

VMware® Infrastructure 3

Advanced Technical Design Guide

~and~

Advanced Operations Guide

Two books in one!



Ron Oglesby
Scott Herold
Mike Laverick

Chapter 13: Updating and Patching

GOTCHA:

As with any update downloaded from VMware's website you should use MD5sum against your download to check that it has not been corrupted during any internet download process.

During the lifetime of VI-3 it is inevitable that VMware will issue new releases, updates, and patches. Indeed they already have, from ESX 3.0.0 to 3.0.1 and VirtualCenter 2.0.0 to 2.0.1. There are three levels of release numbers from VMware which follow the convention of "Product Name" X.Y.Z:

- An increment to the X digit is classed as a *major release* and generally reflects a brand new product. Without some kind of software assurance agreement in place your old licenses will not cover a new product such as ESX 2.0.0 to ESX 3.0.0.
- An increment to the Y digit is classed as a *minor release* and mainly includes high severity patches – but can also include new features such as ESX 3.0.1 to 3.1.0.
- An increment to the Z digit is classified as a *maintenance release*, and they usually roll-up a number of bug fixes that cannot be held back for a minor release.

As with all software – if your versions are all of the same release then you should have no problems at all. If you blend your releases together you will find you may receive intermittent, unpredictable, and unusual software errors. Choosing the correct order of your update is critical for peace of mind. I would recommend this order for your updates:

1. Update VirtualCenter.
2. Update the VI Client(s).
3. Update the ESX hosts.
4. Update VMware Tools inside the VM's.

-
5. Apply any individual patches.

Depending on the software there are manual methods for processing the updates and methods which automate some of the updates. For bulk purposes, I will show you all of them so once you have mastered the manual methods you will understand the more automated methods. Automated or bulk methods exist for ESX Hosts and VMware Tools and individual patches can be scripted and chained together to ease their deployment.

Of course another way of approaching this issue is never to update VMware software and always carry out a clean installation. It's possible to evacuate the ESX host of all its VMs to other hosts in a DRS cluster by entering maintenance. Once that was completed we could power off the ESX host, and remove it from the VirtualCenter inventory. We could wipe the original ESX and re-install the new software, ideally with a kickstart script. Finally, we would add it back into the Inventory licensed and with VMotion enabled. This would leave us just with maintenance patches and upgrading VMware Tools for our VMs. It's a convoluted process that's for sure – but it does deliver the goal of clean installations without VM downtime.

Updating VirtualCenter

In the absence of later versions of VirtualCenter (2.0.1) than this book uses, I've chosen to update from VirtualCenter 2.0.0 to VirtualCenter 2.0.1. I will also assume you have followed VMware recommendations to run the License Server and VirtualCenter on the same system. If you are running VirtualCenter and SQL in VMs, I would recommend a backup or using snapshots to protect yourself during the update process.

1. Insert or attach to the VirtualCenter 2.0.1 CD/Media and begin the installation.
2. Choose VirtualCenter Management Server 2.0 from the list.

Figure 13.1 shows the message shown indicating a previous version of VirtualCenter has been discovered.

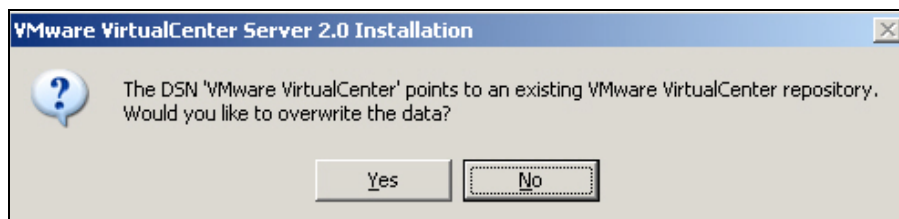
Figure 13.1



3. Choose Next.
4. Complete the installation as normal, supplying the credentials for the database.

The installer should prompt you with this message shown in Figure 13.2. Notice how you choose NO, to not over-write your data. Choosing Yes destroys your existing database!

Figure 13.2



5. Choose No.
6. The remainder of the install is followed as normal – accepting the location of your served license file specified in the previous installation.

Updating the VI Client

If you primarily use the VI Client with VirtualCenter I recommend taking the VI Client that comes with the VirtualCenter CD. After a VirtualCenter or ESX update you will receive an automatic message to update your client if you point your VI Client to a VirtualCenter server or ESX host. Personally I prefer to take this update from VirtualCenter.

1. Insert or attach to the VirtualCenter 2.0.1 CD/Media and begin the installation.
2. Choose Virtual Infrastructure Client from the options.
3. Accept the message to upgrade the client.

Updating ESX 3

There are two approaches to upgrading ESX. You can put an existing server into maintenance mode, rebooting – and update using the ESX CD-ROM installer. The installation ISO will detect the existence of an older version of ESX and then offer you an update option. For most people this method works well and is reliable. This does require physical access to the ESX host or the use of virtual media with ILOs, ILLs, or RAC cards. It also means the ESX host has to be powered off for a long period of time.

Another method allows you to update or patch an ESX host while it is powered on. However, with this approach you cannot have any running VMs on the host during the update. For this reason, the main advantage of this method is that it enables a “headless” update where physical or ILO access might be unavailable.

In this method the administrator downloads a zipped up version of the source code in a .tgz format from VMware’s website. It can be extracted and stored on a conventional storage to which the VMkernel has access such as an SAN, iSCSI, NAS, or you can give the Service Console access to an NFS, FTP, or HTTP “depot.” Depot is the term VMware uses to describe some kind of central storage point for the ROMs contained in the tgz format.

This package can be run in conjunction with ESX patch tool called esxupdate. You can learn more about patching and esxupdate by reading a very simple guide on VMware's website:

http://www.vmware.com/pdf/esx3_esxupdate.pdf

It's important you download the correct tar package. There are two. One is used with upgrades from ESX 2.x.x to ESX 3.x.x and contains an upgrade.pl script. The second is a "full" version of the product which merely contains ROMs suitable for our kind of update from one flavor of ESX 3.x.x to another.

1. **Download the tgz update file** from VMware's download page.
2. **Upload to your storage location.**

Note:

Choose a storage location which will be accessible to the ESX host. Personally, I prefer to put my update packages on an SAN location. This is wasteful from a storage perspective. I know every one of my ESX hosts will have access to it and delivery of the update will not be inhibited by my Ethernet network.

3. **Extract the tgz file** with the following:

```
tar -xzf esx-3.0.1-full-*.tgz
```

Note:

Where -X is used to extract a file(s); -z to uncompress file(s); -v with verbose information; -f force an extract even if the file has a colon in it.

4. **On the Server you wish to update**, Enter **Maintenance Mode**.

Note:

If you have DRS configured for fully-automated this should trigger a VMotion event, evacuating the ESX host of all its VMs. Alternatively, you may need to power off or manually VMotion VMs from your ESX host to other ESX hosts.

5. **Login to the Service Console** as **ROOT**.

-
6. Issue the command to force the update.

```
esxupdate -r file:/vmfs/volumes/nfs1/32039 -n  
update
```

Note: Switches

-r

is not required but does stop an unwanted warning. If you don't specify the **-r** switch you will get the warning "*INFO: No repository URL specified, going with file: <path to where you currently located>*". If you run **esxupdate** without the **-r** switch then **esxupdate** assumes you are *not* using an FTP, NFS, or HTTP deport and simply processes the files in the current directory location. If you specify **-r** you can trigger the update from anywhere on the command-line and **esxupdate** does not issue a warning about a non-specified update path.

32039

is the build number of ESX. In this case this is the build current number for ESX 3.0.1.

-n

instructs **esxupdate** not to do a reboot at the end of the installation process.

Note: End of the Update Message

At the end of the process you should find **esxupdate** ends with:

```
INFO: --- TOTALS: nnn packages installed, 0  
pending or failed, 0 excluded INFO: Install  
succeeded - please come again!
```

7. **Reboot the ESX host** – after the reboot, you may **Exit Maintenance Mode**.

Updating VMware Tools

After you have updated ESX server and have your VMs running once more – you will soon notice that VMware Tools need upgrading as well. I frequently run on old versions of VMware Tools in my development lab. I tend to move backwards and forwards from one release of ESX to another – and so I have never really bothered with keeping in synch with VMware Tools. The same cannot be said with a production environment. If you want support from VMware it's important that VMware Tools is updated, especially if you are seeking support with a guest operating system issue.

If you wish to see the status of all your VMs and their VMware Tools the easiest way of doing this is the following:

1. **Select a high-level container** such as a cluster, datacenter, or folder.
2. Select the **Virtual Machine** tab.
3. **Right-click** the **column headings**.
4. Select **Tools Status** from the list.

Note:

VMware Tools status will report information like the following:

Tools OK

Not Running

Not Installed

ToolsOld

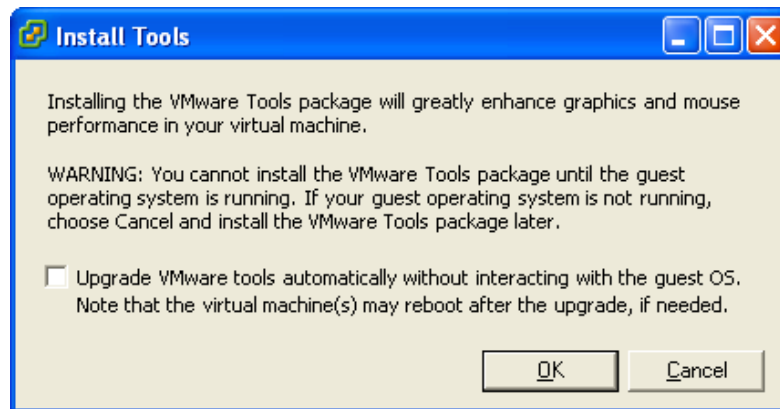
Additionally, if you look on the "Summary" tab of each VM it will state "VMware Tools: out of date."

There are two ways of upgrading VMware Tools. You can trigger a semi-automatic update while logged into VirtualCenter. The update has to be manually triggered but no interaction is required within the VM. Alternatively there is

a “bulk method” of upgrading VMware Tools from the command-line of the VirtualCenter server using a tool called vmware-vmupgrade.

Semi-Automatic Updates of VMware Tools

1. **Right-click the VM** in the Inventory.
2. Choose **Install VMware Tools**.
3. In the dialog box pop-up place a tick in the box.



Note:

You *may* need to reboot at the end of the process. I found my Windows NT4 guest did reboot, but my Windows 2003 did not.

Bulk Updates with the VirtualCenter VMware-upgrade command

VMware-upgrade will deal with VMs that report “ToolsOld” and also “Not Installed.” This “bulk method” only works for Windows guest operating systems. If it detects a Linux, Novel, Solaris, or Windows NT4 guests it will simply skip it completely. VMware-upgrade was originally designed to upgrade VMs from ESX 2.x to 3.x where both the virtual hardware and VMware Tools need to be upgraded. Fortunately, it can still be used to update ESX 3 VMs with a new version of the VMware Tools.

The only downside of the bulk update tool is you must power off your VMs beforehand. All of this is a major annoyance, but it must be remembered that a

VMware Tools install or update generally requires a reboot within the guest operating system for the update to take effect anyway.

There are a number of ways triggering the update of VMware Tools.

- **Update large numbers of VMs:**

Use a path to an ESX host held in the “Host & Clusters” view in the VirtualCenter inventory. This uses the `-h` switch in `vmware-vmupgrade`.

- **Update groups of VMs:**

Use a path to the VM held in the “Virtual Machines & Templates” view in the VirtualCenter inventory. This uses the `-n` switch in `vmware-vmupgrade`.

During an update the tools go through a number of stages. Notice at the end of the update process your VM is left in its original state – powered off. If you wish to automate this process you could look at the VirtualCenter Software Development Kit (SDK) to automate the power off before the update, trigger the update, and then power back on your VMs. Perhaps a more clumsy way which involves no scripting knowledge would be to use VMware Schedule Tasks to handle the power off and on events and Windows Scheduled Tasks to execute a batch file containing your `vmware-vmupgrade.exe` commands. Below is the list of the main stages the update tool executes:

- Find ESX host or VM in the inventory
- Confirm the VM(s) are powered off
- Sets a VMware Tools update
- Powers on VM (adjustable using the `-m` switch)
- Trigger a VMware Tools update inside the powered on VM
- Power off the VM (adjustable with the `-t` switch)

Per-ESX Host based VMware Tools Update

1. Power down the VMs you wish to update.
2. Logon to the VirtualCenter Server.

Note:

It is possible to use Microsoft's Remote Desktop Connection software if you have enabled it on your VirtualCenter server.

3. Open a command prompt to the following:

```
C:\Program Files\VMware\VMware VirtualCenter  
2.0
```

4. Type (all one command):

```
vmware-vmupgrade.exe -u vi3book\administrator -  
p vmware -h "London DataCenter/Intel  
Hosts/Intel Cluster/esx1.vi3book.com" -m 2 -t  
10
```

Note:

The lines above have been wrapped for readability – when you type the command it should be one continuous line of text.

The switches `-u` and `-p` are required, and they set the user name and password to authenticate against VirtualCenter. The `-h` switch is also required, and it sets the path to an ESX host within the Inventory. In this case all powered off VMs running on `esx1.vi3book.com` will be updated.

The switches `-m` and `-t` are optional and set how many VMs can be simultaneously updated and how long VMs are allowed to stay powered on (in minutes). This deals with the issue of VMs that will not power down gracefully.

Per-VM based VMware Tools Update

1. Power down the VMs you wish to update.
2. Logon to the VirtualCenter Server.

-
3. Open a command prompt to the following:

```
C:\Program Files\VMware\VMware VirtualCenter  
2.0
```

4. Type (all one command):

```
vmware-vmupgrade.exe  
-u vi3book\administrator -p vmware  
-n "London DataCenter/Mike's VM's/vm1"  
-n "London DataCenter/Mike's VM's/vm2"  
-n "London DataCenter/Mike's VM's/vm3"  
-n "London DataCenter/Mike's VM's/vm4"  
-n "London DataCenter/Mike's VM's/vm5"  
-n "London DataCenter/Mike's VM's/vm6"
```

Note:

As you can see, with the `-n` switch we can specify multiple VMs, and yes, you must specify `-n` each and every time!

Unfortunately, in this release it is not possible to specify simply a folder or have VirtualCenter assume that every VM in that folder (and subfolder) is updated with a new Version of VMware Tools.

GOTCHAS:

There are some frequent errors people see with `vmware-vmupgrade`. Firstly, remember the VMs have to be powered off first. If not the tool will give you this error message:

"London DataCenter/Mike's VM's/vm1: Cannot upgrade. VM is not powered-off"

Secondly, people often forget to input the `/` to indicate the end of one object in the VirtualCenter inventory and the start of another. If you do this you will get the following type of error message:

"Failed to upgrade: failed to find object at London DataCenter\Mike's VM's\vm1"

Lastly, the most common error is failing to authenticate with VirtualCenter correctly:

“Failed to connect to VirtualCenter server: vim.fault.InvalidLogin”

Patching ESX

Currently, individual patches are free to download from VMware’s website. They come in three flavors:

- **Security**

These patches prevent a potential security breach and should be installed immediately.

- **Critical**

These patches prevent data loss or service failures and should be installed immediately.

- **General**

These patches are non-urgent and affect a small number of users. They include bug fixes and driver updates. You should assess the relevance of these updates before downloading and applying them.

If you wish to use esxupdate to apply these patches – you need to download the versions compatible with the tool. Generally they contain two files – a descriptor file in an XML format and an RPM file, and we can use a script to chain the various updates together. With each patch for ESX server you will be given an advisory on whether powering off the VMs is required or a reboot of the ESX host is required. They are currently phrased in this way:

“All virtual machines on the host must be either shut down or migrated using VMotion before applying the patch. No reboot of the ESX Server Host is required after applying this patch.”

Or

“There is no need to shut down the virtual machines on the host or to migrate them using VMotion before applying the patch. No reboot of the ESX Server Host is required after applying this patch.”

Or

“All virtual machines on the host must be either shut down or migrated using VMotion before applying the patch. A reboot of the ESX Server Host is required after applying this patch.”

It’s actually quite difficult to remember this differing advice especially if you are planning to do a bulk update. So I feel it’s probably safest to take a conservative approach and say that no update to the ESX host is executed without first entering maintenance mode – followed by an ESX host reboot.

Manual Case-by-Case Patching

1. Download the patches from VMware’s website you wish to apply.

Note:

These are currently held here:

http://www.vmware.com/download/vi/vi3_patches.html

2. Upload to a central storage location (SAN, iSCSI, NAS, FTP or HTTP).
3. At the Service Console untar the update with the following:

```
tar -xvzf ESX-nnnnnnnn.tgz
```

4. To find more information about the patch you can use the `esxupdate` command to read its info and xml file with the following:

```
esxupdate -r  
file:/vmfs/volumes/nfs1/patches/ESX-5031800 -l  
info
```

Note:

This return information is formatted as follows:

```
Product           : VMware ESX Server
Vendor            : VMware, Inc. (support@vmware.com)
Release:          : ESX-5031800
Release Date      : Mon Feb  5 13:54:51
                  : PST 2007
Summary           : RHSA-2006:0749 tar
                  : security update
Description       :
This patch contains Red Hat security fix for
tar command.
```

CVE-2006-6097: GNU tar 1.16 and 1.15.1, and possibly other versions, allows user-assisted attackers to overwrite arbitrary files via a tar file that contains a GNUTYPE_NAMES record with a symbolic link. This is not properly handled by the `extract_archive` function in `extract.c` and `extract_mangle` function in `mangle.c`.

```
Upgrade paths     : 3.0.1-32039
Repository URL    :
file:/vmfs/volumes/nfs1/ESX-5031800
RPMs included     : tar-1.13.25-15.RHEL3
```

5. To install the update use the following:

```
esxupdate -r
file:/vmfs/volumes/nfs1/patches/ESX-5031800 update
```

Bulk ESX Patching

Forum and London User Group member Michael Knight has created a script which will untar the patches for you and then put them in date order – and then apply the patches in bulk. You can download this script from <http://www.rtfm-ed.co.uk> which is held under the “Useful Tools” section of the site.

To use Michael’s script make sure you download your tar files to /var/updates directory and then execute the script. Alternatively, you can edit the script to specify the required path.

Summary

Generally, VMware software is very reliable and very secure. However, like any software vendor errors and bugs are bound to happen. In this chapter we have addressed the issue of patching and updating VI-3 from the perspective of automating the process as much as possible with VMware scripts and tools such as esxupdate and vmware-vmupgrade. We have also seen how many of these tasks can be automated using scripts that are freely available on the Internet.