation succeeded for <i>vSphere_object_name</i> .	
Info	Remediating object <i>vSphere_object_name</i> .	
Error	Remediation did not succeed for <i>vSphere_object_name</i> .	Check the Update Manager log (<i>vmware-vum-server-log4cpp.log</i>) for remediation errors.
Info	VMware Tools upgrade succeeded for <i>vSphere_object_name</i> .	
Error	VMware Tools upgrade did not succeed for <i>vSphere_object_name</i> .	
Info	Successfully enabled the option for VMware Tools upgrade on VM power cycle for <i>virtual_machine_name</i> .	
Error	Could not enable the option for VMware Tools upgrade on VM power cycle for <i>virtual_machine_name</i> .	
Info	Successfully disabled the option for VMware Tools upgrade on VM power cycle for <i>virtual_machine_name</i> .	
Error	Could not disable the option for VMware Tools upgrade on VM power cycle for <i>virtual_machine_name</i> .	
Error	Could not remediate <i>virtual_machine_name</i> because the virtual machine has an invalid connection state: <i>virtual_machine_connection_state</i> .	Check the virtual machine's state. Restart the virtual machine to facilitate remediation.
Error	Could not remediate <i>host_name</i> because the host has an invalid connection state: <i>host_connection_state</i> .	Check the state of the host. Restart the host to facilitate remediation.
Info	Staging succeeded for <i>vSphere_object_name</i> .	
Error	Staging did not succeed for <i>vSphere_object_name</i> , <i>error_message</i> .	
Info	Staging patches to host <i>host_name</i> .	
Error	Could not stage patches to <i>host_name</i> because the host has an invalid connection state: <i>host_connection_state</i> .	
Error	Scan or remediation is not supported on <i>vSphere_object_name</i> because of unsupported or unknown OS: <i>operating_system_name</i> .	
Info	VMware vSphere Update Manager download alert (critical/total): <i>ESX data.esxCritical/data.esxTotal</i> .	Provides information about the number of patches downloaded.
Info	VMware vSphere Update Manager notification download alert	
Info	VMware vSphere Update Manager recall alert	
Info	VMware vSphere Update Manager recall fix alert	
Info	VMware vSphere Update Manager informative notification (moderate) alert	
Info	VMware vSphere Update Manager informative notification (important) alert	
Info	VMware vSphere Update Manager informative notification (critical) alert	
Error	Could not scan <i>virtual_machine_name</i> because host <i>host_name</i> is of unsupported version <i>host_version</i> .	For the latest information on which virtual machines can be scanned, see the release notes.

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not remediate <i>virtual_machine_name</i> because host <i>host_name</i> is of unsupported version <i>host_version</i> .	For the latest information on which hosts can be scanned, see the release notes.
Error	Could not scan <i>host_name</i> for patches because it is of unsupported version <i>host_version</i> .	For the latest information on which ESX/ESXi hosts can be scanned, see the release notes.
Error	Could not stage patches to <i>host_name</i> because it is of unsupported version <i>host_version</i> .	You can stage patches to hosts that are running ESX/ESXi 4.0 or later.
Error	Could not remediate <i>host_name</i> because it is of unsupported version <i>host_version</i> .	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.
Error	There is no VMware vSphere Update Manager license for <i>vSphere_object_name</i> for the required operation.	Obtain the required licenses to complete the desired task.
Warning	VMware vSphere Update Manager is running out of storage space. Location: <i>path_location</i> . Available space: <i>free_space</i> .	Add more storage.
Warning	VMware vSphere Update Manager is critically low on storage space! Location: <i>path_location</i> . Available space: <i>free_space</i> .	Add more storage.
Error	An unknown internal error occurred during the required operation on <i>virtual_machine_name</i> . Check the logs for more details and retry the operation.	
Error	Could not install patches on <i>vSphere_object_name</i> .	
Info	Installation of patches <i>patch_ID</i> started on host <i>host_name</i> .	
Info	Installation of patches <i>patch_ID</i> succeeded on <i>host_name</i> .	
Info	The following additional patches are included to resolve a conflict for installation on <i>vSphere_object_name</i> : <i>message</i> .	
Info	To resolve a conflict for installation on <i>vSphere_object_name</i> , the following additional patches might need to be included in the baseline: <i>message</i> .	
Info	VMware vSphere Update Manager could not find patches to resolve the conflict for installation on <i>vSphere_object_name</i> .	
Info	Installation of patches succeeded on <i>vSphere_object_name</i> .	
Info	Start rebooting host <i>host_name</i> .	
Info	Waiting for host <i>host_name</i> to reboot.	
Info	Host <i>host_name</i> is successfully rebooted.	
Error	Cannot reboot host <i>host_name</i> .	
Error	Cannot stage patch <i>patch_name</i> to <i>host_name</i> .	
Info	Staging of patch to <i>host_name</i> succeeded.	
Info	Started staging of patches <i>patch_IDs</i> on <i>host_name</i> .	
Info	Sysprep settings are restored.	
Info	Sysprep is disabled during the remediation.	
Info	Could not scan orphaned VM <i>virtual_machine_name</i> .	
Info	Could not remediate orphaned VM <i>virtual_machine_name</i> .	

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Could not download patch packages for following patches: <i>message</i> .	Check your network connections to make sure that your patch source is reachable.
Warning	<i>virtual_machine_name</i> contains an unsupported volume <i>volume_label</i> . Scan results for this VM might be incomplete.	
Info	Canceling task on <i>vSphere_object_name</i> .	
Warning	There are running tasks for the entity <i>vSphere_object_name</i> that cannot finish within a specific time. The operation will stop.	
Warning	Action is not supported for Linux VM/VA <i>virtual_machine_or_virtual_appliance_name</i> . VMware Tools is not installed or the machine cannot start.	
Warning	Action is not supported for offline or suspended virtual appliance <i>virtual_appliance_name</i> .	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 <i>virtual_appliance_name</i> .	
Info	Could not discover virtual appliance <i>virtual_appliance_name</i> .	An error occurred during the discovery of the virtual appliance.
Error	Auto update is set to ON for virtual appliance <i>virtual_appliance_name</i> .	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 <i>virtual_appliance_name</i> . The appliance does not support updates by vCenter Server.	
Info	Open <i>vSphere_object_name</i> firewall ports.	
Info	Close <i>vSphere_object_name</i> firewall ports.	
Info	Patch definitions for <i>vSphere_object_name</i> are missing. Download patch definitions first.	
Info	Patch definition for <i>vSphere_object_name</i> 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.	

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
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 version <i>host_version</i> is not supported for upgrade.	
Error	The host cannot be upgraded due to incompatible partition layout.	
Error	Upgrade requires at least <i>disk_size</i> MB free space on root partition, only <i>disk_size</i> MB found.	
Error	Upgrade requires at least <i>disk_size</i> MB free space on bootbank, only <i>disk_size</i> MB found.	
Error	Upgrade requires at least <i>disk_size</i> MB free space on VMFS datastore, only <i>disk_size</i> MB found.	
Warning	Insufficient memory found on the host: <i>memory_size</i> MB required, <i>memory_size</i> MB found.	
Error	Error in ESX configuration file <i>configuration_file</i> .	
Error	The passwords cannot be migrated because the password encryption scheme is incompatible.	
Warning	Unsupported devices found on the host.	
Warning	The software modules <i>modules</i> found on the host are not part of the upgrade image. These modules will be removed during upgrade.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch feature installed on the host will be removed during upgrade.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch software package <i>package_name</i> in the upgrade image is incompatible with the Cisco Nexus 1000v software package <i>package_name</i> installed on the host. Upgrading the host will remove the feature from the host.	
Warning	There is no Cisco Nexus 1000v vNetwork Distributed Switch software package in the upgrade image. Upgrading the host will remove the feature from the host.	
Warning	Cisco Nexus 1000v vNetwork Distributed Switch software package <i>package_name</i> in the upgrade image is incompatible with the Cisco Nexus 1000v VSM managing the vDS. Upgrading the host will remove the feature from the host.	
Warning	There is no Cisco Nexus 1000v vNetwork Distributed Switch software package in the upgrade image that is compatible with the Cisco Nexus 1000v VSM managing the vDS. Upgrading the host will remove the feature from the host.	
Warning	EMC PowerPath module <i>module</i> installed on the host will be removed during upgrade.	
Error	Upgrade precheck script error.	

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Info	Successfully scanned <i>vSphere_object_name</i> for Virtual Hardware upgrades.	
Error	Could not scan <i>vSphere_object_name</i> for Virtual Hardware upgrades.	
Error	Virtual Hardware upgrade did not succeed for <i>virtual_machine_name</i> , 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 <i>virtual_machine_name</i> , 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 <i>virtual_machine_name</i> , 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 <i>virtual_machine_name</i> , 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 scan was not performed for <i>virtual_machine_name</i> . Virtual Hardware upgrade scan is supported only for VMs that run on ESX 4.0 hosts and higher. Virtual Hardware upgrade scan is not supported for virtual appliances.	
Warning	Virtual Hardware upgrade was not performed for <i>virtual_machine_name</i> . Virtual Hardware upgrade is supported only for VMs that run on ESX/ESXi 4.0 and higher. Virtual Hardware upgrade is not supported for virtual appliances.	
Info	Virtual Hardware upgrade succeeded for <i>vSphere_object_name</i> .	
Error	Could not perform Virtual Hardware upgrade on <i>vSphere_object_name</i> .	
Error	VM <i>virtual_machine_name</i> has either VMware vSphere 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 <i>host_name</i> has a VM <i>virtual_machine_name</i> with VMware vSphere 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 is migrated to another host.
Error	Error while waiting for VMware Tools to respond. Verify that VMware Tools is running in VM <i>virtual_machine_name</i> .	
Error	The version of VMware Tools installed in <i>virtual_machine_name</i> does not support automatic upgrade. Upgrade VMware Tools manually.	
Info	Suspended VM <i>virtual_machine_name</i> has been skipped.	
Warning	Cannot remediate host <i>host_name</i> 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.

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Cannot scan host <i>host_name</i> 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 <i>host_name</i> 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 <i>host_name</i> 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 <i>host_name</i> 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 <i>host_name</i> 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 <i>host_name</i> 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 <i>host_name</i> 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	Host <i>host_name</i> is a PXE booted ESXi host. Scanning, staging, and remediation are not supported on PXE booted ESXi hosts of version 4.x.	
Warning	Host <i>host_name</i> is a PXE booted ESXi 5.0 host. You did not enable remediation of this host.	You can enable remediation for PXE booted ESXi hosts of version 5.0.
Warning	Cannot remediate host <i>host_name</i> 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 remediate host <i>host_name</i> because it cannot enter maintenance mode.	
Error	Cannot remediate host <i>host_name</i> because it cannot enter maintenance mode <i>reason</i> .	
Error	Cannot migrate VM <i>virtual_machine_name</i> from <i>source_host_name</i> to <i>destination_host_name</i> .	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 <i>virtual_machine_name</i> on host <i>host_name</i> .	
Error	Cannot disable FT for VM <i>virtual_machine_name</i> on host <i>host_name</i> .	Update Manager does not scan, stage, or remediate hosts on which virtual machines are with enabled FT.

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Cannot check compatibility of the VM <i>virtual_machine_name</i> for migration with vMotion to host <i>host_name</i> .	
Error	VMware vSphere Update Manager could not restore HA admission control/DPM settings for cluster <i>cluster_name</i> to their original values. These settings have been changed for patch installation. Check the cluster settings and restore them manually.	
Error	VMware vSphere Update Manager could not restore initial Fault Tolerance state of one or more virtual machines. Check the Fault Tolerance settings and restore them manually.	
Error	VMware vSphere Update Manager could not restore the original power state for all VMs in cluster <i>cluster_name</i> . These settings have been changed for patch installation. You can manually restore the original power state of the VMs.	
Error	VMware vSphere Update Manager could not restore the original removable device connection settings for all VMs in cluster <i>cluster_name</i> . These settings have been changed for patch installation. You can manually restore the settings for the VMs.	
Error	Cannot deploy upgrade agent on host.	
Error	Unable to verify host reboot. To complete the upgrade reboot the host <i>host_name</i> manually.	Reboot the host.
Error	Cannot run upgrade script on host.	
Error	Host patch <i>patch_name</i> conflicts with patch <i>patch_name</i> 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 <i>patch_name</i> conflicts with the package <i>package_name</i> 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 <i>patch_name</i> conflicts with patch <i>patch_name</i> 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 <i>patch_name</i> conflicts with the package <i>package_name</i> 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 <i>package_name</i> is successfully imported.	
Error	Import of package: <i>package_name</i> did not succeed.	
Info	<i>number_bulletins</i> 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.	

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Error	Cannot remediate the host because the removable devices cannot be disconnected from the VMs that are running on the host.	
Error	PXE booted ESXi host <i>host_name</i> is supported for staging and remediation.	
Warning	Patch <i>patch_name</i> was excluded from the stage operation because its prerequisite <i>prerequisite_name</i> 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 <i>patch_name</i> was excluded from the remediation because its prerequisite <i>prerequisite_name</i> 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 <i>host_name</i> because its power state is <i>state</i> .	
Error	Cannot stage patches to the host <i>host_name</i> because its power state is <i>state</i> .	
Error	Cannot remediate the host <i>host_name</i> because its power state is <i>state</i> .	
Error	Could not scan host <i>host_name</i> 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 stage patches to host <i>host_name</i> 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 <i>host_name</i> 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.
Info	Scanning PXE booted ESXi host <i>host_name</i> .	
Warning	Staging patches to PXE booted ESXi host <i>host_name</i> . If the host is rebooted prior to remediation of the staged patches, these patches will no longer remain staged and will be lost.	
Warning	Remediating PXE booted ESXi host <i>host_name</i> . If the host is rebooted prior to updating the image profile associated with the host, the applied patches will no longer remain installed and will be lost.	
Error	Could not download virtual appliance upgrade metadata.	
Error	Could not download virtual appliance upgrade metadata for <i>virtual_appliance_name</i> .	
Error	<i>download_URL</i> is not a valid virtual appliance download URL.	

Table 13-1. Update Manager Events (Continued)

Type	Message Text	Action
Warning	Staging patches whose installation requires a host reboot is not supported on PXE booted ESXi host <i>host_name</i> . Update your image profile.	
Warning	Remediation of PXE booted ESXi host <i>host_name</i> against patches that require a host reboot is not supported. Remove these patches from the baseline to install the patches that do not require a reboot. To install patches requiring a reboot, update your image profile.	
Info	Successfully downloaded virtual appliance upgrade metadata.	
Error	Host <i>host_name</i> cannot download files from the VMware vSphere Update Manager patch store. Check the network connectivity and firewall setup, and verify that the host can access the configured patch store.	
Error	Remediation did not succeed for <i>host_name</i> . The host could not enter maintenance mode.	
Error	Remediation did not succeed for <i>host_name</i> . The host could not exit maintenance mode.	
Error	Remediation did not succeed for <i>host_name</i> . The host did not reboot after remediation.	
Error	Remediation did not succeed for <i>host_name</i> . VMware vSphere Update Manager timed out waiting for the host to reconnect.	
Error	Remediation did not succeed for <i>host_name</i> . VMware vSphere Update Manager timed out waiting for the host to reconnect after a reboot.	
Error	Remediation did not succeed for <i>host_name</i> . Restoring the power state or device connection state for one or more virtual machines on the host did not succeed.	
Error	Remediation did not succeed for <i>host_name</i> . The patch metadata is corrupted. This might be caused by an invalid format of metadata content. You can try to re-download the patches.	
Error	Remediation did not succeed for <i>host_name</i> . There were errors while downloading one or more software packages. Check the VMware vSphere Update Manager network connectivity settings.	
Error	Remediation did not succeed for <i>host_name</i> . The host has virtual machines <i>machine</i> with connected removable media devices. This prevents the host from entering maintenance mode. Disconnect the removable devices and try again.	
Error	The patches selected for remediation on the host <i>host_name</i> depend on other patches that have conflicts.	
Error	Remediation did not succeed for <i>host_name</i> .	

Patch Repository and Virtual Appliance Upgrades

14

Update Manager stores patch and extension metadata, as well as downloaded virtual appliance upgrades in the Update Manager repository.

You can use the patch 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.

You can use the virtual appliance repository to view change log information about the virtual appliance upgrades and accept EULAs for the available upgrades.

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 repository that you want to view.

The patch repository and the virtual appliance upgrades are displayed in the Update Manager Administration view.

This chapter includes the following topics:

- [“View Available Patches and Extensions,”](#) on page 147
- [“Add and Remove Patches or Extensions from a Baseline,”](#) on page 148
- [“Host Patch Severity and Host Patch Category,”](#) on page 148
- [“Search for Patches or Extensions in the Patch Repository,”](#) on page 150
- [“View Available Virtual Appliance Upgrades and Accept EULAs,”](#) on page 151

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 on the Home page, click **Update Manager** under Solutions and Applications. 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 in the Update Manager Administration view 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 on the Home page, click **Update Manager** under Solutions and Applications. 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.

Host Patch Severity and Host Patch Category

In contrast to earlier releases, vSphere 5.0 introduces a two-level category and severity classification of patches and updates. ESXi 5.0 and later host patches have severity and category information included in the metadata, and the values for severity and category are reclassified.

ESX/ESXi 4.0 and earlier host patches have only severity information in the metadata, but not category information. Update Manager 5.0 and later translates metadata from the format for earlier patches to the reclassified format, so that earlier patches without category information are included in dynamic baselines correctly.

The Update Manager interface displays the severity and category for patches in the **Patch Repository** tab. You can use severity and category as criteria for the creation of dynamic patch baselines. Update Manager uses tags in `bulletin.xml` as the source for the value of severity and category of patches.

Severity and Category Values in Different vSphere Releases

Update Manager 5.0 and later correlates the severity and category metadata in patches for different ESX/ESXi releases so that earlier patches without category information are included in dynamic baselines correctly.

Correspondence between severity and category information in vSphere 5.x and earlier releases

Category metadata in patches is first introduced in vSphere 5.0. Severity metadata in patches have different meanings in different vSphere releases.

Table 14-1. Correspondence between Severity and Category Information in vSphere 5.x and earlier releases

Severity value in vSphere 4.x and earlier	Severity value in vSphere 5.x	Category value in vSphere 5.x
Critical	Critical	Other
Security	Critical	Security

Table 14-1. Correspondence between Severity and Category Information in vSphere 5.x and earlier releases (Continued)

Severity value in vSphere 4.x and earlier	Severity value in vSphere 5.x	Category value in vSphere 5.x
General	Moderate	Other
Everything else	Low	Other

Category values in vSphere 5.x

Update Manager provides the following category values for patches and notifications.

Security	A patch containing one or more security vulnerabilities fix and other bug fixes.
BugFix	A patch containing one or more bug fixes.
Enhancement	A patch containing hardware enablement enhancement.
Recall	A bulletin specifying the need to recall a package.
RecallFix	A bulletin to notify customers that a fix is available for the recalled VIBs.
Info	A bulletin containing generic notification about a wide range of issues.
Other	A bulletin containing updates for backward compatibility (for example, for updates without a category specified, or obsoleted categories.)

Severity values for specific categories in vSphere 5.x

The definitions of severity values differ based on the specific category.

Table 14-2. Description of severity values for specific categories

Category values in vSphere 5.x	Critical	Important	Moderate	Low
Security category	Vulnerabilities that can be exploited by an unauthenticated remote attacker or vulnerabilities that break guest or host operating system isolation. The exploitation results in the compromise of confidentiality, integrity, and availability of user data or processing resources without user interaction. Exploitation might be leveraged to propagate an Internet worm or execute arbitrary code between virtual machines and the host.	Vulnerabilities whose exploitation results in the compromise of confidentiality, integrity, or availability of user data and processing resources. Such flaws might allow local users to gain privileges, allow authenticated remote users to execute arbitrary code, or allow local or remote users to cause a denial of service.	Flaws where the ability to exploit is mitigated to a significant degree by configuration or difficulty of exploitation, but in certain deployment scenarios might still lead to some compromise of the confidentiality, integrity, or availability of user data and processing resources. These are the types of vulnerabilities that might have had a critical impact or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect unlikely configurations.	All other issues that have a security impact. Vulnerabilities where exploitation is believed to be extremely difficult, or where successful exploitation would have minimal impact.
BugFix category	The issues being fixed can potentially cause data loss or severe service disruptions.	The issues being fixed can cause certain type of devices, configuration, or component failure, such as a process failure.	The issues being fixed can cause inconsistency in operations or command failure.	The issues being fixed are considered to have low impact on product operations.
Recall, RecallFix, and Info categories	Update Manager creates an alert notification, which appears in the Notifications tab and triggers an alarm in the vSphere Client.	Update Manager creates a warning notification, which appears in the Notifications tab and triggers an alarm in the vSphere Client.	Update Manager creates an information notification, which appears in the Notifications tab.	Update Manager creates an information notification, which appears in the Notifications tab.

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.
Category	Specifies the category of patches or extensions to include.
Release 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.

NOTE With Update Manager 5.x you can sort security patches by category. In earlier vSphere releases, security patches are only classified by severity. In Update Manager 5.x, old patches that are marked as Security are classified as Category Security and Severity Critical. This ensures that earlier security-related patches appear in the predefined critical updates dynamic baseline.

- 4 Click **Find**.

If you want to clear the search field and remove the filter, click **Clear**.

The contents of the Patch Repository are filtered according to the criteria you entered.

View Available Virtual Appliance Upgrades and Accept EULAs

You can view available virtual appliance upgrades in the Update Manager Administration view.

Available virtual appliance upgrades are stored in the Update Manager repository. When you upgrade virtual appliances, you can select to which version to upgrade. You can view and filter available upgrades. You can also view change logs and accept EULAs for the available virtual appliance upgrades.

Prerequisites

Connect the vSphere Client to a vCenter Server system with which Update Manager is registered, and on the Home page, click **Update Manager** under Solutions and Applications. 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 Update Manager Administration view, click the **VA Upgrades** tab to view all available virtual appliance upgrades.
- 2 (Optional) If available, click **EULA - Not Accepted** in the **EULA** column to accept EULAs for virtual appliance upgrades.

You can accept EULAs from either the Remediation wizard or from the **VA Upgrades** tab. EULAs need to be accepted only once.
- 3 (Optional) Right-click the name of a virtual appliance and select **View change log** to view additional information in the Virtual Appliance Change Log Details window.

Common User Goals

With Update Manager, you can scan and remediate the objects in your vSphere inventory to keep them up to date with the latest updates.

The common user goals provide task flows that you can perform with Update Manager to upgrade, apply extensions and patches to your vSphere inventory objects and make them compliant against attached baselines and baseline groups.

- [Applying Patches to Hosts](#) on page 154

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 155

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 157

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 160

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 161

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 Patching Hosts Using Baseline Groups](#) on page 164

You can use baseline groups to apply upgrade and patch baselines together for upgrading and updating hosts in a single remediation operation.

- [Upgrading Virtual Appliances](#) on page 165

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 Hosts Compliant With the Most Recent Patches](#) on page 166
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 167
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 171
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.
- [Setting a Bandwidth Limit for Downloading of ESXi 5.x Patches](#) on page 173
You can limit the bandwidth used for downloading patches to ESXi 5.x hosts by using either the vSphere Client or the ESXi Shell. Limiting the patch download bandwidth prevents network congestion in slow networks.

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 9, “Configuring Update Manager,”](#) on page 59.

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.

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.

Some updates might require that the host enters maintenance mode during remediation. You should configure the Update Manager response when a host cannot enter maintenance mode. If you want to apply updates at a cluster level, you should configure the cluster settings as well. 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 71.

- 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 81. For detailed instructions about creating a dynamic patch baseline, see [“Create a Dynamic Patch Baseline,”](#) on page 81.

- 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 93.

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 97.

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 100.

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 100.

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 121.

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 122.

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.x and ESXi 5.x 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 New Download Source,”](#) on page 64.

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 66.

- 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 URL Addresses for Hosts and Virtual Appliances,”](#) on page 55.

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 167.

- 2 Configure the Update Manager host and cluster settings.

Some updates might require that the host enters maintenance mode during remediation. You should configure the Update Manager response when a host cannot enter maintenance mode. If you want to apply updates at a cluster level, you should configure the cluster settings as well. 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 71.

- 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 81. For detailed instructions about creating a dynamic patch baseline, see [“Create a Dynamic Patch Baseline,”](#) on page 81.

- 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 93.

- 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 97.

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 100.

- 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 100.

- 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 122.

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 *VMware vSphere 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 81.

- 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 93.

- 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 97.

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 100.

- 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 100.

- 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 121.

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 122.

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.

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.

- 1 Configure the Update Manager host and cluster settings.

Some updates might require that the host enters maintenance mode during remediation. You should configure the Update Manager response when a host cannot enter maintenance mode. If you want to apply updates at a cluster level, you should configure the cluster settings as well. 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 71.

- 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 66.

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 82.

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 93.

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 97.

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 100.

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 100.

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 121.

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 122 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 162

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 163

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.

You can perform orchestrated upgrades of hosts at the folder, cluster, or datacenter level.

Update Manager 5.5 supports upgrade from ESXi 4.x, ESXi 5.0 and ESXi 5.1 to ESXi 5.5 and migration from ESX 4.x to ESXi 5.5. You cannot use Update Manager to upgrade a host to ESXi 5.5 if the host was upgraded from ESX 3.x to ESX 4.x. Such hosts do not have sufficient free space in the /boot partition to support the Update Manager upgrade process. Use a scripted or interactive upgrade instead.

IMPORTANT After you have upgraded or migrated your host to ESXi 5.5, you cannot roll back to your version ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software. Back up your host configuration before performing an upgrade or migration. If the upgrade or migration fails, you can reinstall the ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 software that you upgraded or migrated from, and restore your host configuration. For more information about backing up and restoring your ESX/ESXi configuration, see *vSphere Upgrade*.

- 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 71.

- 2 Import an ESXi image (which is distributed as an ISO file) and create a host upgrade baseline.

Import an ESXi 5.5 image so that you can upgrade the hosts in your vSphere inventory. You can import a host image from the **ESXi Images** tab of the Update Manager Administration view.

For the complete procedure about importing host upgrade releases, see [“Import Host Upgrade Images and Create Host Upgrade Baselines,”](#) on page 85.

- 3 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 93.

- 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 97.

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 100.

- 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 100.

- 6 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 125.

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 91.

- 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 93.

- 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 98.

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 100.

- 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 100.

- 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 131.

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 Patching 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.

Some updates might require that the host enters maintenance mode during remediation. You should configure the Update Manager response when a host cannot enter maintenance mode. If you want to apply updates at a cluster level, you should configure the cluster settings as well. 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 71.

- 2 Import an ESXi image (which is distributed as an ISO file) and create a host upgrade baseline.

You must import an ESXi image, so that you can upgrade the hosts in your vSphere inventory. You can import ESXi images from the **ESXi Images** tab of the Update Manager Administration view.

For a complete procedure about importing ESXi images, see [“Import Host Upgrade Images and Create Host Upgrade Baselines,”](#) on page 85.

- 3 Create fixed or dynamic host patch baselines.

Dynamic patch baselines contain a set of patches, which updates automatically according to patch availability and the criteria that you specify. Fixed baselines contain only patches that 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 81. The detailed instructions about creating a dynamic patch baseline are described in [“Create a Dynamic Patch Baseline,”](#) on page 81.

- 4 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 90.

- 5 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 93.

- 6 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 97.

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 100.

- 7 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 100.

- 8 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 127.

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.

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.

This workflow describes how to upgrade the virtual appliances in your vSphere inventory. You can upgrade virtual appliances at the folder 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 87.

- 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 93.

- 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 98.

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 100.

- 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 100.

- 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 131.

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 Hosts Compliant With the Most Recent Patches

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 Updates,”](#) on page 67.

- 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 81.

- 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 93.

4 Schedule a scan.

You can schedule periodic scans of the hosts in your vSphere inventory. For a detailed description of the procedure, see [“Schedule a Scan,”](#) on page 100.

5 Schedule remediation for the hosts.

Schedule remediation tasks at times convenient for you for the hosts in your vSphere inventory. For more information about scheduling remediation, see [“Scheduling Remediation for Hosts, Virtual Machines, and Virtual Appliances,”](#) on page 133.

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 8, “Installing, Setting Up, and Using Update Manager Download Service,”](#) on page 51.

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 168

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 169

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 170

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 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 171
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 172
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_metaid)
ORDER BY r.entity_uid, u.meta_uid
```

The query displays all patches that are applicable to the scanned objects in the inventory.

Setting a Bandwidth Limit for Downloading of ESXi 5.x Patches

You can limit the bandwidth used for downloading patches to ESXi 5.x hosts by using either the vSphere Client or the ESXi Shell. Limiting the patch download bandwidth prevents network congestion in slow networks.

Note You should not limit the download bandwidth when you upgrade hosts. When you start an upgrade remediation, ESX/ESXi hosts are put into maintenance mode, and a limited download rate might cause hosts to remain in maintenance mode for an extended period of time.

Patches are software updates that address a particular issue or enhancement on the host. Update Manager downloads patches for ESXi 5.x hosts from download sources on the Internet. The download sources can be provided by VMware or third-party vendors. To patch hosts by using Update Manager, you use patch baselines.

To upgrade ESX/ESXi 4.x, ESXi 5.0 or ESXi 5.1 host to ESXi 5.5, you must upload at least one ESXi 5.5 .iso image to the Update Manager repository and create a host upgrade baseline. For more information about different types of software updates, see [“Downloading Updates and Related Metadata,”](#) on page 17.

In the Update Manager process, hosts download patches during remediation or staging operations. To prevent patch downloads from using all available bandwidth in slow networks, you can configure bandwidth throttling for ESXi 5.x hosts.

- [Limit the Update Download Bandwidth by Using the vSphere Client](#) on page 173
From the **Configuration** tab of the vSphere Client, you can set a maximum value for the bandwidth that an ESXi 5.x host uses when downloading VIBs.
- [Limit the Update Download Bandwidth by Running an esxcli Command](#) on page 174
You can set a maximum value for downloading VIBs to ESXi 5.x hosts by running an `esxcli` command.

Limit the Update Download Bandwidth by Using the vSphere Client

From the **Configuration** tab of the vSphere Client, you can set a maximum value for the bandwidth that an ESXi 5.x host uses when downloading VIBs.

Procedure

- 1 Log in to the vSphere Client.
- 2 In the vSphere inventory pane, select the ESXi 5.x host for which you want to limit the update download bandwidth.
- 3 On the **Configuration** tab, click **Advanced Settings** in the Software pane.
- 4 In the Advanced Settings window, click **UserVars**.
- 5 Type a value for `UserVars.EsximageNetRateLimit` to set the maximum rate for downloading VIBs in bytes per second.

For example, type **1048756** to limit the download rate to 1048756 bytes per second, or 1MB per second. Typing **0** removes the bandwidth limit.

Limit the Update Download Bandwidth by Running an esxcli Command

You can set a maximum value for downloading VIBs to ESXi 5.x hosts by running an `esxcli` command.

Procedure

- 1 Verify that you can run `esxcli` commands on the ESXi 5.x host.

All `esxcli` commands are available in the ESXi Shell and also included in the vCLI package. For improved security, VMware recommends you install the vCLI package or deploy the vMA virtual appliance, then run commands against your ESXi hosts, instead of running commands in the ESXi Shell itself. By default, remote command execution is disabled on an ESXi host. For more information about running `esxcli` commands or enabling remote command execution, see *Getting Started with vSphere Command-Line Interfaces*.

- 2 Run the `esxcli` command with a bandwidth limit value that suits your environment.

```
esxcli system settings advanced set -o /UserVars/EsximageNetRateLimit -i 1048756
```

The command limits the download rate to 1048756 bytes per second, or 1MB per second.

- 3 (Optional) To verify that you have set a download rate limit, run the following command.

```
esxcli system settings advanced list -o /UserVars/EsximageNetRateLimit
```

The following report appears.

```
Path: /UserVars/EsximageNetRateLimit
Type: integer
Int Value: 1048756
Default Int Value: 0
Min Value: 0
Max Value: 2147483647
String Value:
Default String Value:
Valid Characters:
Description: Set the maximum rate, in bytes/sec, for downloading
VIBs (0=no limit)
```

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:

- [“Update Manager Web Client Remains Visible in the vSphere Web Client After Uninstalling Update Manager Server,”](#) on page 176
- [“Connection Loss with Update Manager Server or vCenter Server in a Single vCenter Server System,”](#) on page 176
- [“Connection Loss with Update Manager Server or vCenter Server in a Connected Group in vCenter Linked Mode,”](#) on page 177
- [“Gather Update Manager Log Bundles,”](#) on page 178
- [“Gather Update Manager and vCenter Server Log Bundles,”](#) on page 178
- [“Log Bundle Is Not Generated,”](#) on page 178
- [“Host Extension Remediation or Staging Fails Due to Missing Prerequisites,”](#) on page 179
- [“No Baseline Updates Available,”](#) on page 179
- [“All Updates in Compliance Reports Are Displayed as Not Applicable,”](#) on page 180
- [“All Updates in Compliance Reports Are Unknown,”](#) on page 180
- [“VMware Tools Upgrade Fails if VMware Tools Is Not Installed,”](#) on page 180
- [“ESX/ESXi Host Scanning Fails,”](#) on page 181
- [“ESXi Host Upgrade Fails,”](#) on page 181
- [“The Update Manager Repository Cannot Be Deleted,”](#) on page 181
- [“Incompatible Compliance State,”](#) on page 182

Update Manager Web Client Remains Visible in the vSphere Web Client After Uninstalling Update Manager Server

After you uninstall Update Manager server, the **Update Manager** tab might remain visible under the **Monitor** tab in the vSphere Web Client.

Problem

The **Scan** and **Attach** buttons appear active, but if you click them, the following error message appears:

There was an error connecting to VMware vSphere Update Manager.

Also after uninstallation of Update Manager server, the Update Manager installation directory might still contain files. This does not affect future installations of Update Manager.

Solution

- ◆ Log out and log in to the vSphere Web Client.

The **Update Manager** tab disappears from the **Monitor** tab in the vSphere Web Client.

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 VMware and third-party Web sites.

Problem

Updates for virtual appliances and ESX/ESXi hosts might be unavailable.

Cause

- Misconfigured Web server proxy.
- Third-party servers are unavailable.
- VMware update service is unavailable.
- Poor network connectivity.

Solution

- Check the connectivity settings. For more information, see [“Change the Update Manager Network Settings,”](#) on page 61.
- Check the third-party Web sites to determine whether they are 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. 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 or that the object is not supported for scan.

Solution

Schedule a scan or manually start a scan.

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 version ESX/ESXi 4.0 or later.

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 vSphere 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 vSphere Update Manager Update Download task before performing the scan. For more information, see [“Run the VMware vSphere Update Manager Update Download Task,”](#) on page 76.

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.

The Update Manager Repository Cannot Be Deleted

When you uninstall the Update Manager server, you might want to delete the Update Manager repository.

Problem

You might not be able to delete the Update Manager repository.

Cause

The maximum number of characters that a filename (including the path) can contain on the operating system is set to 255 by default.

As part of the patch and upgrade download process, the files that Update Manager downloads in the Update Manager repository, might have paths that are deeper than the Windows `MAX_PATH`. You cannot open, edit, or delete such files, by using Windows Explorer, for example.

Map a network drive to a folder that is as deep in the folder tree of the Update Manager repository as possible. This shortens the virtual path.

IMPORTANT Ensure that you have the necessary permissions on the network drive and the Update Manager repository. Otherwise, you might not be able to delete the files from the Update Manager repository.

Solution

- ◆ Map the local folder to a network drive, in a command prompt run the following command.

```
subst Z: C:\Documents And Settings\All Users\Application Data\VMware\VMware Update Manager\data\vaupgrade\
```

For example, if the path to the folder of the Update Manager repository where Update Manager stores virtual appliance upgrades is the following: C:\Documents And Settings\All Users\Application Data\VMware\VMware Update Manager\data\vaupgrade\... , and the total length of this path exceeds 255 characters, you should map a network drive to the vaupgrade directory (inclusive) or a directory deeper.

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.

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 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

- 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 for 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

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,”](#) on page 186
- [“VUMV_UPDATES,”](#) on page 186
- [“VUMV_HOST_UPGRADES,”](#) on page 186
- [“VUMV_VA_UPGRADES,”](#) on page 187
- [“VUMV_PATCHES,”](#) on page 187
- [“VUMV_BASELINES,”](#) on page 187
- [“VUMV_BASELINE_GROUPS,”](#) on page 188
- [“VUMV_BASELINE_GROUP_MEMBERS,”](#) on page 188
- [“VUMV_PRODUCTS,”](#) on page 188
- [“VUMV_BASELINE_ENTITY,”](#) on page 189
- [“VUMV_UPDATE_PATCHES,”](#) on page 189
- [“VUMV_UPDATE_PRODUCT,”](#) on page 189
- [“VUMV_ENTITY_SCAN_HISTORY,”](#) on page 189
- [“VUMV_ENTITY_REMEDIATION_HIST,”](#) on page 190
- [“VUMV_UPDATE_PRODUCT_DETAILS,”](#) on page 190
- [“VUMV_BASELINE_UPDATE_DETAILS,”](#) on page 190
- [“VUMV_ENTITY_SCAN_RESULTS,”](#) on page 191
- [“VUMV_VMTOOLS_SCAN_RESULTS,”](#) on page 191
- [“VUMV_VMHW_SCAN_RESULTS,”](#) on page 191
- [“VUMV_VA_APPLIANCE,”](#) on page 192
- [“VUMV_VA_PRODUCTS,”](#) on page 192

VUMV_VERSION

This database view contains Update Manager version information.

Table 17-1. 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 17-2. 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 17-3. 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 17-4. 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 17-5. 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 17-6. 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 17-6. VUMV_BASELINES (Continued)

Field	Notes
TARGET_COMPONENT	Target component, such as HOST_GENERAL, VM_GENERAL, VM_TOOLS, VM_HARDWAREVERSION, or VA_GENERAL
BASLINE_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 17-7. VUMV_BASELINE_GROUPS

Field	Notes
BASLINE_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 17-8. VUMV_BASELINE_GROUP_MEMBERS

Field	Notes
BASLINE_GROUP_ID	Unique ID generated for this baseline group by the Update Manager server
BASLINE_GROUP_VERSION	Version of the baseline group
BASLINE_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 17-9. 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 17-10. VUMV_BASELINE_ENTITY

Field	Notes
BASLINE_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 17-11. 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 17-12. 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 17-13. 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 17-14. 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 17-15. 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 17-16. VUMV_BASELINE_UPDATE_DETAILS

Field	Notes
BASLINE_NAME	Baseline name
BASLINE_ID	Unique ID generated for this baseline by the Update Manager server
BASLINE_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
BASLINE_UPDATE_TYPE	Baseline type: fixed or dynamic
UPDATE_METAUID	Update meta ID
TITLE	Update title

Table 17-16. 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 17-17. 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 the latest results for VMware Tools scan.

Table 17-18. 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 information about the latest results for virtual machine hardware scan.

Table 17-19. 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 17-19. 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 17-20. 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 17-21. 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

A

- accessing, patch repository **147**
- add third-party URL, Update Manager **64**
- adding
 - baseline to baseline group **92**
 - patch to a baseline **148**
 - third-party patch source in UMDS **55**
 - third-party URL in Update Manager **64**
- alert notifications **70**
- apply extensions to hosts **160**
- apply patches to hosts **154**
- apply third-party patches **155**
- associate UMDS depot with Update Manager
 - Apache **170**
 - IIS **169**
 - portable media drive **168**
- attached baselines and groups, filtering **94**
- attaching
 - baseline **93**
 - baseline group **93**
 - baseline group in Update Manager Web Client **94**
 - baseline in Update Manager Web Client **94**
 - overview **20**

B

- baseline
 - attaching **93**
 - attaching in Update Manager Web Client **94**
 - compliance with vSphere objects **101**
 - creating **80**
 - deleting **89**
 - detaching **95**
 - detaching in Update Manager Web Client **96**
 - overview **18**
 - working with **79**
- baseline group
 - add baselines **92**
 - attaching **93**
 - attaching in Update Manager Web Client **94**
 - compliance with vSphere objects **101**
 - creating **89**
 - deleting **93**
 - detaching **95**
 - detaching in Update Manager Web Client **96**
 - editing **91**

- overview **18**
- remove baselines **92**
- working with **79**
- baseline groups, overview **20**
- baselines
 - default baselines **20**
 - no updates available **179**
 - types **19**

C

- checking for notifications **68**
- cluster, configure settings **73**
- cluster settings **71**
- common user goals **153**
- compatibility
 - Database Formats for Update Manager **26**
 - Operating Systems for Update Manager **26**
 - Update Manager and vCenter Server **26**
 - Update Manager and vSphere Client **26**
- compliance information, viewing **101**
- compliance state
 - compliant **105**
 - incompatible **105**
 - non-compliant **105**
 - of baselines **105**
 - of updates **104**
- compliance view, overview **102**
- compliance, unknown **180**
- configuring
 - cluster settings **73**
 - download sources **62**
 - host settings **72**
 - local Oracle connection **33**
 - mail sender settings **76**
 - Microsoft SQL Server 2008 R2 Express **30**
 - Microsoft SQL Server database **30**
 - network connectivity settings **61**
 - notification checks **68**
 - Oracle database **32**
 - proxy settings **66**
 - remote Oracle connection **33**
 - smart rebooting **75**
 - snapshots **70**
 - UMDS **54**
 - UMDS patch download location **54**

- update download schedule **67**
- Update Manager **59**
- Update Manager download source **16**
- Update Manager patch download location **75**
- URL for downloading VA upgrades **55**
- conflict updates **183**
- connection loss with Update Manager **176, 177**
- connection loss with vCenter Server **176, 177**
- creating
 - 32-bit DSN on 64-bit operating system **30**
 - baseline **80**
 - baseline group **89**
 - dynamic patch baseline **81**
 - extension baseline **80**
 - extension baselines **82**
 - fixed patch baseline **81**
 - host baseline group **90**
 - host upgrade baseline **84, 86**
 - new data source (ODBC) **31**
 - patch baseline **80**
 - virtual appliance upgrade baseline **87, 88**
 - virtual machine and virtual appliance baseline group **91**

D

- database
 - privileges **27**
 - setup **29**
- database views
 - VUMV_BASELINE_ENTITY **189**
 - VUMV_BASELINE_GROUP_MEMBERS **188**
 - VUMV_BASELINE_GROUPS **188**
 - VUMV_BASELINE_UPDATE_DETAILS **190**
 - VUMV_BASELINES **187**
 - VUMV_ENTITY_REMEDIATION_HIST **190**
 - VUMV_ENTITY_SCAN_HISTORY **189**
 - VUMV_ENTITY_SCAN_RESULTS **191**
 - VUMV_HOST_UPGRADES **186**
 - VUMV_PATCHES **187**
 - VUMV_PRODUCTS **188**
 - VUMV_UPDATE_PATCHES **189**
 - VUMV_UPDATE_PRODUCT **189**
 - VUMV_UPDATE_PRODUCT_DETAILS **190**
 - VUMV_UPDATES **186**
 - VUMV_VA_APPLIANCE **192**
 - VUMV_VA_PRODUCTS **192**
 - VUMV_VA_UPGRADES **187**
 - VUMV_VERSION **186**
 - VUMV_VMHW_SCAN_RESULTS **191**
 - VUMV_VMTOOLS_SCAN_RESULTS **191**

- datacenter
 - scan **99**
 - scanning **99**
- delete the repository **181**
- deleting
 - baseline **89**
 - baseline group **93**
 - ESXi images **87**
 - Update Manager repository **181**
- detaching
 - baseline **95**
 - baseline group **95, 96**
 - baseline in Update Manager Web Client **96**
- download, Update Manager **37**
- download patches, UMDS **56**
- download sources, configuring **62**
- download the Update Manager installer **37**
- download virtual appliance upgrades with UMDS **56**
- downloading metadata **17**
- DPM **71**
- DRS **71**

E

- editing
 - baseline group **91**
 - host extension baseline **84**
 - host upgrade baseline **87**
 - patch baseline **84**
 - virtual appliance upgrade baseline **89**
- enable
 - Update Manager Client **39**
 - Update Manager Web Client **40**
 - Update Manager Web Client plug-in **40**
- ESXi 5.5 **119**
- ESXi 5.x **119**
- ESXi images
 - delete **87**
 - importing **85**
 - overview **18**
- events, list of **136**
- events, viewing **135**
- export and import baselines **157**
- extension baseline, creating **80**
- extension details, overview **107**
- extensions, filtering **83**

F

- filtering
 - attached baselines and groups **94**
 - extensions **83**
 - objects in Compliance view **94**
 - patch repository **150**
 - patches **83, 150**

fixed patch baseline, creating **81**

FT **71**

G

generate database reports

overview **171**

using Microsoft Office Excel 2003 **171**

using Microsoft SQL Server query **172**

generating

Update Manager and vCenter Server log files **178**

Update Manager log bundles **178**

Update Manager log files **178**

H

HA **71**

host, scanning failure **180**

host baseline group, creating **90**

host extension baseline, editing **84**

host extension baseline, creating **82**

host extension remediation or staging fails **179**

host from a Virtual SAN cluster, maintenance mode **120**

host settings **71**

host upgrade baseline

creating **84, 86**

editing **87**

host upgrade scan messages, virtual switch **111**

host upgrade, third-party software **121**

hosts

apply extensions **160**

apply patches **154**

apply third-party patches **155**

download third-party patches **64**

download third-party patches using UMDS **55**

manually scanning **97**

manually scanning in Update Manager Web Client **98**

remediation **122**

remediation against baseline groups **127**

remediation against upgrade baseline **125**

remediation failure response **72**

scanning failure **181**

schedule scan **100**

upgrade **162**

upgrade and update **164**

upgrade failure **181**

I

identify the SQL Server authentication type **32**

import

ESXi image **85**

ESXi images **18**

patches **66**

incompatible compliance state resolution **182**

information notifications **70**

install

Update Manager Web Client **40**

Update Manager Web Client plug-in **40**

installation, database privileges **27**

installation requirements **36**

installing

UMDS **51, 52**

Update Manager **35, 36**

Update Manager Client **39**

Update Manager server **38**

introduction of, Update Manager Web Client **14**

inventory objects, update **166**

L

limit update download bandwidth, overview **173**

log bundles, generating for Update

Manager **178**

log bundles, generating for Update Manager and vCenter Server **178**

log files, generating for Update Manager **178**

log files, generating for Update Manager and vCenter Server **178**

M

mail sender settings, configuring **76**

maintaining Update Manager database **30**

missing package **183**

N

network connectivity settings, configuring **61**

not installable status **184**

notifications

overview **68**

view **69**

O

offline bundles

import **66**

overview **62**

Oracle database, configuring **32**

orchestrated upgrade

of hosts **162**

of virtual machines **163**

overview **161**

overview of

attaching **20**

baseline groups **20**

compliance view **102**

configuring Update Manager **59**

ESX host remediation **118**

- ESXi host remediation **118**
- extension details **107**
- hosts remediation **116**
- offline bundles **62**
- orchestrated upgrades **115**
- patch details **106**
- remediation **22, 115**
- scanning **21, 97**
- staging patches **22**
- UMDS **51**
- Update Manager Client **14**
- Update Manager process **15**
- Update Manager Web Client **14**
- upgrade details **107**

P

- patch baseline
 - creating **80**
 - editing **84**
- patch details, overview **106**
- patch download location
 - configuring for UMDS **54**
 - configuring for Update Manager **75**
- patch download task, running **76**
- patch fix notifications **68**
- patch recall notifications **68**
- patches
 - configure UMDS **54**
 - conflicting **183**
 - deleting **181**
 - download using UMDS **56**
 - filtering **83, 150**
 - import **66**
 - include in a baseline **148**
 - severity and category metadata **148**
 - staging **121**
 - viewing **147**
- pre-remediation check report **130**
- prerequisites, for the database **27**
- privileges **77**
- proxy settings, configuring **66**
- PXE booted ESXi hosts, enable remediation **74**

R

- remediate **119**
- remediation
 - of hosts **122, 125, 127**
 - of virtual appliances **131**
 - of virtual machines **131**
 - overview **22**
- remediation of Virtual SAN host **120**
- remediation, overview **115**

- removing, Update Manager **49**
- removing, baselines from baseline groups **92**
- restart Update Manager **76**
- roll back **131**
- running, patch download task **76**

S

- scan
 - datacenter folder **99**
 - vCenter instance **99**
- scanning
 - datacenter **99**
 - hosts **97**
 - hosts in Update Manager Web Client **98**
 - overview **21, 97**
 - schedule **100**
 - vCenter instance **99**
 - viewing results **100**
 - virtual appliance **98, 99**
 - virtual machine **98, 99**
- schedule, scanning **100**
- scheduled remediation
 - for hosts **133**
 - for virtual machines and virtual appliances **133**
- set up and use UMDS **168**
- setting up and using UMDS **53**
- severity and category, mapping **148**
- shared repository, using **64**
- smart rebooting, configuring **75**
- snapshot, configuring **70**
- staging, overview **22**
- staging patches **121**
- supported database formats **26**
- system requirements for Update Manager **25**

T

- tasks and events, viewing **135**
- testing patches **157**
- third-party URL, adding in UMDS **55**
- throttle update download bandwidth
 - command line **174**
 - vSphere Client **173**
- troubleshooting
 - baselines **179**
 - compliance **180**
 - conflicting updates **183**
 - connection loss **176, 177**
 - ESX host applicable **180**
 - ESX/ESXi host scanning failure **181**
 - ESXi host upgrade failure **181**
 - extension remediation or staging failure **179**

- generating Update Manager and vCenter Server log bundles **178**
- generating Update Manager log bundles **178**
- incompatible compliance state **182**
- log files are not generated **178**
- missing package **183**
- not installable status **184**
- scanning **180**
- unsupported upgrade **184**
- Update Manager tab **176**
- Update Manager Web Client **176**
- VMware Tools upgrade fails **180**

U

UMDS

- add third-party URL **55**
- compatibility matrix **52**
- configuring **54**
- download data **54**
- download host updates **54**
- download patches **56**
- download VA upgrades **56**
- download virtual appliance upgrades **54**
- export downloaded patches **56**
- installing **51, 52**
- overview **51**
- setting up and using **53**
- upgrading **51**
- understanding, Update Manager **13**
- uninstalling
 - Update Manager Client **49**
 - Update Manager server **49**
- uninstalling Update Manager **49**
- unsupported upgrade **184**
- update, inventory objects **166**
- update download schedule, modify **67**
- update download, overview **17**
- Update Manager
 - add third-party URL **64**
 - best practices **45**
 - common user goals **153**
 - database **29**
 - database views **185**
 - deployment configurations **45**
 - deployment models usage **47**
 - download installer **37**
 - hardware requirements **25**
 - installing **35**
 - network connectivity settings **60**
 - patch repository **147**
 - process **15**
 - recommendations **45**

- restart the service **76**
- supported Operating Systems **26**
- system requirements **25**
- understanding **13**
- uninstalling **49**
- upgrading **41**
- Update Manager PowerCLI script **157**
- Update Manager tab remains visible after
 - Update Manager server uninstallation **176**
- Update Manager Web Client **14**
- updated information **11**
- updates, deleting **181**
- upgrade
 - of hosts **162**
 - virtual machines **163**
- upgrade and update, hosts **164**
- upgrade details, overview **107**
- upgrade hosts **125**
- upgrade VMware Tools **132**
- upgrading
 - Java components **43**
 - JRE **43**
 - UMDS **51**
 - Update Manager **41**
 - Update Manager server **42**
 - Update Manager Client **43**
 - virtual appliances **165**
- using
 - Internet as a download source **63**
 - shared repository as a patch download source **64**

V

- VA upgrades, download with UMDS **56**
- vCenter instance, scanning **99**
- viewing
 - compliance information **101**
 - events **135**
 - notifications **69**
 - patches **147**
 - scan results **21, 100**
 - tasks and events **135**
- virtual appliance
 - configure URL in UMDS **55**
 - manually scan **98, 99**
 - scanning **98, 99**
 - schedule scan **100**
- virtual appliance remediation, overview **131**
- virtual appliance upgrade baseline
 - creating **87, 88**
 - editing **89**

- virtual appliance upgrades
 - accept EULA **151**
 - view available **151**
- virtual appliances, upgrade **165**
- virtual machine
 - manually scan **98, 99**
 - remediation failure **70**
 - scanning **98, 99**
 - schedule scan **100**
 - snapshot **70**
- virtual machine and virtual appliance baseline
 - group, creating **91**
- virtual machine remediation, overview **131**
- virtual machines, upgrade **163**
- Virtual SAN host remediation **120**
- VMware Tools **132**
- VMware Tools upgrade fails,
 - troubleshooting **180**
- VMware Tools upgrade on power cycle **132**
- VMware Tools, status **112**

W

- warning notifications **70**