Best Practices for Patching VMware® ESX/ESXi

VMware ESX 3.5/ESXi 3.5

The ever-increasing sophistication of today's software, whether an operating system or an enterprise application, means occasional improvements are needed to defend against new variants of security risks, provide feature enhancements, and correct bugs. These improvements can come in different forms such as patches or updates and are delivered using multiple vehicles. Software complexity may make the patch process seem complex if you are not familiar with the definitions and usage of the patching procedures and options available. VMware ESX is a complex software product that greatly benefits from the patches that VMware offers between ESX version releases.

This best practices document gives a brief explanation of patching and the different mechanisms for applying patches for the VMware ESX 3.5 product line.

Broadly speaking, there are two kinds of patching:

- Proactive patch management is intended to prevent unplanned downtime.
- Reactive patching occurs in response to an issue that is currently affecting the running system and that needs immediate relief. The most common response to an issue is to apply the latest patch or patches, which might seem capable of fixing the issue.

Either approach requires detailed investigation of the proposed fix.

This paper does not focus on the differences in detail between proactive patch management and reactive patch management. Instead, it focuses on the ESX patching model, patch packaging, and deliverables— key topics you need to understand to maintain your ESX systems.

To gain the most from this paper, you should:

- Have a basic understanding about the patching process for ESX 3.5
- Know what types of patches are available to you
- Have access to the related documentation listed in "Resources" on page 7

This paper covers the following topics:

Patch Overview

VMware releases ESX patches using two types of release vehicles: *patch releases* and *update releases*.

A patch release contains units called patch bundles or, simply, bundles and is issued approximately every month. These bundles contain only bug fixes.

An update release also contains units called bundles, but in addition it also includes a roll-up bundle. Update releases are issued approximately every quarter. The bundles in update releases contain bug fixes and also new features and hardware support. A roll-up bundle is simply an aggregate bundle, or "super bundle," that groups together a set of patch bundles. Update releases are delivered to a broader set of users, including end users and OEM vendors. Update releases are delivered as patch bundles and also as upgradeable ISO images, tarball (`.tgz`) files, and `dd` images. This paper describes how to use each of these delivery vehicles appropriately.

A patch bundle contains a set of software changes for bug fixes, new features, new hardware support, or some combination of these changes. Patch bundles contain two types of data: the metadata in XML format and the binary in RPM format. A patch bundle can contain one or more RPMs and can require you to apply one or more prior patch bundles.

To automate patching for a large set of ESX hosts, VMware provides a VMware VirtualCenter Server extension called VMware Update Manager. Update Manager enables you to apply updates and patches across ESX hosts and all managed virtual machines. See the Update Manager release notes for a list of guest operating systems that Update Manager can scan and remediate. This tool gives you the ability to create user-defined security or bug fix baselines that represent a state of compliance. As a security or VMware Infrastructure administrator, you can then compare hosts and virtual machines against these baselines to identify systems that are not in compliance. See the VMware Update Manager *Administration Guide* for details.

Patch Delivery and Packaging

VMware gives you the flexibility of choosing your patch management strategy based on your company business environment or IT master plans. If you have a larger deployment, you might opt to update ESX hosts using update releases to take advantage of additional new features and hardware support. If you have a smaller deployment, you might require only a small set of patches to be applied for known bug fixes or security protection using patch releases. The types of bundles offered in each release are listed below. See the *ESX Server 3 Patch Management Guide* for details. Pay particular attention to the section on patch naming conventions.

- Patch releases offer bundles with names that follow the patterns of these examples:

  `ESX350-200801001-BG`—a bundle for a bug fix

  `ESX350-200801002-SG`—a bundle for a security fix

- Update releases offer bundles with names that follow the patterns of these examples:

  `ESX350-200803001-UG`—a bundle for an update release

  `ESX350-200803002-UG`—a bundle for an update release

  `ESX350-Update-02`—a roll-up of bundles to bring a system up to the level of ESX 3.5 Update 2

VMware provides several alternatives to update an ESX 3.5 host to ESX 3.5 Update 1 or ESX 3.5 Update 2. The most straightforward method is to apply the `ESX350-Update-02` roll-up bundle from the update release. The other two methods involve installing either the ISO or tarball files to perform the upgrade. See the tables below for details. The results are the same whether you use the roll-up patch bundle from the update release or the corresponding ISO or tarball. However, if you are not using Update Manager, it is more convenient to jump start to a fresh ESX host by using ISO installs. Both ISO and tarball files are useful if you are upgrading a prior ESX release to the current ESX release—for example, using an ISO image to upgrade a host from ESX Server 3.0.x to ESX 3.5. The ISO image and upgrade tarball are released through the VMware Store, which requires registered customers to log in with their passwords. An ESX host that you patch with the update release roll-up patch bundle should be functionally equivalent to and physically the same as if you upgraded it using a CD created from the ISO or using the tarball from the same update release.

For the URL of the patch download page, see "Resources" on page 7.

Table 1. Deliverables in an ESX 3.5 Update Release and Their Use

Patching Options	Download Location	Installation Tool	Description	When to Use This
Patch bundles	For online updates, use Update Manager Signature Update	Update Manager	■ All patch bundles with suffix `-UG` ■ One roll-up bundle: `ESX350-Update<n>`	`-UG` bundle can be used individually for fixing specific bugs. Roll-up bundle is best used to bring a system up to an update release level. Both are applied by Update Manager..
	For offline updates, use the Download Patches page on the VMware Web site	`esxupdate`	■ All patch bundles with suffix `-UG` ■ One roll-up bundle: `ESX350-Update<n>` ■ `contents.zip`	Update Manager is not in the environment. Apply individual host updates using `esxupdate`.
ISOs	Use the Download page on the VMware Web site	Installer	Filename similar to this example: `esx-3.5.0_Update_2-110268.iso`	Fresh Install, CD upgrade.

Tarballs	Use the Download page on the VMware Web site	■ ESX Server 2.x: `upgrade.pl`
		■ ESX 3.x: `esxupdate`
			Filename similar to one of these examples:
			`upgrade-from-esx2.x-3.5.0_Update_2-110268.tar.gz`
			`upgrade-from-esx3.0.x-3.5.0_Update_2-110268.zip`
			`upgrade-from-esx3.5-3.5.0_Update_2-110268.zip`
				Upgrade from previous versions of ESX using `esxupdate` for ESX 3.x or **`upgrade.pl`** for ESX Server 2.x.

Table 2. Deliverables in an ESXi 3.5 Update Release and Their Use

Patching Options	Download Location	Installation Tool	Description	When to Use This

Patch bundles	For online updates, use Update Manager Signature Update	Update Manager	All three patch bundles with suffix `-UG`. Examples:
			`ESXe350-200808201-I-UG.zip`
			`ESXe350-200808202-T-UG.zip`
			`ESXe350-200808203-C-UG.zip`
				Update Manager is used for host remediation.

	For offline updates, use the Download Patches page on the VMware Web site	■ VMware Infrastructure Update ■ `vihostupdate (RCLI)`	One offline patch bundles with suffix `-O-UG`. Example: `ESXe350-200808201-O-UG`	Update Manager is not available. Host updates are applied using `esxupdate`.
ISOs	Use the Download page on the VMware Web site	Installer	Filename similar to this example: `VMware-VMvisor-Installer CD-3.5.0_Update_2-110271.i386.iso`	Fresh install for ESXi installable.
dd images	Internal only for OEM.	`esxddi` tool	dd image delivered to OEM directly.	OEMs deliver customized dd in their systems being shipped.

Table 3. Deliverables of an ESX 3.5 Patch Release and Their Use

Patching Options	Download Location	Installation Tool	Description	When to Use This
Patch bundles	For online updates, use Update Manager Signature Update	Update Manager	All patch bundles with suffix –BG or SG	Update Manager is used for host remediation.
	For offline updates, use the Download Patches page on the VMware Web site	esxupdate	All patch bundles with suffix –BG or SG or contents.zip	Update Manager is not in production. Use esxupdate for host remediation.

Table 4. Deliverables of an ESXi 3.5 Patch Release and Their Use

Patching Options	Download Location	Installation Tool	Description	When to Use This
Patch bundles	For online updates, use Update Manager Signature Update	Update Manager	All three patch bundles with suffix –BG or SG. Examples: ESXe350–200808201–I–BG .zip ESXe350–200808202–T–BG .zip ESXe350–200808203–C–BG .zip	Update Manager is used for host remediation.
	For offline updates, use the Download Patches page on the VMware Web site	■ VMware Infrastructure Update ■ vihostupdate (RCLI)	One offline patch bundle with suffix –O–BG. Example: ESXe350–200808201–O–BG	Update Manager is not in production. Use either RCLI or Virtual Infrastructure Update for host remediation.

Patch Preparation

Preparing your environment properly is important for a smooth and quick patching process. The recommended procedures below apply to the esxupdate or VMware Update Manager methods of patching.

Selective Patch Installation

Always apply the latest VMware–esx–scripts patch bundle first, before applying other bundles. This type of bundle contains fixes or enhancements for the esxupdate utility. Because esxupdate is invoked by Update Manager when remediating hosts, it is a good practice to patch esxupdate before patching anything else.

Effective Outage Planning

If you are installing multiple patches simultaneously to one ESX host and more than one patch requires a host reboot, you can minimize the number of host reboots.

- For installation using esxupdate, you can install patch bundles using the ––noreboot option. You can reboot the host at the end of the installation process.
- For installation using Update Manager, all bundles within a given baseline are installed prior to a host reboot. Patch install optimization is built in.

You can also take advantage of VMware Infrastructure 3 version 3.5 product features for patching. When performing host level remediation with esxupdate or Update Manager, you can use VMotion to migrate virtual machines before you install patches. When performing DRS cluster-level remediation with VMware Update Manager, patches are installed on each applicable host within the cluster. Virtual machines are automatically migrated using VMotion from the host being patched to other hosts within the cluster. The host being patched automatically enters and exits maintenance mode, and it reboots automatically if required.

Risk Mitigation

It is a good practice to have standby ESX hosts that are VMotion-compatible in the event of patch hiccups. If necessary, you can use the standby ESX host as a destination host for virtual machine migration with VMotion or as an alternative host for powering on virtual machines.

Understanding the Impact of Patching an ESX Host

The normal operations of an ESX host may be affected when you are applying patch bundles. Certain patch bundles may require the reboot of an ESX host. The description of each bundle lists the system impact, specifically the impact to the ESX host and the virtual machines running on that host. These system impacts are defined as follows:

- VM Shutdown & Host Reboot

  The virtual machines need to be powered off or migrated to other hosts with VMotion. The ESX host will enter maintenance mode during patch installation, exit maintenance mode upon completion, and then reboot. Both Update Manager and `esxupdate` will trigger entering maintenance mode. If you use Update Manager to remediate the ESX host within a DRS-enabled cluster, online virtual machines will be migrated to other hosts automatically using VMotion. Otherwise, you must manually migrate these virtual machines or shut them down.

- No VM Shutdown & No Host Reboot

  Patch installation does not affect running virtual machines, thus no shutdown nor migration with VMotion is required. The ESX host does not enter maintenance mode during patch installation.

- VM Shutdown & No Host Reboot

  Patch installation requires the host to be in maintenance mode. Running virtual machines need to be powered off or migrated to other hosts with VMotion. The ESX host will enter maintenance mode during patch installation and exit maintenance mode when patch installation completes. Both Update Manager and `esxupdate` will trigger entering maintenance mode. If the ESX host is within a DRS-enabled cluster, online virtual machines will be migrated to other hosts using VMotion. Otherwise, you must manually migrate these virtual machines or shut them down.

Patch Dependencies

In ESX 3.5 patch bundles, dependencies can exist between patch bundles. A bundle that does not require a host reboot may affect system availability if its dependent bundle requires host reboot. There are two types of bundle dependencies: supersedes and requires.

- Supersedes

  A patch bundle may have a listing of other patch bundles that it supersedes and renders obsolete. Bundles in both patch and update releases can supersede other bundles. Also by definition, all fixes contained in the ESX 3.5 Update 2 roll-up also contain the fixes from the roll-up of Update 1.

- Requires

  A patch bundle may also have a hard-coded dependency on other bundles because of a bug fix and VMware sometimes needs to release these fixes by binding several RPMs into the same patch bundle. This kind of dependency must be maintained for a period of time, usually between two update releases. This dependency is defined under `<IDList field="requires">` in the patch bundle `descriptor.xml` file. This dependency is enforced by Update Manager and `esxupdate`.

These dependencies affect only ESX 3.5 patch bundles. ESXi 3.5 patch bundles have no such dependencies.

For better organization, VMware recommends that you not include roll-up bundles and other patch bundles in the same baseline, including any Update Manager baseline. VMware recommends defining a roll-up in its own baseline. Logically a roll-up bundle brings an ESX host to a specific update release level (such as ESX 3.5 Update 1 or ESX 3.5 Update 2) and releases usually include new features and hardware support in addition to bug fixes. In large deployments where patch management is more complex, organizing your baselines in this method will increase simplicity and reduce risk.

Patching the esxupdate Utility

When patching ESX hosts using Update Manager or `esxupdate` directly, the patch bundles are applied using the `esxupdate` utility on the ESX host. Any problems in the `esxupdate` utility show up as problems with the patching process. In some cases, running `esxupdate` could potentially result in the patching process being broken into two steps. The only disadvantage of such a two-step process is that the overall patch process takes longer and it might require two ESX reboots instead of one. Nevertheless, we recommend that you take precautions against this behavior. Because the `esxupdate` utility has been fixed in ESX 3.5 Update 2, we recommend that you first update the `esxupdate` utility by applying the patch bundle that corrects it. The patch bundle that corrects `esxupdate` has a description of “Update to VMware-esx-scripts,” and in this case has a bundle ID of `ESX350-200808202-UG`. After applying this bundle, you can proceed to apply the roll-up bundles for ESX 3.5 Update 2.

Because `esxupdate` is the backbone for patch installation, it is a good practice to patch `esxupdate` before patching anything else.

Understanding the Impact of Patching an ESXi Host

ESXi host patching is different from patching an ESX host in that three bundles are delivered in any patch or update release. There are never more than three bundles in a particular release. The three patch bundles generated for an ESXi host update are for:

- Firmware
- VMware Tools
- VI Client.

Depending on which components need fixes, these three components might not all be patched in a particular patch release, but all three are included even when some contain no changes. For update releases, all three components are released together with new changes. In the packages that VMware provides, an offline bundle such as `ESX350-200806401-O-BG`—a “dash-O” bundle—always contains the latest versions of the three components.

There is no dependency mechanism in place for ESXi bundles. You should always apply all three pieces of the latest patch, especially when using Update Manager. As a best practice for Update Manager, you should use dynamic baselines, which will ensure the latest copies of these three components are installed. If you prefer to use static baselines, make sure they always include the patches with the latest release date. If you are not using Update Manager-—for example, if you can use offline bundle patching—a roll-up bundle always contains the latest patches for the three ESXi components. This roll-up bundle has a name similar to `ESX350-200806401-O-BG`. VMware commonly refers to such a bundle as a “dash-O” bundle. If your datacenter uses both Update Manager and offline patching using `vihostupdate` or VMware Infrastructure Update, you should make sure that the Update Manager baseline also contains the latest versions of all three bundles. VMware Infrastructure Update always chooses the latest version of all these three components when patching the host.

Identifying Build Numbers after Patch Install

In some cases, after patches have been installed on an ESX 3.x host, different build numbers are reported for different components of ESX Server.

VMware ESX hosts are patched according to a model in which each patch bundle updates only a few components (RPMs) of the ESX installation at a time. Not all components of the installation are upgraded during each patch installation. When a patch is applied, the build numbers of the updated components change. As a result, the ESX installation can have different components at different build numbers, depending upon which patch bundles have been applied.

You can find details in KB article "Determining Detailed Build Number Information for VMware ESX Server 3.5 and ESX Server 3.0.x Hosts."

Resources

- "Determining Detailed Build Number Information for VMware ESX Server 3.5 and ESX Server 3.0.x Hosts"
  http://kb.vmware.com/kb/1001179
- Download page on the VMware Web site
  http://www.vmware.com/download/
- Download Patches page on the VMware Web site
  http://support.vmware.com/selfsupport/download
- *ESX Server 3 Patch Management Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_esxupdate.pdf
- *ESX Server 3i Configuration Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35u2/vi3_35_25_u2_3i_server_config.pdf
- *ESX Server 3i Embedded Setup Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3i_e/r35u2/vi3_35_25_u2_3i_setup.pdf
- *Introduction to VMware Infrastructure*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_intro_vi.pdf
- Product documentation for VMware ESX and VMware ESXi
  http://www.vmware.com/support/pubs/vi_pubs.html
- VMware ESX and VMware ESXi *Resource Management Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_resource_mgmt.pdf
- VMware Infrastructure *Upgrade Guide*
  http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_upgrade_guide.pdf
- VMware Update Manager *Administration Guide*
  http://www.vmware.com/pdf/vi3_vum_10_admin_guide.pdf
- "VMware Update Manager 1.0 Update 3 Release Notes"
  http://www.vmware.com/support/vi3/doc/vi3_vum_10u3_rel_notes.html

If you have comments about this documentation, submit your feedback to: docfeedback@vmware.com

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

Revision: 20081009 Item: BP-069-PRD-01-01