

# Patch Management for ESX Server 3

Last updated: February 13, 2008.

The VMware® ESX Server 3 software maintenance utility, `esxupdate`, is a utility that efficiently updates VMware ESX Server hosts. Use it to install software updates, enforce software update policies, and track installed software. The benefits of this mechanism include smaller distribution downloads, incremental updates, ability to automate update deployment, selectability by update classification, and automatic dependency resolution.

---

**NOTE** This document deals only with the following versions of `esxupdate`:

- The version supplied with ESX Server 3.0.2
- The version in place on ESX Server 3.0.1 hosts after patch ESX-5874303 has been applied
- The version in place on ESX Server 3.0 hosts after patch ESX-1000074 has been applied

The patches listed above contain critical fixes to `esxupdate`. VMware strongly recommends that you apply the patches if you are running ESX Server software version 3.0 or 3.0.1. The patches can be downloaded from [http://www.vmware.com/download/vi/vi3\\_patches.html](http://www.vmware.com/download/vi/vi3_patches.html).

---

This technical note addresses the following topics:

- [“Introduction”](#) on page 1
- [“Recommended Updating Practices”](#) on page 2
- [“The Maintenance Utility – esxupdate”](#) on page 3
- [“Using Depots to Update Multiple ESX Servers”](#) on page 5
- [“Patch Management FAQs”](#) on page 7
- [“Conclusion”](#) on page 8
- [Example , “Providing Documentation Feedback,”](#) on page 8

## Introduction

The process of applying software updates to an ESX Server system has become complex. Each new update introduces changes into the existing system, and it is crucial to apply only the required updates in order to stay current with security fixes and minimize the changes to your software environment while doing so.

Beginning with version 3.0 of ESX Server, a new software update model was introduced to address the challenges outlined above. This update model facilitates selective application of software updates specific to a particular environment. It also provides the flexibility of staying current with security and critical updates and allowing noncritical updates to be applied at a later time.

## Software Release Type Definitions

The most up-to-date and detailed information regarding VMware support policies can be found at: <http://www.vmware.com/support/policies/>. All information contained in this technical paper is superseded by the information appearing in that Web site.

**Major Releases or Upgrades:** A major release will normally include all the bug fixes provided by releases for the previous version. In addition, it will contain fixes for critical and serious bugs discovered since the last

release, and as many fixes for noncritical bugs as is feasible within our development schedules. As appropriate, bugs identified and not fixed in the release will be documented in the Release Notes. Major Releases also provide functional enhancements. Our Product Managers are alerted to all product enhancement requests, and are responsible for setting the priorities by which requested new features are implemented (also subject to technical feasibility). The version for a major releases is identified by a change in the "x" position to the product version number, e.g., VMware Workstation 4.0 will be a new major release from VMware Workstation 3.x. Your license key for version 3.x will not work with version 4.0. Customers on full Support and Subscription are entitled to major releases as a feature of their support service. VMware Infrastructure customers, with licenses supported under Limited Support and Subscription variants of Platinum and Gold Support, must purchase major releases separately.

**Minor Releases or Updates:** Minor Releases are released regularly to provide fixes for bugs identified in current releases, and may include some minor enhancements. These minor releases go through full QA testing. Such minor releases are cumulative, so you only need to install the latest minor release to benefit from all the available bug fixes. They are usually limited to high severity bug fixes. The number in the "y" position changes in the versioning of a minor release e.g., VMware Workstation 3.1 is a minor release for VMware Workstation 3.0, and contains a number of bug fixes and support for Japanese localization and some other features. The licensing scheme typically remains the same for minor releases, e.g., your license key for 3.0 works with 3.1.

**Maintenance Releases or Updates:** A maintenance release is provided on an as needed basis, for example when a bug or a set of bugs are affecting a number of customers severely and one cannot wait for the next product update. Maintenance releases go through full quality assurance (QA) testing, and are scheduled on an as needed basis. A maintenance release is identified by a change in the "z" position of the product version, e.g., VMware GSX Server 1.0.3 for Linux is a maintenance release that supersedes VMware GSX Server 1.0.2 for Linux.

**Patch:** Software *patches* are typically issued to address one or more security fixes or critical fixes. VMware strongly recommends that you evaluate and apply these updates to your environment as soon as possible.

**Software bundle:** A collection of software packages distributed in a format compatible with the `esxupdate` utility. A bundle consists of an XML file called the "descriptor" and one or more RPM (Red Hat Package Manager) packages.

## Software Update Classification

Updates fall into three categories:

- **Security:** The patches that belong to this category fix one or more potential security vulnerabilities in the product. They should be implemented immediately to prevent the vulnerabilities from being exploited.
- **Critical:** The patches that belong to this category fix flaws in the product that can potentially cause data loss or severe service disruptions. They should be implemented immediately.
- **General fixes:** The patches that belong to this category can be fixes for minor flaws (e.g. usability issues) that potentially affect a small subset of customers or new driver updates and new small non-intrusive enhancements. These optional patches should be evaluated to determine their applicability or necessity to a particular customer before they are applied.

## Recommended Updating Practices

The recommended strategy for updating software includes these practices:

- Determine whether an update is necessary for your environment. Security fixes and critical fixes are typically the most essential.
- Analyze the risk factor of applying the update. For example, assess the virtual machine and ESX Server host downtime requirements.
- Minimize the change to your software environment whenever possible.
- Apply only those updates that address known issues in your environment.
- Keep your environment as current as possible.

## The Maintenance Utility – *esxupdate*

The *esxupdate* maintenance utility is a command of the VMware ESX Server software that applies software updates to ESX Server hosts. You can also use it to enforce software update policies and to track installed software. Run *esxupdate* from the ESX service console while you are logged on as user `root`.

You can use the *esxupdate* utility to investigate the contents of a bundle, to query the history of applied bundles on an ESX Server system, or to install a bundle.

The activity of the utility is recorded in a log file:

```
/var/log/vmware/esxupdate.log
```

## Update Workflow

The *esxupdate install* command performs the following steps:

- 1 Validates the update bundle.
- 2 Checks for prerequisites (correct ESX version, virtual machines powered off, and so on).
- 3 Checks for software dependencies.
- 4 Updates *esxupdate*, if an update is available.
- 5 Extracts the RPMs from the bundle.
- 6 Installs the RPMs.
- 7 Reboots the ESX Server, if necessary.

## Update Information

An update bundle (an XML descriptor file, a header directory, and a directory of one or more RPMs) is delivered as a tarball, with a name in the form:

```
ESX-xxxxxxx.tar.gz
```

Where `xxxxxxx` is the knowledge base article identification number for the specific patch. Retrieve information about the bundle from the VMware KB system by browsing to the appropriate URL in the form **<http://kb.vmware.com/kb/xxxxxxx>**.

You must untar this file into a convenient location in the service console file system or under an NFS mount:

```
mkdir /var/updates
mv <updatename>.tar.gz /var/updates
cd /var/updates
tar -xvzf <updatename>.tar.gz
cd <updatename>
```

To get information about this bundle, use the `info` command:

```
esxupdate info
```

If the current working directory is not the directory containing the update, you must specify the path in the command:

```
esxupdate -r file:/var/updates/<updatename> info
```

For a detailed list of all RPMs available in this bundle, include the `-l` option:

```
esxupdate -l info
```

or

```
esxupdate -l -r file:/var/updates/<updatename> info
```

## Update Installation

The `esxupdate update` command verifies the bundle and its dependencies and installs the RPMs. After the update is complete, the ESX Server system reboots, if necessary. Some updates require that all virtual machines on the host be powered off or moved elsewhere using VMotion. If this is the case, `esxupdate` does not proceed with update installation and displays an error message on the console. Virtual machines must manually be powered off, or moved by means of VMotion, before proceeding with an update.

### Installing an Update

From within the update directory, run the command by entering:

```
esxupdate update
```

To run `esxupdate` from a different directory, specify the bundle path in the command:

```
esxupdate -r file:/var/updates/<updatename> update
```

### Specifying Update Terminal Verbosity

Specify the verbosity of `esxupdate` terminal output by using the `-v` option as shown below.

```
esxupdate -v 10 -r file:/var/updates/<updatename> update
```

The default value of verbosity is 20. A verbosity value of 10 produces the most detailed reporting. The other values for controlling verbosity of `esxupdate` terminal output are:

```
10=debug
20=info
30=warning
40=error
```

The complete log file is found in:

```
/var/log/vmware/esxupdate.log
```

Each execution appends to that file. To scan the log file for summary information use:

```
grep summary /var/log/vmware/esxupdate.log
```

### Installing Successive Updates Without Rebooting

Not all updates require a reboot of the ESX Server host, but when a reboot is required, it might be convenient to apply more than one update in succession before rebooting. The release notes of each update will specify if a reboot of your ESX Server host is required. For updates where a restart of the host is required, the ESX Server host reboot can be prevented by using the `--noreboot` option. For example, you can apply a patch from the `file:/var/updates/` directory without rebooting the server as follows:

```
esxupdate --noreboot -r file:///var/updates/<updatename> update
```

If the final update in your sequence includes a reboot, do not use the `--noreboot` option on the final update, and all the changes you applied take effect. If the final patch does not include a reboot, you might have to manually reboot your ESX Server host for the changes to take effect.



**CAUTION** When applying successive updates using the `--reboot` option, your system can be left in an unstable state if any of the updates that you installed require a reboot. If you are unsure of the reboot requirements for the patches when installing successive patches, VMware recommends that you reboot the system to ensure ESX Server stability.

---

## Querying Currently Installed Updates

Use the `esxupdate` utility to query the database of installed ESX Server software. The utility can list all the RPMs in a particular bundle.

### Listing All Installed Updates

To get a list of all installed updates, execute this command in the ESX Server console:

```
esxupdate query
```

Example output for this command when no bundles have been installed is shown below:

```
Installed patches / ISOs:
----- Name ----- Install Date --- Summary ---
3.0.0-24265    01:59:33 05/11/06
```

The value in the Name column reports the release number and build number of the ESX Server software.

The output shown below is with a new update installed:

```
Installed patches / ISOs:
----- Name ----- Install Date --- Summary ---
3.0.0-24596    16:38:21 05/22/06
esx-200603     18:23:06 05/25/06 Legato Networker dependency fix
```

The value “200603” in the Name column identifies the knowledge base number of the bundle. The value in the Summary column gives a brief description of the update.

### Listing Details of Updates

To get information about a particular update, run the following command:

```
esxupdate info <updatename>
```

For a detailed list of all the RPMs installed in a particular update, use the `-l` option:

```
esxupdate -l info <updatename>
```

```
Product       : VMware ESX Server
Vendor        : VMware, Inc. (support@vmware.com)
Release       : esx-200603
Release Date  : Tue May 2 05:30:24 PDT 2006
Summary       : Legato Networker dependency fix
Description   :
```

```
    This patch satisfies the dependencies for installing Legato Networker Client in the
    service console.
```

```
Repository URL: file:/root/updates/esx-200603
Install start  : 18:22:43 05/25/06
Install finish: 18:23:06 05/25/06
RPMs installed:
  VMware-esx-X11-3.0.0-23456
  pdksh-5.2.14-21
```

## Using Depots to Update Multiple ESX Servers

The centralized depot reduces the burden of maintaining multiple copies of update bundles for multiple server deployment. The `esxupdate` utility supports three types of remote depot.

- NFS
- HTTP
- FTP

## Using an NFS Update Depot

An NFS server running in a standalone Linux machine or on an ESX Server system could function as a centralized depot. Other ESX Server systems can then mount the NFS volume and use it as a depot.

To set up an NFS server, edit the `/etc/exports` file, add the following lines, and restart the NFS service:

```
/data/updates *(ro)
```

The preceding example assumes that the bundles have been untarred into the `/data/updates` directory in the NFS server. You can customize this path.

Mount the NFS share on the local ESX Server machine using the `mount` command. In this example, the NFS share is mounted under `/data/updates`.

### Querying Bundles

To query for update information, run the following command at the ESX Server command prompt:

```
esxupdate -r file:/data/updates/<updatename> info
```

For a detailed list of all RPMs available in this bundle in addition to the above information, include the `-l` option:

```
esxupdate -l -r file:/data/<updates>/updatename info
```

### Installing Bundles

Execute the `esxupdate` command pointing to the mounted NFS depot:

```
esxupdate -r file:/data/updates/<updatename> update
```

To change the verbosity of `esxupdate` logs, use the `-v` option:

```
esxupdate -v 10 -r file:/data/updates/<updatename> update
```

## Using an HTTP Update Depot

You can set up a central server running Apache or IIS to serve untarred updates to all ESX Server systems through HTTP. The examples given below are for setting up Apache to serve updates. The `DocumentRoot` directive must point to the correct path. Set `/var/www/html/esx3` as the update depot:

```
DocumentRoot "/var/www/html"

<Directory /var/www/html/esx3>
    Options +Indexes
</Directory>
```

Other Apache directives and configuration can be left at their default values. Restart Apache after applying these changes.

### Querying Bundles

On the ESX Server, reconfigure the firewall to allow outgoing connections.

```
esxcfg-firewall --AllowOutgoing
```

The preceding command sets up ESX Server to make an HTTP connection to the update depot. To query for update information:

```
esxupdate -r http://<http server hostname>/<updatename> info
```

For a detailed list of all RPMs available in this depot, include the `-l` option in the preceding commands:

```
esxupdate -l -r http://<http server hostname>/<updatename> info
```

### Installing Updates

Execute `esxupdate` command pointing to the HTTP update depot as shown below.

```
esxupdate -r http://<http server hostname>/<updatename> update
```

To change the verbosity of `esxupdate` logs, use the `-v` option:

```
esxupdate -v 10 -r http://<http server hostname>/<updatename> update
```

## Using an FTP Update Depot

You can set up an FTP server to serve ESX Server software updates. You must point the `esxupdate` utility to this FTP server to install updates.

### Querying Bundles

On the ESX Server reconfigure the firewall to allow outgoing connections.

```
esxcfg-firewall --AllowOutgoing
```

The preceding command sets up the ESX Server system to make an FTP connection to the update depot. To query for update information, enter:

```
esxupdate -r ftp://<FTP server hostname>/<updatename> info
```

For a detailed list of all RPMs available in this depot, include the `-l` option in the preceding commands.

```
esxupdate -l -r ftp://<FTP server hostname>/<updatename> info
```

### Installing Updates

Execute `esxupdate` and point to the FTP update depot:

```
esxupdate -r ftp://<FTP server hostname>/<updatename> update
```

To change the verbosity of `esxupdate` logs, use the `-v` option:

```
esxupdate -v 10 -r ftp://<FTP server hostname>/<updatename> update
```

## Patch Management FAQs

### Can I apply patches to my ESX Server host in any order or do the patches need to be applied in sequence?

Patches for ESX Server 3.x can be applied in any order on ESX Server 3.0 hosts with patch ESX-1000074 and ESX Server 3.0.1 hosts with patch ESX-5874303. Later versions of ESX Server will include this fix and will not need a patch. With the fix, when an RPM contained in a patch is newer on the host, `esxupdate` will apply all other portions of the patch and leave the newer RPM already installed on the host untouched.

For ESX Server 3.0 and 3.0.1 hosts without the patches, package downgrade issues might occur if the updates are not applied in the chronological order in which they were issued. Refer to [KB 10230](#) for more information on the behavior of `esxupdate` in this situation.

### When an RPM on my ESX Server host has a Linux equivalent, can I use the Linux RPM to update my system?

No, VMware recommends that you only update your ESX Server host with RPMs supplied by VMware. These RPMs have been tested and are known to work with your system.

### Can I patch my ESX 3.X system with a patch that says 3.Y?

No, patches for a particular version of ESX Server host can be used only with that version. If the patch for the 3.X system does not indicate that a corresponding patch for 3.Y exists, either the issue has been fixed in 3.Y or no patch yet exists for that issue.

### Can I remove patches from my ESX Server system once they have been installed?

The `esxupdate` utility does not support rolling back or removing any type of updates. You cannot remove patches once they have been installed.

### How do I know which updates have already been applied to my system?

Use the command `esxupdate query` as described in the section “[Querying Currently Installed Updates](#)” on page 5.

### **The build number of my ESX host changed after I applied a patch. Is this normal?**

It is normal for some portions of your ESX Server software installation to change build numbers when patches are applied. For details on how to determine the build number for each of the components of your ESX Server installation, refer to [KB 1001179](#).

### **How do I know how much space is required to install a patch?**

There are two main considerations when determining the amount of space required to install a patch:

- The `/boot` directory should always have at least 32MB free.
- The disk space allocated to the Service Console should have free space of at least twice the size of the update to be installed (that is, the size of the `.tar.gz/.zip` file).
- The directory `/var/log` should have enough free space to available for the logs created during the update process.

### **The command `esxupdate -l query` returns a message that some packages are missing, duplicate or wrong versions. Is this normal?**

Following an upgrade of the ESX Server software, it is normal to see some packages reported as missing or with duplicate or wrong versions. For further details, please refer to [KB 1000760](#) for details on the packages listed for a specific upgrade.

## **Conclusion**

The new update classification and the `esxupdate` utility offer a more flexible way of updating and maintaining ESX Server systems. Fixes are more granular and the update mechanism is more modular, which minimizes the changes introduced to a software environment.

## **Providing Documentation Feedback**

If you would like to provide feedback on the accuracy or content of this document or any other document, send email to [docfeedback@vmware.com](mailto:docfeedback@vmware.com). For all other questions and comments, please consult your service representative.