RTFM Education

Beyond the Manual... with Mike Laverick

By Mike Laverick



and

vi3book.com


For Errors/Corrections please contact:

mikelaverick@rtfm-ed.co.uk

# Appendix C: What's New and Different in VI 3.5

**WARNING:**
This appendix was written whilst ESX 3.5 and VirtualCenter 2.5 were still in a Beta and Release Candidate format. As a consequence of the terms and conditions of the VI 3.5 Beta Programme it was at the time impossible to include information about this in the VI-3 book without breaching the very same terms and conditions that allowed this appendix to be written.

One of the challenges of writing a book in the technical arena is that software is constantly evolving and changing – VMware is no different in this respect. That said 99% of what has been written in the core chapters of the VI-3 book still applies to the new release.

As you might expect software changes can be introduced between Beta/Release Candidate and the "General Availability" of the product. As this appendix will be released the day VI-3.5 reaches GA you may indeed find discrepancies in the document when compared to the GA. It will be updated and re-released as differences are discovered.

**Usage Notice:**
Due to the lack of a Service Console in VMware ESX Server 3i, any references to usage of the esxcfg-* commands *do not* apply to that product.

**Expected Audience:**
This appendix is in tended to be read by two types of reader. The first type of reader will be those who have bought the VI-3 Book and discovered differences between ESX 3.0.x and ESX 3.5 and VirtualCenter 2.0.x and VirtualCenter 2.5. The second type of reader is one who is already very familiar with the VI-3.0.x product and merely wishes to know the differences between it and VI-3.5.

**Terminology:**
Right now it doesn't seem horribly clear what the actual name will be of ESX 3i. It's like to end up with many names. But for clarity I will be using ESX 3i to describe the version of ESX that lacks the full Service Console. Some alternative names of ESX 3i are:

- VMware Embedded ESX Server 3.5
- VMware Hypervisor
- ESX 3i
- ESX 3i 3.5
- ESX HW (Hardware) – used at the Alpha Stage

The functionality covered in this appendix was tested against both ESX 3.5 and the ESX 3i platforms. However, as it is unclear at this stage how quickly ESX 3i will be adopted, I decide to write about ESX 3i in detail in a different appendix.

**What this guide doesn't do:**
This guide is about updating skills and knowledge. It does not cover upgrading an existing ESX 3.0.x and VirtualCenter 2.0.x environment. I will write a separate guide on this subject once VI-3.5 has released for general availability.

## *VI 3.5 Licensing*

VMware have made a number of subtle but significant changes to their licensing. What has not changed is licensing ESX host by the number of completed sockets, so it is still no more expensive to use single core, dual core or quad core servers. VMware has release guidelines on

pricing per socket – but these could change in the run up to the GA. This said the structure of the licensing model is likely to remain unchanged.

The product can now be purchased in four main ways:

- ESX 3i Only
- ESX Foundation
- Standard
- Enterprise
- VirtualCenter Foundation

The ESX 3i product will in most cases ship "embedded" to new servers. However, ESX 3i can be purchased separately from a server. This version runs from a hard-drive as opposed to being embedded in memory. If purchased in this stand-alone version for installation to hard-drive VMware will charge $495 per socket.

The Foundation Edition of VI 3.5 replaces what was previously known as the "Started Edition". Previously the Starter Edition had a number of very useful features disabled. The Foundation Edition is a much more attractive proposition as it will include ESX 3.5, ESX 3i, VCB and the new VMware "Update Manager". Additionally, there will be no restrictions on the amount memory or CPUs addressable. Critically, there will be no restrictions on the type of storage you choose to use. VMware have stated the list price will be $995 for two sockets. You can see the Foundation Edition as VMware's reaction to the customer demand for a version of VI-3 that is attractive to midsize and smaller IT departments. Additionally, there is also a VirtualCenter Foundation edition which is limited to managing three ESX nodes. This is designed for those smaller environments that want to have access to DRS and HA.

The Standard Edition will include all the features of the Foundation Edition. Additionally, it will support VMware's HA Clustering feature – and will be priced at $2,995 for two sockets.

Finally, the Enterprise Edition will include all the features of Standard Edition and will include VMotion and brand new features such as "Storage VMotion" and "Distributed Power Management". These new features can still bought separately "a la carte" and bolted into a Standard Edition purchase. The Enterprise Edition has a list price of $5,750 for two sockets.

As with the upgrade from ESX 2.x.x to ESX 3.x.x customers who have a valid SnS contracts will get features for which they have an existing license for free. This means existing enterprise customers will qualify for a free upgrade to the VI 3.5 Enterprise Edition with the new features at no additional cost.

ESX 3i and 3.5 have significant improvements from hardware and performance perspectives including:

- VMware now support 128GB RAM in a server, and 256GB is experimentally supported.
- There is also experimental support for up to 64 logical processors.
- SATA drives are now supported for hosting VMFS volumes
- 10-Gigabit Ethernet
- Infiniband
- Virtual Machine hardware "enlightenments" such as NPIV, MMU and NPT. These are hardware improvements which the VM is now aware of
- 64GB RAM to the VM

From early analysis it appears that VMware have modified the terms they use to describe license files. Although the terms have changed, the license files function in the same way. VMware have dropped from the terms "Host" LIC files and "Served" LIC files. These terms have been replaced with "Single Host" and "Central_VCMS". Occasionally, customers have found the terms host and served confusing, and this change is intended to be make the terms more intuitive. Single host

LIC files are used with ESX managed without VirtualCenter, and "Central_VCMS" licenses are intended to be used with VirtualCenter and the VMware License Server.

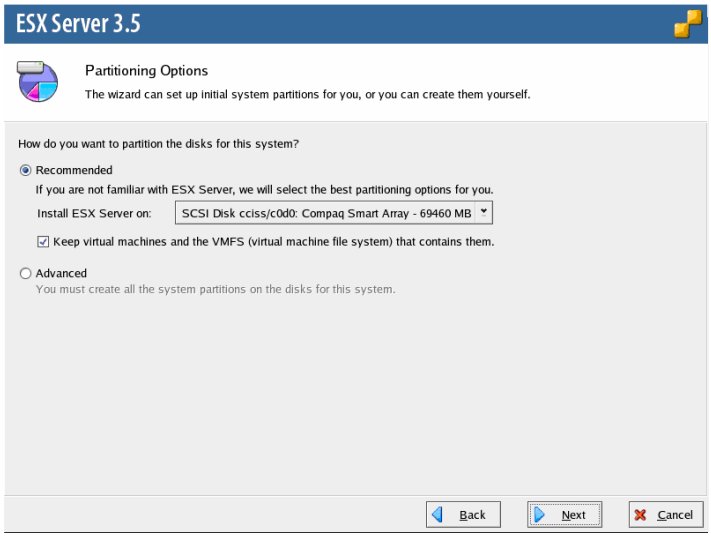
# *ESX Installation*

Despite these significant changes to the capacity and functionality of ESX, there are comparatively few if any changes in the install routine. If you have been keeping up with the various maintenance releases most of these changes were introduced in ESX 3.0.2.

The first major change is to the "Partitioning Options" page shown in Figure C.1. In previous releases the option to "Keep virtual machines and the VMFS" was not by default selected. In the ESX 3.0.2 and ESX 3.5 this is now selected. As you might recall from the installation chapter this option is designed for people re-installing ESX who wish retain VMs which are stored locally.

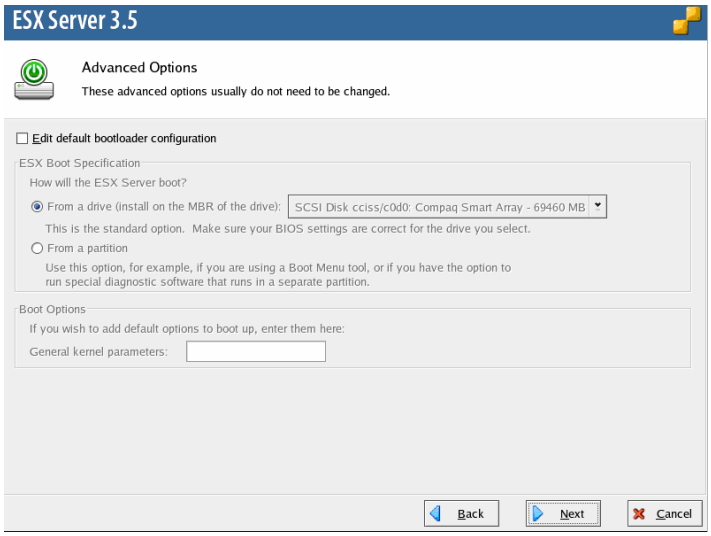
Additionally, if you decide to use the option "Recommended" partition scheme you find the local VMFS volume is no longer labeled "storage1" but is a string which is a concatenation of the ESX host name and storage1 e.g. esx1:storage. This has been implemented to ensure that both the volume name and data store label are unique to the ESX host and VirtualCenter. In ESX 3i the naming convention for the automatic VMFS volume created on a blank system is "datastore1".

**Figure C.1**




The second major change in the installation procedure is the location of the Master Boot Record shown in Figure C.2. In most cases the MBR should be located on the same LUN you selected for the partition table (the drop-down list in Figure C.1). This is now assumed as part of the installation. If you choose a local LUN the MBR will be on a local LUN, and if you select a SAN based LUN (for diskless SAN booting) the MBR will be on the SAN LUN, selected in the "Partition Options" page. You should have no real need to enable the "Edit default bootloader configuration". This modification of the installer is a good one from VMware as it will reduce the chances of incorrectly installing the MBR and thus causing boot problems immediately after the ESX installation.

**Figure C.2**




## Post ESX Install

After installing ESX you might want to use a web-browser to visit the ESX hosts "welcome" web-page. From here you can download and install the latest VI Client (Version 2.5). There is nothing especially new here except there is a new link in the right-hand side of the page. This link allows you to browse the data stores available on that ESX host. Interestingly, in the release candidate I was not asked to authenticate before using this featre. Figure C.3 shows this new option.

**Figure C.3**


On the same page you will see there is a link to use the "Scripted Installer". However, the scripted installer web-pages are still disabled. It has to be enabled using the method outlined in Chapter 12: ESX on the Command-Line of the VI-3 book. On the subject of scripted installations, I found in my tests that the scripted installations I used to deploy ESX 3.0.0, 3.0.1 and 3.0.2 worked with very few modifications or revisions with ESX 3.5. However, what differences I did discover I have documented below.

# *ESX Scripted Installations*

As part of my testing, I took my kickstart scripts used to deploy ESX 3.0.x and used them unmodified to script the installation of ESX 3.5. This was primarily to test that the "Ultimate Deployment Appliance" (UDA) that I use to deploy ESX still worked with the new version of ESX. For those who don't know the UDA is a virtual appliance created by Carl Thijssen of the Netherlands. It allows you to press F12 when a physical or virtual machine boots and use the PXE boot method to deploy many different operating systems including ESX.

http://www.ultimatedeployment.org
http://www.rtfm-ed.co.uk/?page_id=366

## Networking Changes in Kickstart Scripts

Kickstart scripts automate the manual tasks of configuring an ESX host including the creation of virtual switches. One thing I did notice is that default behavior for NIC Team has altered in ESX 3.5. In ESX 3.0.x a vSwitch created with esxcfg-vswitch that is allocated two physical NICs retained the default load-balancing policy of "Route based on the originating virtual port ID". However, with ESX 3.5 the default changed. Although the policy still states "Route based on the originating virtual port ID" the NICS are actually allocated in an Active/Standby method. Figure C.4 and C.5 shows the configuration in question. It's not clear at this juncture whether this is a bug. I found that using the esxcfg-vswitch commands manually produced the same result.

**Figure C.4**

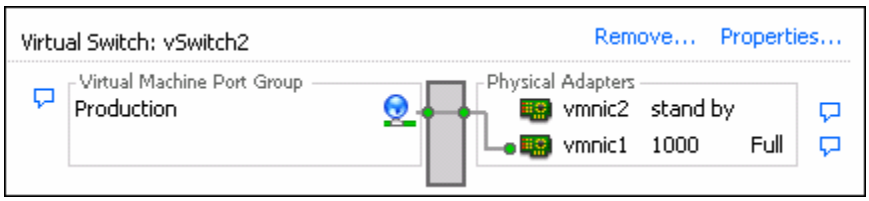
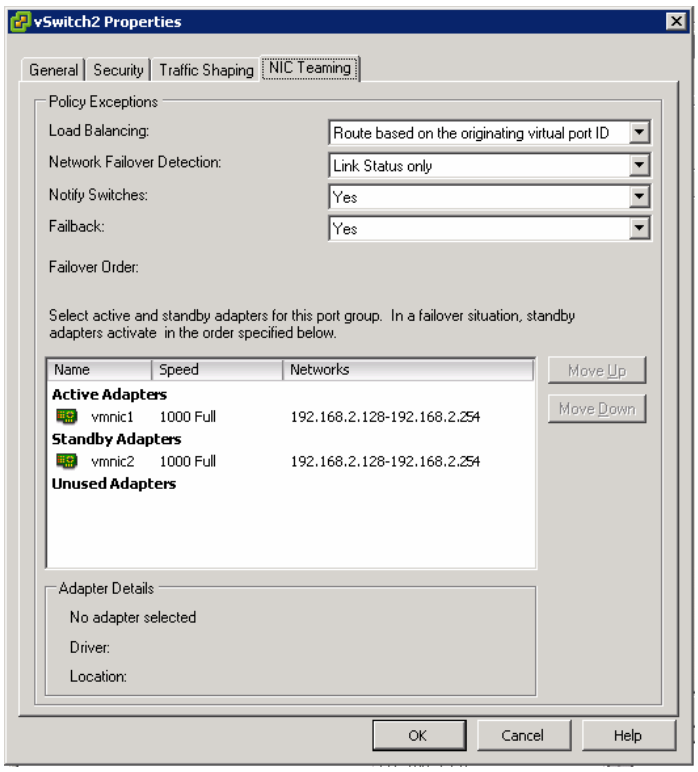



**Figure C.5**




**Note:**
A vSwitch created manually via the VI Client with two or more physical switches continues to default to being active/active and use the policy of "Route based on originating virtual port ID.

## Enabling VMotion in Kickstart Scripts

In the past I had enabled VMotion using the largely undocumented vimsh command. For example:

**vimsh -n -e "/hostsvc/vmotion/vnic_set portgroup4"**

Unfortunately, the syntax of vimsh has changed. vimsh in ESX 3.0.x uses the "internal ID" of the portgroup and this value was viewable in previous releases using the esxcfg-vswitch –l command. This value is no longer displayed in ESX 3.5.

A new naming convention exists which makes reference to the "Device". Each VMkernel Port created generates a "virtual device" ID with the naming of vmk0, vmk1. The values are serialized so your first VMkernel Port Group would be vmk0, and second VMkernel Port Group would be vmk1. The correct syntax is now:

**vimsh -n -e "hostsvc/vmotion/vnic_set vmk0"**

If you are unsure of the correct vmk value, then after you have scripted the creation of your vSwitches open a command-prompt on the ESX host and enter the vimsh interactive shell by typing the command on its on:

**vimsh**

Then type:

**hostsvc/vmotion/netconfig_get**

This will create the output below which allows you to identify the vmk value

**Sample Output from netconfig_get:**

```
(vim.host.VMotionSystem.NetConfig) {
  dynamicType = <unset>,
  candidateVnic = (vim.host.VirtualNic) [
    (vim.host.VirtualNic) {
      dynamicType = <unset>,
      device = "vmk0",
      key = "key-vim.host.VirtualNic-vmk0",
      portgroup = "VMotion",
      spec = (vim.host.VirtualNic.Specification) {
        dynamicType = <unset>,
        ip = (vim.host.IpConfig) {
          dynamicType = <unset>,
          dhcp = false,
          ipAddress = "10.0.0.3",
          subnetMask = "255.255.255.0",
        },
        mac = "00:50:56:6f:ba:6b",
      },
      port = <unset>,
    },
    (vim.host.VirtualNic) {
      dynamicType = <unset>,
      device = "vmk1",
      key = "key-vim.host.VirtualNic-vmk1",
      portgroup = "iSCSI",
      spec = (vim.host.VirtualNic.Specification) {
        dynamicType = <unset>,
        ip = (vim.host.IpConfig) {
          dynamicType = <unset>,
          dhcp = false,
          ipAddress = "172.168.3.203",
          subnetMask = "255.255.255.0",
```

```
        },
        mac = "00:50:56:6c:bf:c0",
      },
      port = <unset>,
    }
  ],
  selectedVnic = <vim.host.VirtualNic:key-vim.host.VirtualNic-vmk0>,
}
```

## Enabling the ISCSI Software Initiator in Kickstart Scripts

Enabling the iSCSI Software Initiator no longer by default opens the iSCSI port of 3260 on the firewall. This now has to be done using the command:

**esxcfg-firewall -e swISCSIClient**

Additionally, the iSCSI Software Initiator device name has changed. In ESX 3.0.x the HBA was referred to as vmhba40, it is now referred on as vmhba32. This means that if you use the vmkiscsi-tool to set the iSCSI target values the syntax of the command would be something like

**vmkiscsi-tool -D -a** 172.168.3.99 **vmhba32**

## Creating local VMFS Volumes in Kickstart Scripts

In previous releases it was possible to create a VMFS partition using the part entry in the partitioning section of kickstart script. For example:

**part None --fstype vmfs3 --size 1 --grow --ondisk=cciss/c0d0**

However, ESX 3.0.x would create the partition but would not format it, as result many people would use the vmkfstools command to format the volume on first boot up with something like:

**vmkfstools -C vmfs3 -S** esx1_localstorage **vmhba0:0:0:9**

Whilst this will still work in kickstart scripts it isn't really required as the installer now automatically formats the local VMFS volume for you on first boot up, and automatically imposes the volume and datastore label convention of:

**hostname:storage1** e.g. esx1:storage1

It can be deleted after the installation if you wish to prevent end-users creating VMs on local storage.

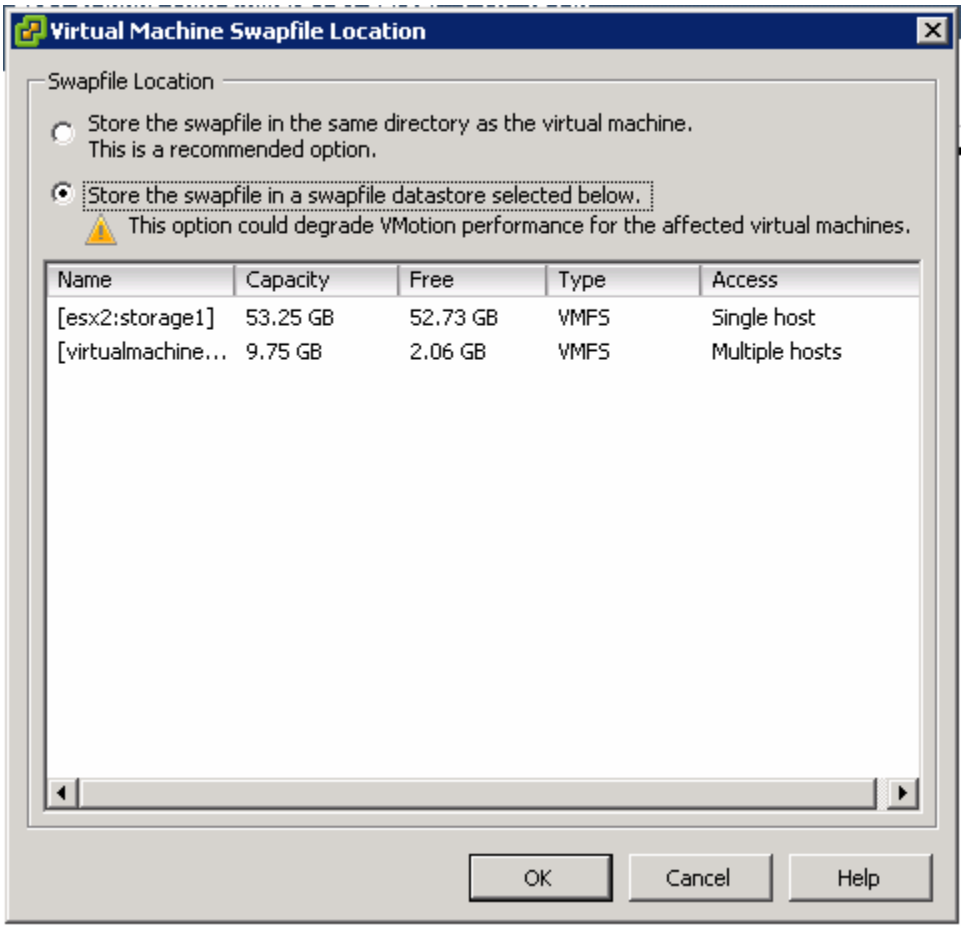
## The VMkernel Swap File

With release of ESX 3.0.x the location and nature of the VMkernel Swap file changed considerably. In ESX 2.x.x the VMkernel Swap file was manually created per-ESX host on local storage. In ESX 3.x.x the VMKernel swap is dynamically created per-VM based on the difference between the VMs "Limit" and "Reservation" value – this has not changed with ESX 3.5. So if you give a VM a 1GB limit and 256MB reservation the swap file created will be 768MB in size. This VM-swap file is created on the fly in the VMFS volume where the VMs VMX file is located. ESX3i and ESX 3.5 allow this location to be modified. However, you must be careful where you relocate your swapfile to, as this could affect VMotion. You can change the VMkernel Swap file location using the following steps:

1. Select the **Configuration Tab**, and in the **Software pane** choose option **Virtual Machine Swapfile Location**
2. Click the **Edit…** option on the right-hand corner of the VI Client

3. In the dialog box select the option "**Store the swapfile in a swapfile datastore selected below**". Figure C.6 shows the Virtual Machine Swapfile Location dialog box

**Figure C.6**




**Note:**
Notice the recommendation from VMware is accept the default location of the swapfile. You will find in other areas of the product that you are now asked for you prefered location of the swapfile – for example in creating a DRS cluster

# *Installing the VI Client*

If you read the appendix on using ESX3i you will find the install of VI client from an ESX 3.5 host – looks and feels exactly the same. As with the ESX3i VI Client installation, if Microsoft .NET 2.0 is not installed on your management PC, then the VI Client will install it for you.

After the installation is over and the VI Client is loaded, you will receive a number of certificate pop-ups. Those of you have experience going back to ESX 2.x.x will find this very familiar territory. Back then management was carried out via a web-browser and a web-server ran on each and every ESX host, and VMware used "auto-generated" SSL certificates to ensure your management activity was not open to hackers capturing unencrypted network traffic. The same applies with ESX 3.5 and ESX 3i. These certificates are generated by VMware and do match the ESX and VirtualCenter host name.

However, they are still "untrusted" as they are created by internal processes during the ESX installation. So a little bit of management has to be carried to remove the odd annoying pop-ups such as installing the certificate into your management PC and ignoring any future warnings. Anyone familiar with Windows should be familiar with accepting these types of pop-ups and

carrying out the necessary tick-off boxes to prevent them happening again. This is very much like accepting the RSA Key pop messages from SSH clients like PuTTy.

# *VirtualCenter Installation*

The look and feel of VirtualCenter installation has changed quite significantly from previous releases. None of these changes individually add-up to major change in the setup of VirtualCenter – but collectively they do add-up. With that said, essentially the goal of the install is still one of configuring a Windows Service (vpxd) to speak to a "backend" database (SQL, SQL Express or Oracle) by using Microsoft's Data Source Name (ODBC DSN Management) system and database driver (Microsoft MDAC or Oracle's NetClient). These database systems have their own service pack requirements outlined below

- Microsoft SQL
  - Microsoft SQL Server 2000 Standard edition (SP4)
  - Microsoft SQL Server 2000 Enterprise edition (SP4)
  - Microsoft SQL Server 2005 Enterprise edition (SP1)
  - Microsoft SQL Server 2005 Enterprise edition (SP2)

- Oracle
  - Oracle 9i release 2 Standard edition
  - Oracle 9i release 2 Enterprise edition
  - Oracle 10g Standard edition
  - Oracle 10g Enterprise edition

It's perhaps worth me giving you a quick high-level view of these VirtualCenter installation changes before running the setup program

- The installer no longer has a button to open the Microsoft ODBC Administration tool. DSN setting must be configured for the relevant database(s) before starting the VirtualCenter installation
- VMware has removed support for MSDE evaluation and demonstration purposes and has replaced it with support for Microsoft SQL Express. However, Microsoft SQL Express is not supported for production environments; merely for test and demonstration purposes.
- VirtualCenter can be installed on its own – or used to install other integrated components including the VI Client, Update Manager, VMware Converter
- The Update Manger is responsible for patching ESX, Virtual Machines and VI Clients and has its own database for tracking the patching process and storage location for holding the patches themselves
- The Update Manager includes options to set port numbers and internet connections (proxy server settings and so on) to allow the download of patches
- VirtualCenter and Update Manager can be installed together or separately. Personally, I have more success with Update Manager on a separate Windows instance
- VirtualCenter supports both Windows NT (Windows Authentication) and SQL Authentication. But it is still the case that Windows NT authentication is not supported for a remote SQL server, it is only support if the VirtualCenter server also runs a SQL instance locally
- The installer now asks for authentication credentials for installation of VirtualCenter "extensions" which are third-party plug-ins to VirtualCenter. VMware Converter and Update Manager each have "plugins" which extend the VI Client, adding new buttons and menu options
- There are a number of warning pop-ups to alert the operator to check that the SQL Agent is running and that transaction logs on the SQL or Oracle database need to be properly managed. These pop message also appeared in the VirtualCenter 2.0.2 installation

I felt these differences were significant to run through the entire VirtualCenter setup again from scratch. Apologies if you find this overly repeats the information in the main chapter on the VirtualCenter setup, but I want this appendix to be complete

## Configuring Microsoft SQL Server for VirtualCenter

If you carrying out a full VirtualCenter 2.5 installation you will need two databases: one for VirtualCenter and one for the new VMware Update Manager Service

At the **SQL Server**

1. Open **Enterprise Admins**, and Expand **+ Microsoft SQL Servers, + SQL Server Group, + (Local) (Windows NT)**
2. **Right-click the Database folder**, and choose **New Database** and type: **vc-db** (or something similar/appropriate) – and choose **OK**

3. Expand the **+ Security** tab, and **right-click Logins**, and choose **New Login**
4. **Browse with … button** to select the account created for VirtualCenter database…
5. Choose the option **SQL Server Authentication** and type in the password for the VirtualCenter Database User
6. and set the **Default Database** to be the database created at point 2
7. Click the **Database Access** tab, **Permit** access for the database, for VirtualCenter Database User, also enable the permission **db_owner** – and choose **OK**
8. Click **OK**, and Confirm the password again

   **Note:**
   Repeat this process for the Update Manager Service database, perhaps calling vmware-updateDB. I used the same database user account to authenticate to both databases

## Configuring VirtualCenter with Microsoft DSN

Previous VirtualCenter installations had a button in the installer to load the Data Sources (ODBC) manager. This Microsoft Management tool is used to configure DSN settings to allow the VirtualCenter to "speak" to the Microsoft SQL Database. Prior to starting the VirtualCenter 2.5 installation these settings need to pre-configured for both databases.

At the **VirtualCenter Server**

1. Open **ODBC Data Source Administrator** from Administrative Tools on the Start, Programs menu
2. In the **ODBC Data Source Administrator** choose the **System DSN** tab
3. Click the **Add** button
4. From the end of the list choose **SQL Server**, and select **Finish**
5. In name field of the **Create a New Data Source to SQL Server** dialog box, type **VMware VirtualCenter**

   **Note:**
   The VirtualCenter installation assumes this name

6. From the drop-down list **select your SQL server** and click **Next**
7. Select "**With SQL Authentication…**" and type in the user account and password for the database set up in SQL and click **Next**
8. Enable "**Change the default database to**" and select the VirtualCenter Database you created earlier
9. Click **Next** and **Finish**

   **Note:**
   You should be now able to confirm all the dialog boxes associated with the ODBC setup – and also test that you have connectivity to the database server. This test is nearly always successful. It does *not* test your user account credentials.

**Note:**
Repeat the above steps for the Update Manager Database using "VMware Update Manager" as the name of the DSN

# Installing VirtualCenter 2.5

**Note:**
The installation of the VI Client requires the Microsoft .NET 2.0 libraries. This is not a huge problem if they are not already installed. The .NET libraries are redistributable and are on the VirtualCenter 2.5 CD. If not already installed the VirtualCenter install engine will install the Microsoft .NET 2.0 Framework.

You're now in the position to start the VirtualCenter installation. I would recommend using either the physical CD, an ISO or copying the source code to a local disk. I have attempted installations across the network by mapping a network drive – that didn't seem to work and everything despite running everything across a gigabit network.

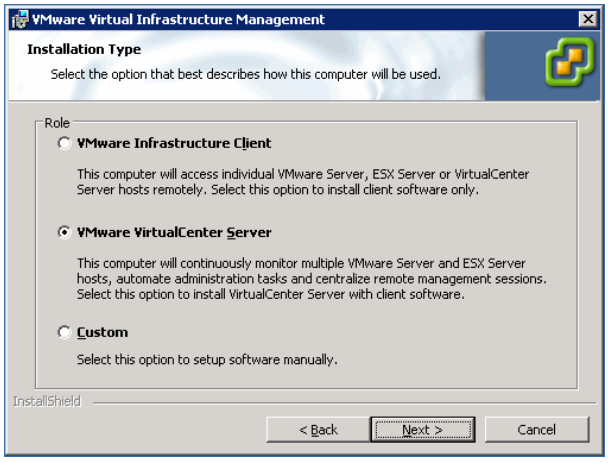
Lastly, although VirtualCenter and the Update Manager can reside on the same Windows instance I would not personally recommend it. For a couple of reasons

- More work for your VirtualCenter server do
- Requires VirtualCenter to have access to the internet to download updates
- Found it to be more reliable to install and enable the VMware Update Plugin when VMware Update Manager is on separate Windows instance

In contrast I found that installing the VMware Enterprise Converter software on the VirtualCenter box was reliable and does not require access to the internet to function

1. **Next your way through the usual install suspects** – welcome dialog box, EULA, Username and Organization
2. After wading through these dialog boxes you will make your way to the **Installation Type dialog box** (Figure C.4). This dialog box allows you to install just the VI Client; just VirtualCenter or custom. The custom option allows you to install all features of VirtualCenter
3. Choose **Custom**

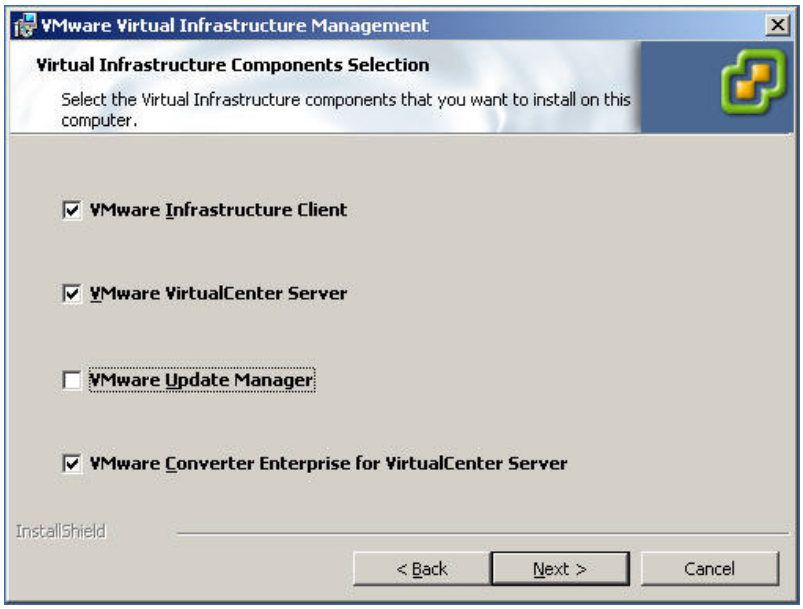
**Figure C.7**




4. The custom option allows you to selective install various components that are now integrated into VirtualCenter including the **VMware VI Client, VirtualCenter, Update Manager, and Converter. In these instructions I kept everything selected, except**

**I did not install VMware Update manager,** as show in Figure C.8

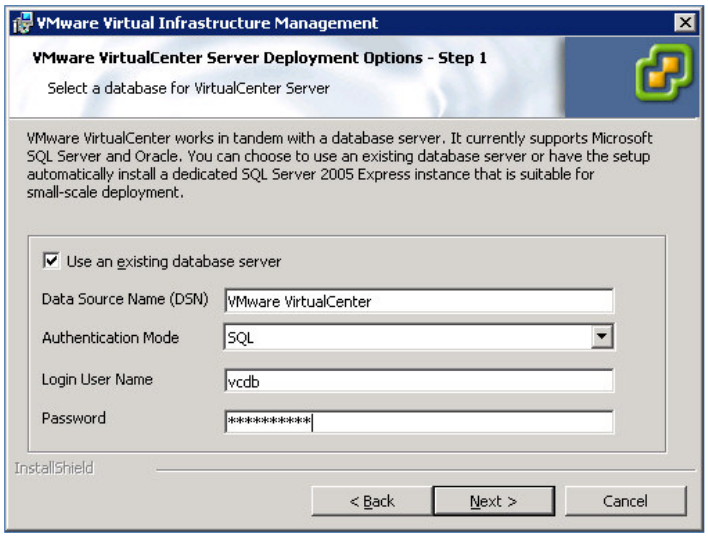
**Figure C.8**




5. Next you will need to tell VirtualCenter where the relevant databases are. **The first database you setup is for the core VirtualCenter database**. Figure C.9 shows the main database dialog box.

   In my case I used SQL authentication mainly because historically I have always used it with VirtualCenter from 1.x.x to 2.0.2.

   **Figure C.9**




6. **After you click next you will receive two pop dialog boxes** (Figures C.10 and C.11). Both of these pop-up dialog boxes are informational and are meant to alert you to potential problems. As long as you do vanilla installations of SQL; locate your data files on a non-Windows OS partition and backup VirtualCenter frequently you should not worry.

   **Figure C.10**

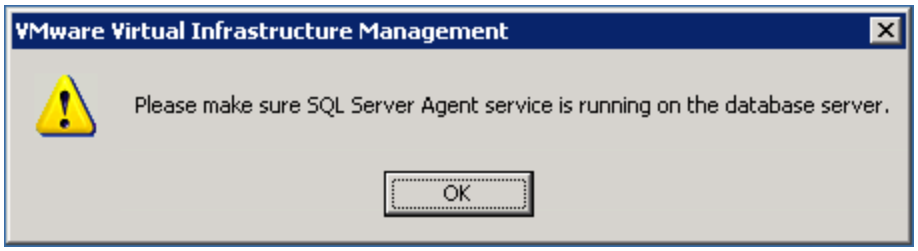
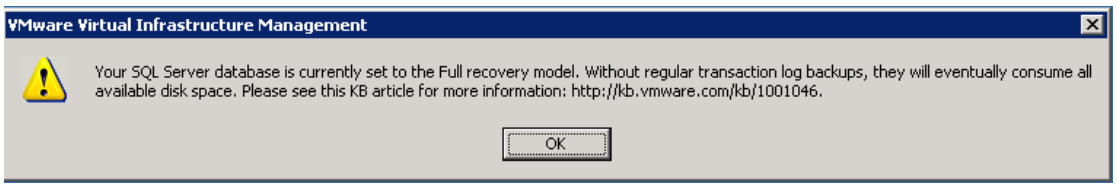



**Figure C.11**

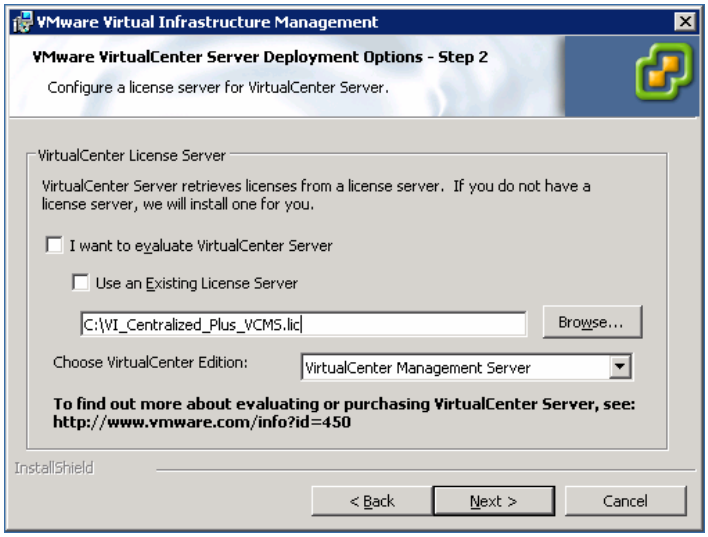



7. **Next you need to license the VirtualCenter installation**. You have three main options:

   **Evaluation**
   **Use an existing License Server**
   **Install a new license server and browse for .LIC file**

   Although the default is "I want to evaluate VirtualCenter" the last option is like to be the most common configuration for a clean installation of VirtualCenter. Additionally, you will need to set if you are using the full enterprise release of VirtualCenter or if you are running it in its "Foundation Management Server" mode

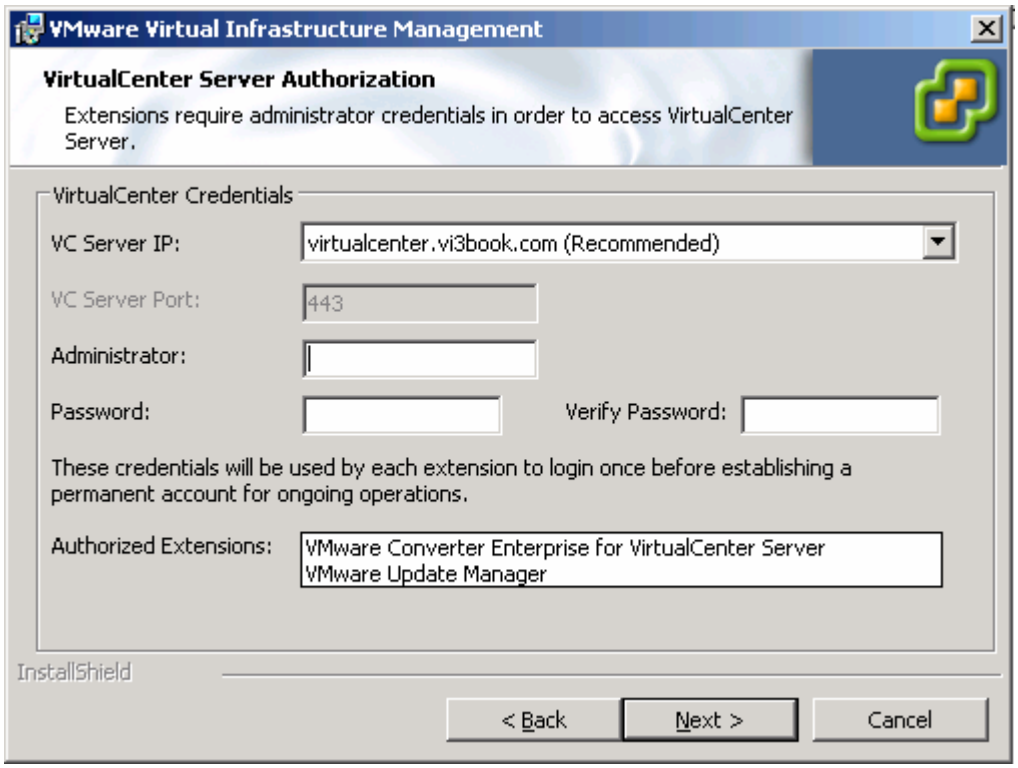
   **Figure C.12**




   **Note:**
   After this dialog box you will be confronted with a dialog box to set all the port numbers for VirtualCenter which you can adjust as per your datacenter policies.

8. Next you will be asked to **set the user credentials for VirtualCenter Extensions.** Figure C.13 shows this dialog box. This allows you to set how the "extensions" communicate to the VirtualCenter server (via the VirtualCenter Web-Server on port 443). In my license file I have two extensions – VMware Converter and Update Manager.

**Figure C.13**




**Note:**
Extension – or "plugins" as they are known in the VI Client – add functionality such as VMware Converter and VMware Update Manager to a "basic" VirtualCenter installation. These plugins are not installed by the main installation, and require a manual installation triggered by the VI Client and plugins menu. They extend the UI of the VI Client to add an "Import Machine" option to the right-click menu of ESX hosts and clusters – and in the case of VMware Update Manager it adds another button along side Inventory, Admin, Events and Schedule Tasks buttons. In order for these plugins to be added successfully and work correctly you need to specify a VirtualCenter user account for their use. This is NOT the user account you used to access the VirtualCenter or Update Manager databases. But the user account you would use to login to VirtualCenter.

9. After this dialog box a **similar port number dialog appears if you choose to install the VMware Converter Service**

10. Click **Install** and then watch the progress indicator. The progress bar updates as each major component is installed. Figure C.14 shows the progress of the installation

**Figure C.14**

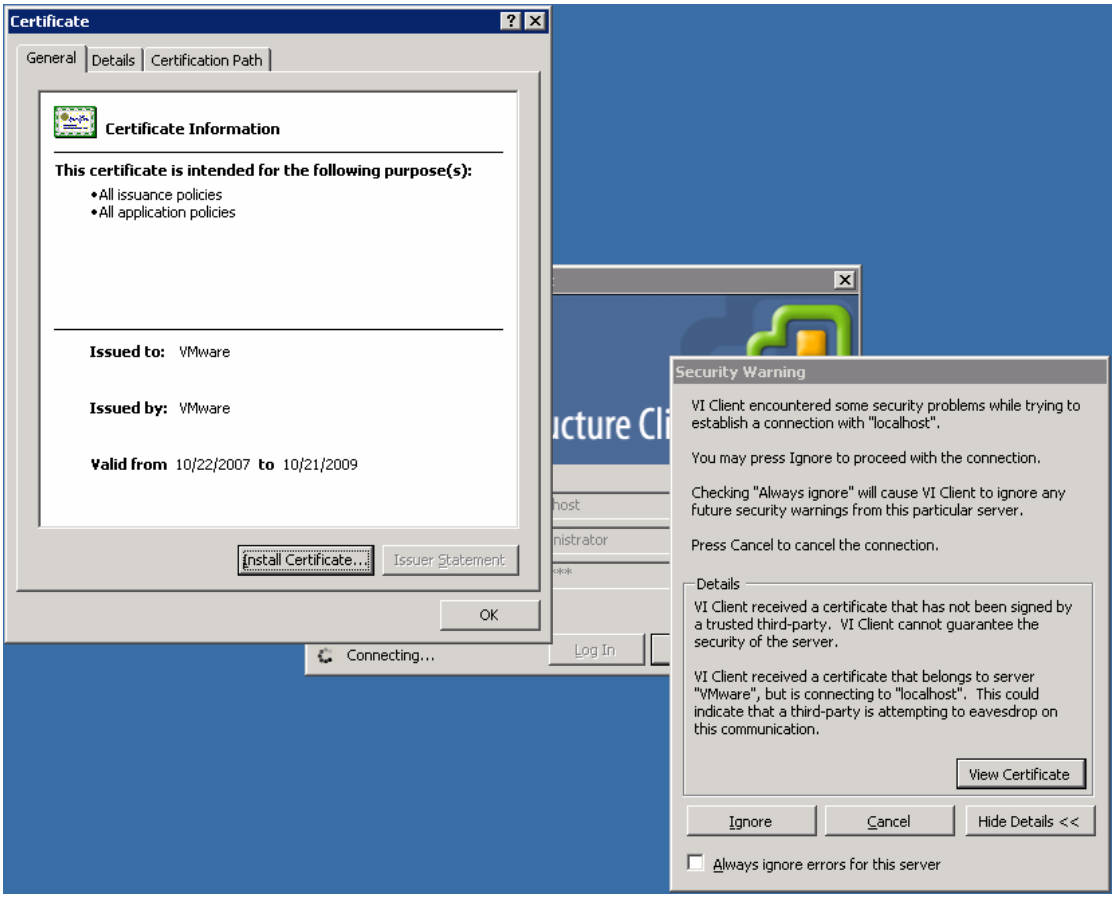

## Login to VirtualCenter

As with ESX 3.5, when you first login to VirtualCenter you will have to do some certificate management. By default the certificate generated for VirtualCenter is called "VMware", rather than the FQDN of the server. Again the certificates are issued from a certificate authority that is untrusted. When you login choose yes to install the root certificate. Figure C.15 shows the certificate warning dialog box.

**Figure C.15**


In addition to this dialog box, you will prompted by a range of dialog boxes to handle the VirtualCenter certificate itself. Figure C.16 shows the VI Client login box and the "Security Warning" dialog. In this case, I installed the VI Client to the VirtualCenter server directly and used "localhost" as the name to connect to. The security warning dialog allows you to click a "View Details" button which gives you an advisory about why this warning is occurring. The View Certificate button will bring up the standard Microsoft certificate dialog that is used to view the certificate details. It is possible to enable "Always ignore errors for this server" and then click ignore

**Figure C.16**




## Getting Started with VirtualCenter

VirtualCenter now has a welcome page to guide you through the initial setup process, those of you who having been using VirtualCenter for a while should be familiar with this process already. What's new here is when you add an ESX host into VirtualCenter you can also enable "Lockdown Mode". This is very similar to the lockdown mode available in ESX 3i. This lockdown mode prevents direct access to the ESX host via the VI Client, forcing all access to occur via VirtualCenter.

If you lockdown the server and then realize you quite like being able to get direct access to an ESX host, then the lockdown mode can be disabled selecting the ESX host, clicking the Configuration Tab and selecting the Security tab. If decide not enable the lockdown mode at the stage of adding the ESX host to VirtualCenter – it can also be enabled from the same location.

Figure C.17 shows the advisory that appears when adding the ESX host and C.18 shows the manual method of enabling and disabling lockdown mode in the Configuration and Security Profile location. Figure C.19 shows the error message when an operator tries to login the ESX host direct with lockdown mode enabled

**Figure C.17**

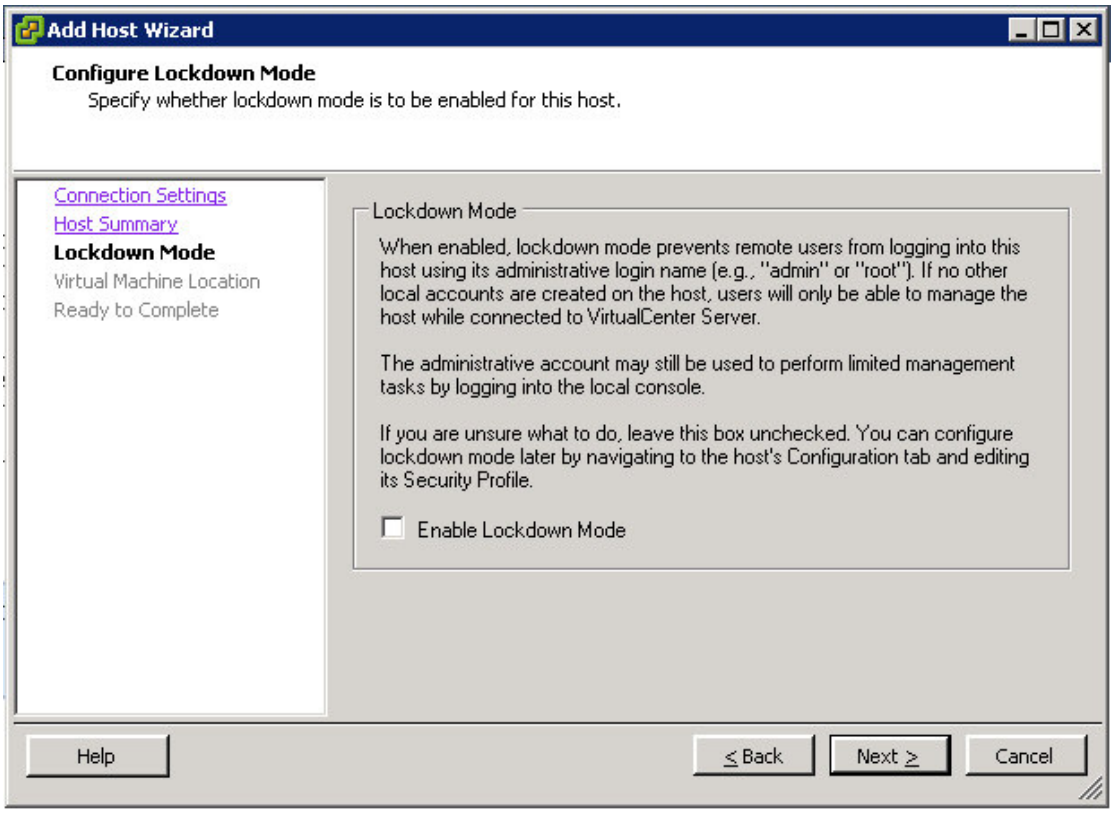
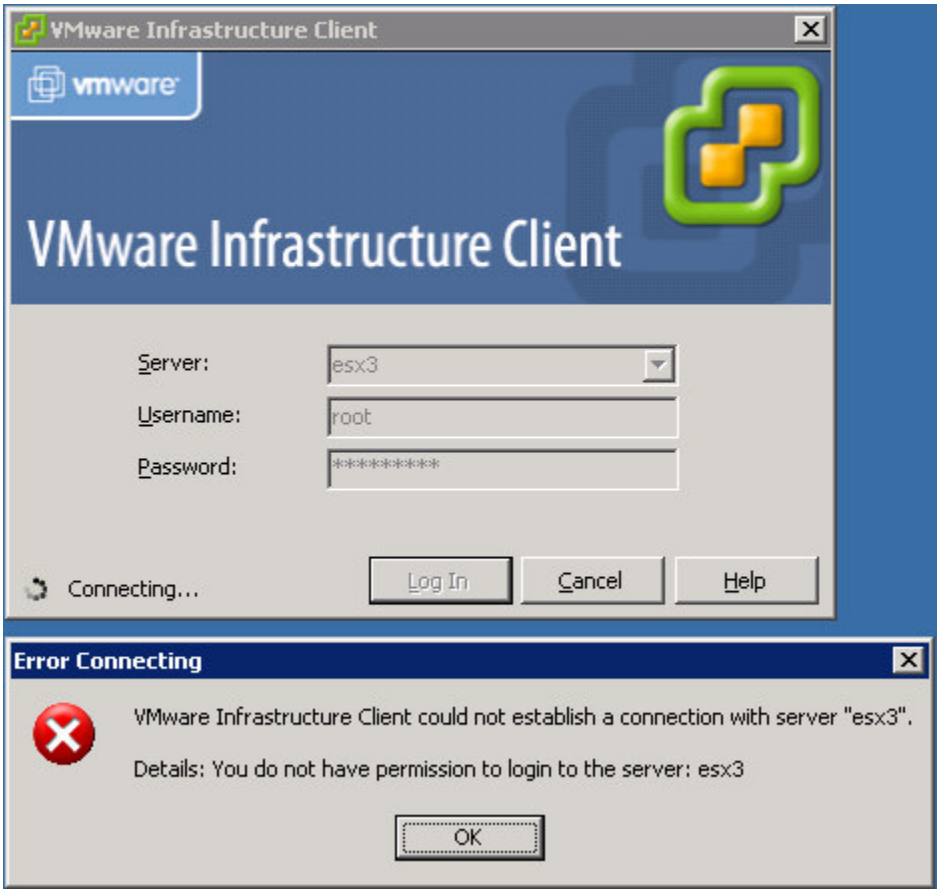



**Figure C.18**


**Figure C.19**




**GOTCHA:**
Lockdown mode does NOT prevent SSH access. If you create local user accounts on the ESX host, these users can still SSH to an ESX host and use the command **su –** to elevate themselves to root access (if they know the password of the root account). It is still the case that by default root is denied access in the /etc/ssh/sshd_config file. If you don't create any local user accounts prior to enabling lockdown this effectively prevents SSH access. Security for SSH is provide by Service Console security.

**Note:**
Adding in the ESX 3i version to VirtualCenter generates the same dialog boxes. From a VirtualCenter perspective managing an ESX 3.5 and ESX 3i host are the same. However, you will have to configure ESX 3i with a static IP address and root password before hand

## Licensing an ESX Host

Typically, the next thing you will want to do is license an ESX host. Without doing so you wouldn't be able create and power on a VM. The licensing process has been slightly refined in this release. Adding an ESX host to VirtualCenter has always set the licensing server name (as long as DNS name resolution is available from the ESX host to the VirtualCenter server). After adding an ESX host under previous releases you would need to set the "host edition". In this release this is set for you.

The dialog boxes for licensing have subtly changed to reflect VMware's change in its licensing model. As you can see Figure C.20 (ESX host, Configuration, select the Software Pane, next to the License Source, select the **Edit...** link) allows you set the location of your license. It is still the case that if you want to license your ESX for enterprise VI-3 features such as VMotion, DRS and HA, that this requires a VMware Licensing server. Figure C.21 shows that you no longer need to set the edition you're using (Unlicensed, Starter and Standard). The ESX Server edition is either licensed or unlicensed.

**Figure C.20**

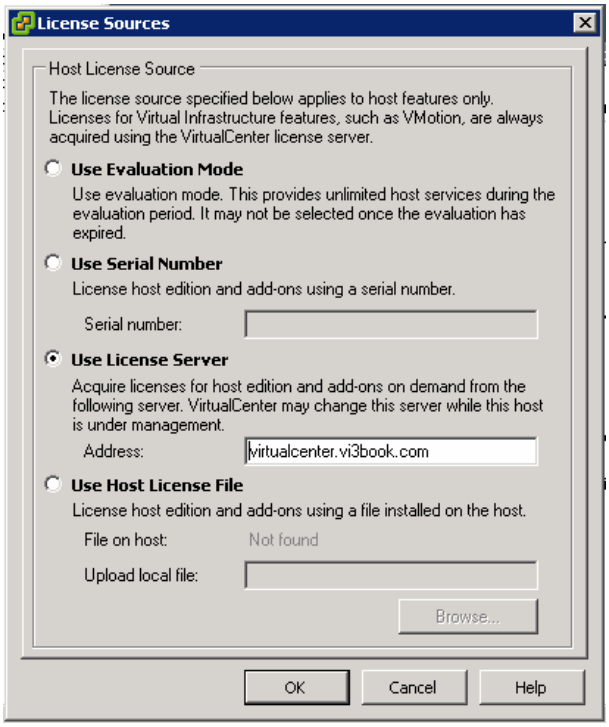
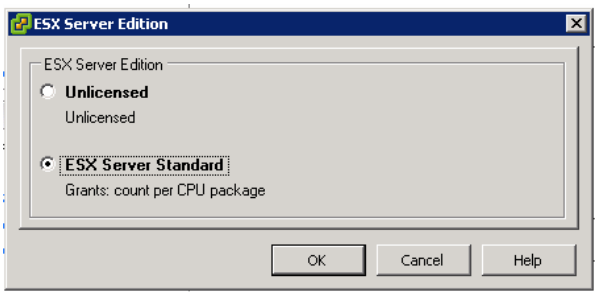



**Figure C.21**




# *Networking*

There are no real substantial changes to the configuration of networking either ESX 3.5 or ESX 3i via VirtualCenter. There are some very slight changes to the look and feel of network configuration, and there some interesting changes to default settings, should you decide to script your ESX 3.5 installation.

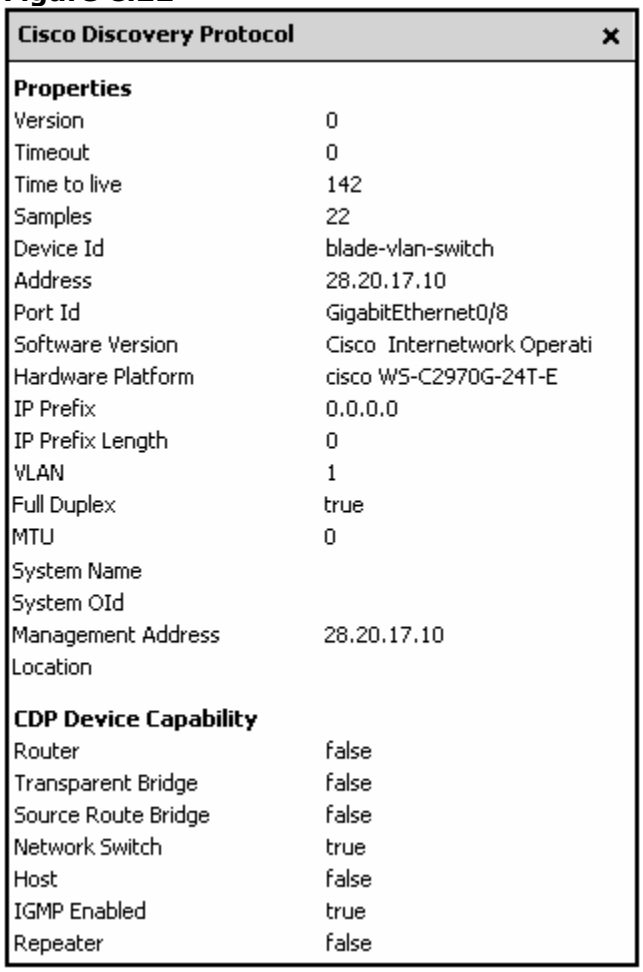
The big changes are in the increased support of new physical devices and the performance enhancements they offer. For these to be of any advantage to your system these devices must be physically present and on the VMware HCL. They include:

- TCP Segmentation Offload
- Jumbo Frames (Limited to specific guest operating systems)
- IOAT v1 (Experimental Supported Only)
- IPv6 Guest Support (Experimental Compliance Support)
- 10 GigE NIC Support
- IP over Infiniband for general networking and iSCSI traffic

## Graphical Changes

If you compare and contrast VirtualCenter 2.0.2 to VirtualCenter 2.5 you will notice some graphical changes. The main one is a new blue info icon which brings up a pop-up information "bubble" which can tell you about the vSwitch configuration, this returns Cisco Discovery Protocol values (CDP).

**Figure C.22**



| Cisco Discovery Protocol | |
|---|---|
| **Properties** | |
| Version | 0 |
| Timeout | 0 |
| Time to live | 142 |
| Samples | 22 |
| Device Id | blade-vlan-switch |
| Address | 28.20.17.10 |
| Port Id | GigabitEthernet0/8 |
| Software Version | Cisco Internetwork Operati |
| Hardware Platform | cisco WS-C2970G-24T-E |
| IP Prefix | 0.0.0.0 |
| IP Prefix Length | 0 |
| VLAN | 1 |
| Full Duplex | true |
| MTU | 0 |
| System Name | |
| System OId | |
| Management Address | 28.20.17.10 |
| Location | |
| **CDP Device Capability** | |
| Router | false |
| Transparent Bridge | false |
| Source Route Bridge | false |
| Network Switch | true |
| Host | false |
| IGMP Enabled | true |
| Repeater | false |

This allows you to see which Cisco switch port is connected to a vSwitch. CDP support can be controlled by esxcfg-vswitch –b and esxcfg-vswitch –B. –b in lower-case allows you to see the status of the discovery process and –B in upper-case allows you to set the CDP protocols settings. There are four possible options

**down**
CDP is disabled (default)

**listen**
The VI Client receives information from the Cisco Switch but does not send information about the vSwitch to the Cisco Administration tools

**advertise**
Advertise is the reverse of listen. It does not report CDP information to the VI Client, but does report information to Cisco Administration tools

**both**
This allows bi-directional communication and is a combination of listen and advertise

Here are examples of using esxcfg-vswitch for CDP usage:

**esxcfg-vswitch -b** vSwitch0 – reports status information
**esxcfg-vswitch -B listen** vSwitch0 - sets the policy of listen for CDP

**Note:**
Cisco CDP packets are only sent once a minute – so may have to wait some time before the VI Client is refreshed

We also have new icons in the vSwitch dialog box to represent vSwitch and Port Group. Figures C.23 and Figure C.24 show the old and new vSwitch dialog boxes respectively

**Figure C.23**

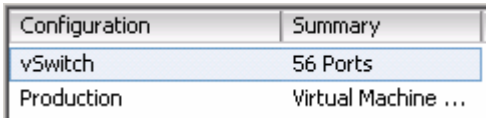
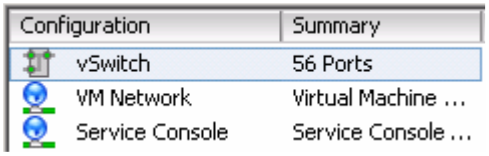
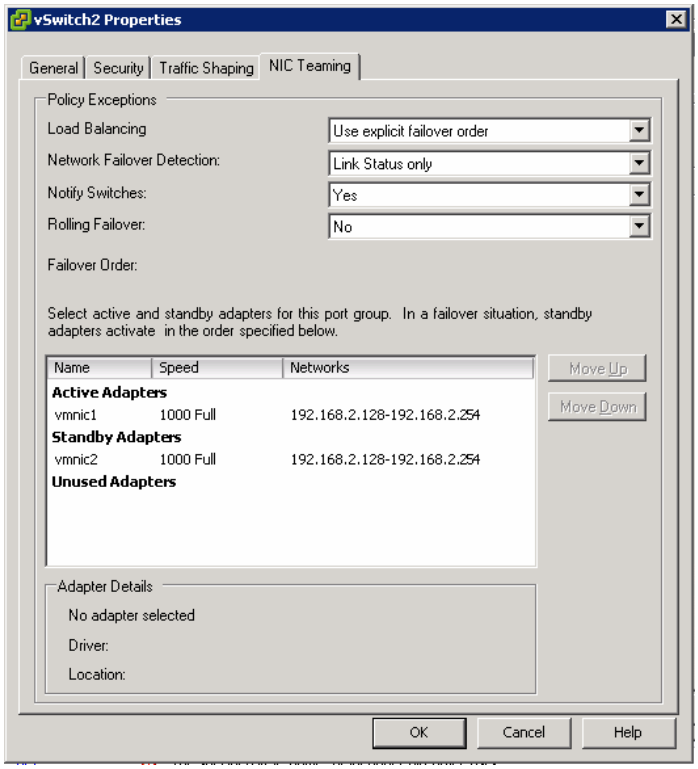



**Figure C.24**



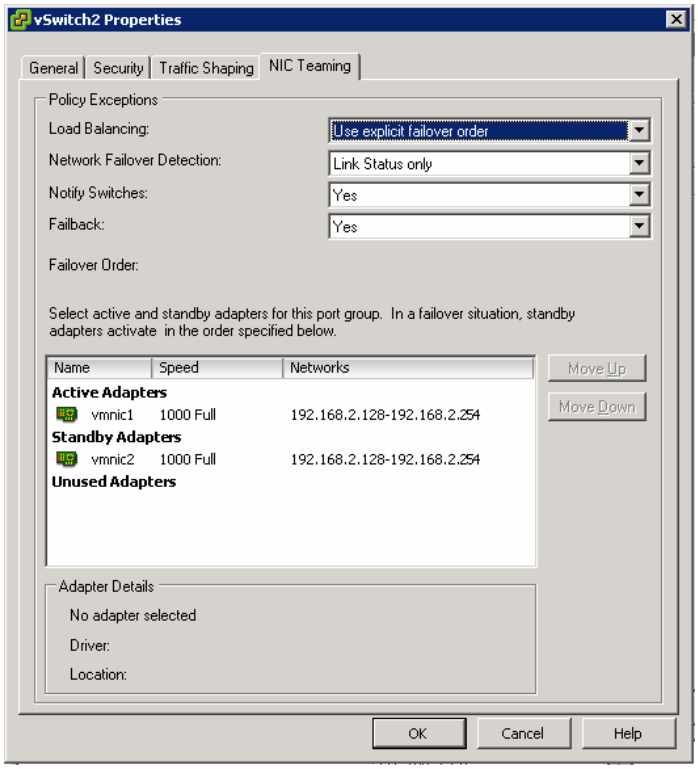

These two examples aren't the only changes made in the networking user interface. VMware have also made some changes to the terminology in the NIC dialog box. Very often these terminology changes have not altered the original functionality of the VI-3 offering. A case in point is the NIC teaming "fail-back" settings. Prior to ESX 3.5 the term that VMware used was "Rolling Failover". Figure C.25 shows the old NIC teaming dialog box from ESX 3.0.x days

**Figure C.25**




You can see here that "Rolling Failover" is set to "No". This means that if vmnic1 failed, vmnic2 would become the active adapter. However, if vmnic1 became available again, network traffic would return to vmnic1. As you can see the term "Rolling Failover" isn't as clear as it could have been. If you think about it, the setting actually controls fail-back, not failover! Fortunately, this clarity in the dialog box has been rectified, by re-labeling the setting. Figure C.26 shows the new terminology in the ESX 3.5 dialog box.

**Figure C.26**



The default setting retains the same meaning because "Rolling Failover" set to "No", means the same as Failback being set to "Yes". When vmnic1 is available again it will be used.

Another graphic change is one that affects ESX 3i. As ESX 3i has no "Service Console" environment in the "classic" ESX sense of the word – the use of the words "Service Console" on the port group on vSwitch0 has been dropped in preference for the more accurate term of "management network". Similarly, if you run the "Add Networking" wizard against an ESX 3i host you will find the option to create a "Service Console" connection has been removed. Figures C.28 and C.29 shows the changes

**Figure C.27**

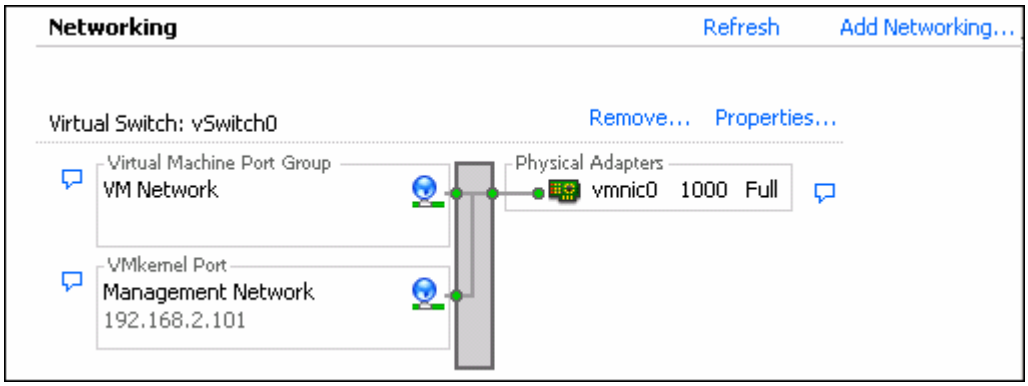
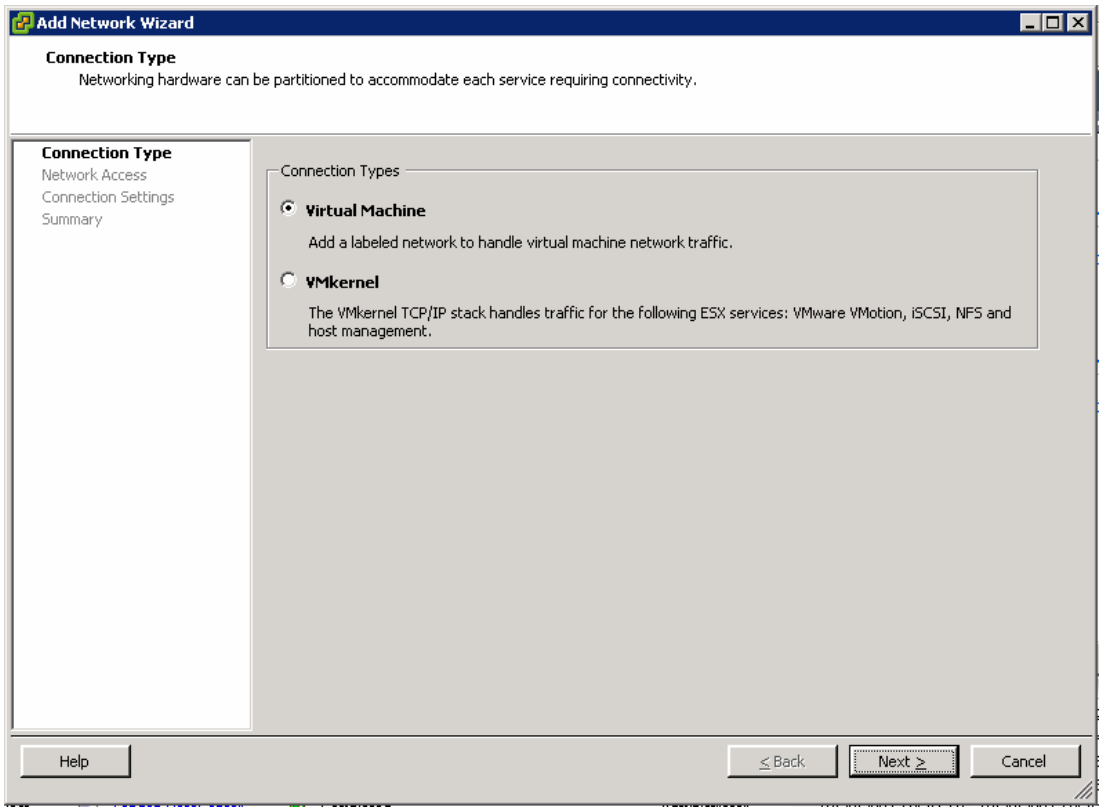



**Figure C.28**

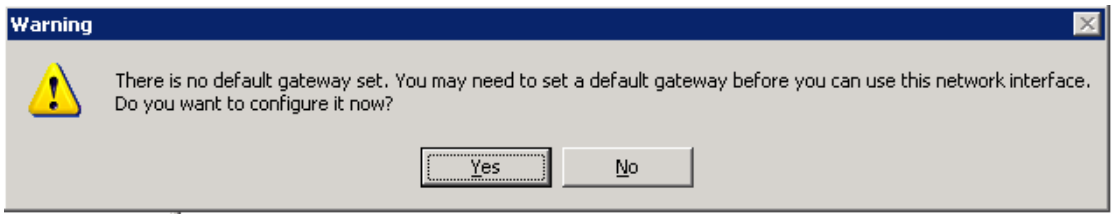



## Routing and Creating a VMKernal Port Group

Another change in terminology has occurred when creating VMkernel Port Groups for either VMotion or IP-based storage. In the past, VI-3 finished the wizard with a pop dialog box which

stated that the operator "*must* set a default gateway". This dialog box has been changed to express the more accurate phrase of "*may* need to set a default gateway". Nonetheless, the VMkernel port group wizard still only allows you to set an IP address and subnet mask, with the wizard opening the "DNS and Routing Configuration" dialog box (which remains unchanged) if you choose "Yes" to the pop-up box. Figure C.29 shows the new routing dialog box; in most case you will choose "No" as routed VMotion is *not* supported by VMware and IP-based storage is best access directly through a switch rather than hopping across routers.

**Figure C.29**




# *Storage*

There are number of critical improvements and extensions of support within storage and ESX 3.5. These include

- Support for a "round-robin" style load-balancing algorithm for Fibre-channel HBAs.
- Along side SCSI and SAS drives, VMware will now support SATA drives both for booting ESX and for hosting VMFS volumes
- iSCSI will be supported with VCB, which previously was only certified with Fibre-channel communications. Indeed this support restriction was actually lifted in ESX 3.0.2. If you do wish to use iSCSI systems with VCB be sure to consult the HCL for these systems as support is relatively new
- Virtual Machines now support n-Port I/O Virtualization (NPIV). This is a Fibre-channel feature which allows the VM to be allocated a WWN. This allows SAN Management tools to see a VM's storage and support features like LUN Masking down to the VM. This feature is really more focused on the VM and so will be covered in the VM section of this document

## Enabling HBA Round-Robin via the VI Client

**Caution:**
Currently, the Round Robin method is experimental and not yet supported for production use.

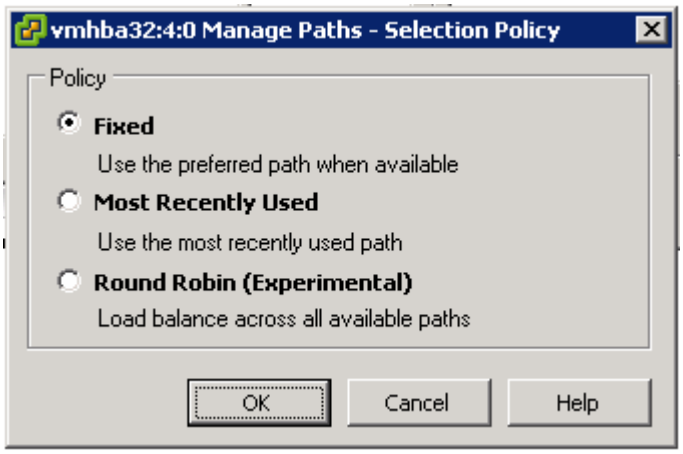
The automatic load-balancing of HBAs is enabled in the multipathing part of the storage configuration. This means we will have four multipathing policies to choose from – MRU, Fixed, Round-Robin, and Custom. Whilst the first three can be configured from the VI Client, the custom policy can only be configured from the command-line using the esxcfg-mpath command and allows you to set your own parameters for when the ESX host makes a switch from one HBA path to another for either fault-tolerance or load-balancing. To configure the HBA path selection policy from within VirtualCenter:

1. **Select the ESX host** and choose the **Configuration Tab**
2. **Right-Click a VMFS volume** and choose **Properties**
3. Click the **Manage Paths** button

   **Note:**
   Alternative way to access this dialog box is to select in the Hardware Pane, Storage Adapters and select the HBA. In the list of LUNs with the vmhba syntax, select a LUN, right-click and choose Manage Paths

4. In the **Manage Paths dialog box**, click the first **Change button**. Figure C.30 shows the policy dialog box with the round robin option

   **Figure C.30**




## Enabling HBA Round-Robin via the CLI

The command esxcfg-mpath now has switches to control what method is used to control the path selection process. The command supports custom policies which include switches for:

- **--policy** (-p)
  Specify if fixed, MRU, Round-Robin or Custom is the policy. This same setting can be configured from the VI Client

- **--custom-max-commands** (-C)
  Load-balance on the number of r/w commands issued on a specified path

- **--custom-max-blocks** (-B)
  Load-balance on the number of I/O blocks issued on a specified path

- **--custom-target-policy** (-T)
  Specify which policy you when connect to the Storage Processors (targets) on the SAN option include using Fixed/Preferred, MRU or Any

- **--custom-HBA-policy** (-H)
  Specify which HBA to used to connect to the target and what conditions trigger its use such as the HBA with the smallest number of outstanding I/O commands

**Note:**
The syntax above shows the long switch (with two dashes) first followed by the shorter switch with a single dash. Below are some examples of using the esxcfg-mpath command.

**Query Path Information:**
esxcfg-mpath -q --lun=vmhba32:4:0

Disk vmhba32:4:0 /dev/sda (69984MB) has
**1 paths and policy of Fixed**
iScsi sw iqn.2006-09.com.VI-3book:esx1<->iqn.2006-09.com.VI-3book:iscsi
vmhba32:4:0 On active preferred

This shows that I'm using the iSCSI Software Adapter, with a policy of "Active Preferred". This is the default for the iSCSI Software Adapter. After changing the policy in the VI Client to be round-robin, and running the same command again the result is:

Disk vmhba32:4:0 /dev/sda (69984MB) has
**1 paths and policy of Round Robin/Balanced**
iScsi sw iqn.2006-09.com.VI-3book:esx1<->iqn.2006-09.com.VI-3book:iscsi
vmhba32:4:0 On active preferred

**Changing the Multipath Policy from the Service Console:**

To Round-Robin: esxcfg-mpath --lun=vmhba32:4:0 -p rr
To Fixed: esxcfg-mpath --lun=vmhba32:4:0 -p fixed
To Custom: esxcfg-mpath --lun=vmhba32:4:0 -p custom

**Setting a Custom Policy:**

To specify a path selection policy that would cause your ESX host to change to any different HBA or Target once 5000 blocks or 100 commands have been issued to a specified path:

esxcfg-mpath --lun=vmhba32:4:0 -H any -B 5000 –C 100 –T any

This would produce the following query result:

Disk vmhba32:4:0 /dev/sda (69984MB) has
1 paths and policy of Custom:
maxCmds=100 maxBlks=5000 hbaPolicy=any targetPolicy=any
iScsi sw iqn.2006-09.com.VI-3book:esx1<->iqn.2006-09.com.VI-3book:iscsi
vmhba32:4:0 On active preferred

## iSCSI Software Adapter

There two main changes within the iSCSI software adapter. In ESX 3.0.x when you enabled the iSCSI software adapter the enabling process automatically opened the TCP port (3260) required for iSCSI communication to occur. This no longer the case. You now must manually open the ports for iSCSI to work properly. This can be done from within the VI Client by selecting

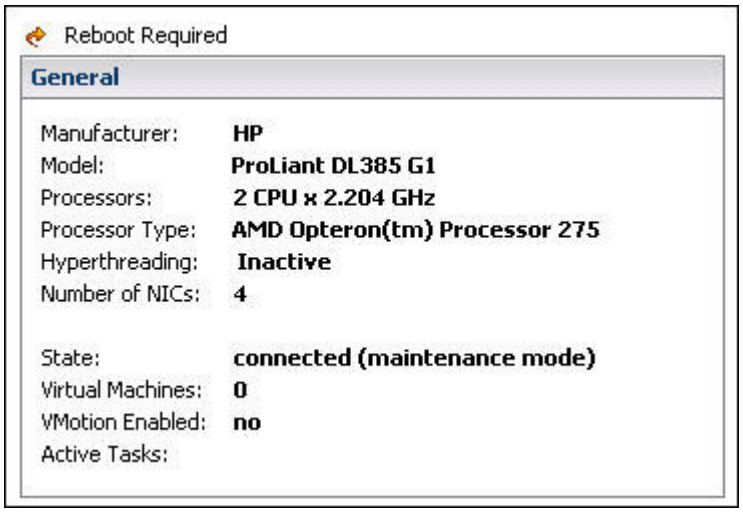
1. **Configuration** tab
2. Under **Software Pane** select **Security Profile**
3. Select **Properties…**
4. In the **Ungrouped Section** select **Software iSCSI Client**

The other change concerns setting your own custom IQN. If you remember when VMware's software adapter is enabled an IQN is automatically generated for the vmhba32 device. The auto-generated IQN looks like this

**iqn.1998-01.com.vmware:esx1-5c11719c**

If you decide to change the default IQN created for the ESX host to a naming convention that befits your organization, you will be warned that a reboot is required. This warning about having to reboot is not new, but what is new is a warning in the "Summary" tab of an ESX host that a reboot is pending. Figure C.31 shows the warning when an ESX host requires a reboot for a configuration change:

**Figure C.31**




**GOTCHA: Service Console Connections**
Some of the other "oddities" about the iSCSI Software Adapter remain unchanged. The main one being, if your iSCSI Target exists on a different network from your primary Service Console (vswif0) connection (as it invariable will do for security and performance reasons) you still require a second Service Console connection (vswif1) for the discovery and authentication process to the iSCSI Target to be successful.

**GOTCHA: ESX 3i is different**
Currently in the ESX 3i product there are no settings to enable the firewall for iSCSI. Additionally, as they don't exist in this product there is no need to create a second Service Console port as is the case in ESX 3.5. In ESX 3i the iSCSI Software Adapter has an identity of vmhba33 because the internal USB controllers use vmhba32. As a consequence, I found that ESX 3i requires much less configuration than ESX 3.5.

## The New Improved DataStore Browser

There is no "Service Console" in ESX 3i. This means there is no SSH or SCP support, either. So tools such as WinSCP and Veeam's FastSCP no longer function as intended. If you wish to upload an ISO file to your VMFS you can now do this from the DataStore Browser. Even without ESX 3i you will find the new datastore browser makes life much easier when uploading or downloading files from your management PC to an ESX host. One common task on a cleanly installed system is copying ISO files from your management network to a datastore on Fibre-channel SAN or iSCSI SAN.

1. **Right-click one of your VMFS** volumes
2. Choose **Browse DataStore**
3. Click the **Upload Icon** (Figure C.32 shows the icon)

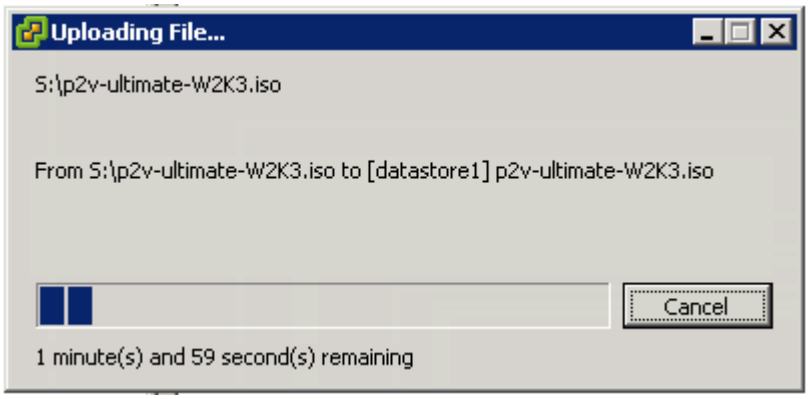
**Figure C.32**


4. Select **Upload File...**
5. **Browse for the ISO** you need and Click **OK**

6. **Confirm the warning that this might replace files with the same name in the VMFS**

   **Note:**
   Then watch the pretty status bars

   **Figure C.33**




   **Note:**
   The DataStore Browser's functionality has been enhanced in VI-3.

   You can now also:

   - Download files from an ESX host datastore to your workstation.
   - Move files from one datastore to another
   - Rename files

# *Virtual Machines*

## Creating new Virtual Machines

When creating a new virtual machine you will spot a number of differences. Most of these changes are minor enhancements from the base VI-3 release. Critically what is new is that the guest operating system list has been updated to include:

Windows 2003 32/64-bit DataCenter Edition
Windows 2008 32/64-bit
Unbutu Linux 32/64-bit

In fact Unbutu Linux has been officially supported since ESX 3.0.2.

In the Release Candidate for ESX 3.5 the words [Experimental] *do not* appear next to the Windows 2008 editions. This support is unlikely to be the case when the product is fully released to customers, as Windows 2008 is still only in a release candidate phase, and has yet to be fully released. We will probably have to wait some time after this Windows release to switch from being experimentally supported to being fully supported by VMware. Indeed some of you might not adopt the new flavor of Windows until a Service Pack from Microsoft has been released for it.

During the creation of a new virtual machine you will have to select what type of network adapter to use. The choice is between a Flexible or Enhanced VMXnet adapter.  Figure C.34 shows the pull down options in the New Virtual Machine Wizard. Both a Flexible and Enhanced VMXnet network adapter use the vmxnet.sys driver in Windows and in other guest operating systems once

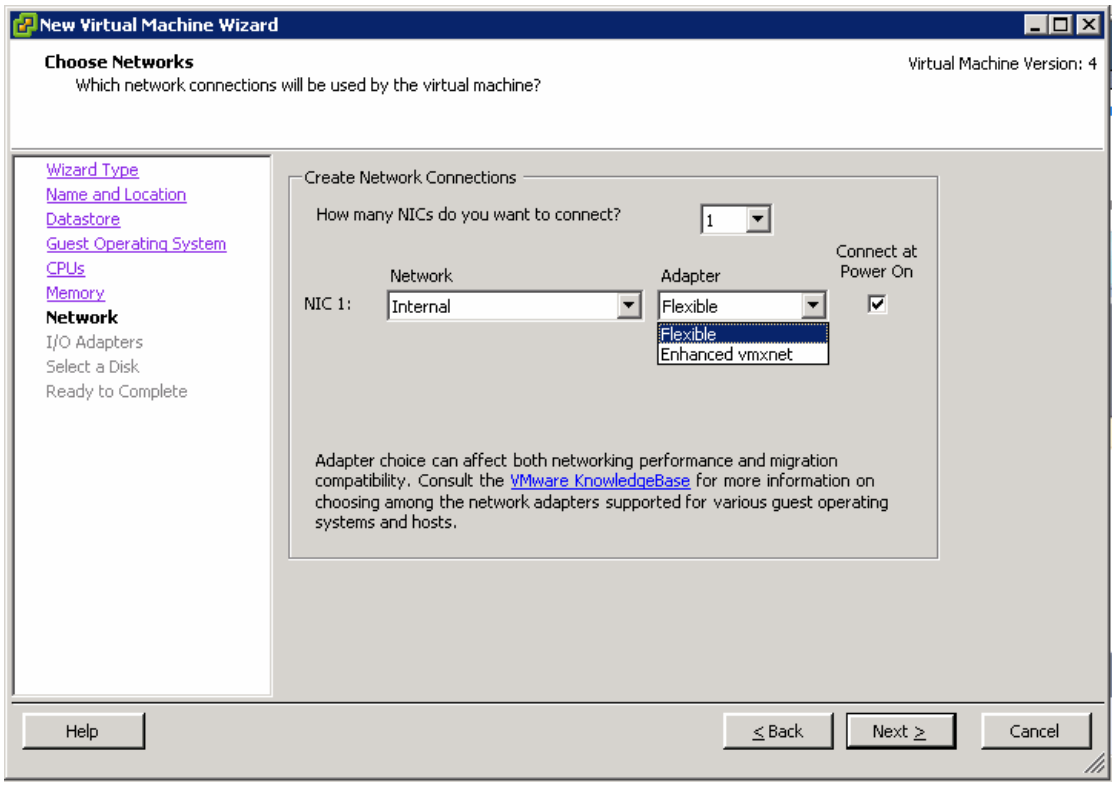
VMware Tools has been installed. The difference is that the Enhanced VMXnet driver is needed for many of the improvements in networking in ESX 3.5 including:

- TCP Segmentation Offload Support
- Jumbo Frames
- IOAT v1 [Experimental Support Only]

As well as having these components implemented at physical level, it is available to only a limited number of guest operating systems including:

- Windows 2003 SP2 (32/64 bit)
- RHEL 5 (32/64 bit)
- SLES 10 (32/64 bit)

**Figure C.34**




**Note:**
TCP Segmentation Offload Support and Jumbo Frame support are enabled by default at the ESX host level. You can see this if you have VMkernel Port Groups enabled and use the esxcfg-vmknic –l command which should now have a TSO MSS column with the value set to be 40960 and MTU of 1500. Figure C.35 shows the output from this command:

**Figure C.35**

```
Interface  Port Group          IP Address      Netmask         Broadcast       MAC Address       MTU     TSO MSS   Enabled
vmk0       VMotion             10.0.0.1        255.255.255.0   10.0.0.255      00:50:56:75:e0:7d 1500    40960     true
vmk1       iSCSI               172.168.3.101   255.255.255.0   172.168.3.255   00:50:56:7f:8c:52 1500    40960     true
```

You can change the MTU value on vSwitch using the Service Console command:

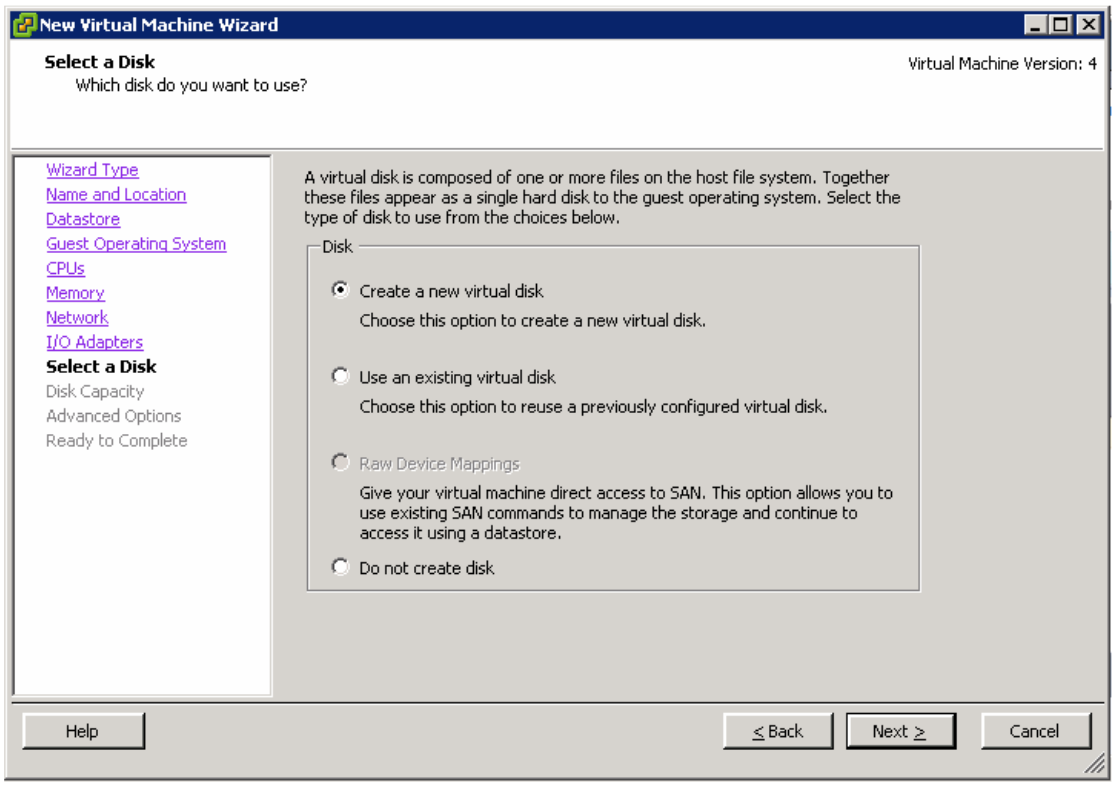
**esxcfg-vswitch -m** 2000 **vSwitch2**

Currently, the maximum MTU value is limited at 9000. If you want to know why this is fixed at 9000 you really need to learn more about Jumbo Frames and the MTU value. That is beyond the scope of this document. Fortunately, there are plenty of "interesting" documents about them on the world wide web.

http://sd.wareonearth.com/~phil/net/jumbo/
http://sd.wareonearth.com/~phil/jumbo.html
http://sd.wareonearth.com/~phil/net/jumbo/jet-mtu.html

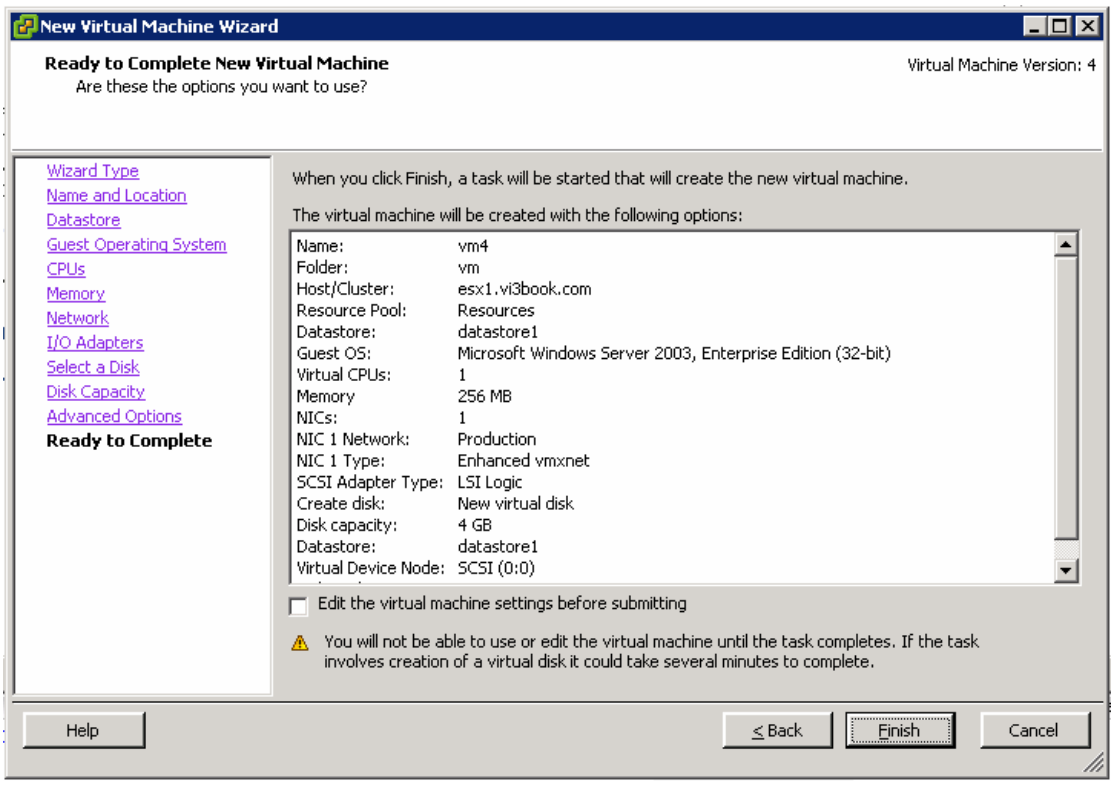
As you progress further through the VM creation wizard, you will see that you now have the option to include a disk (virtual or RDM) in the virtual machine. Figure C.36 shows the new radio button. You might wonder in what scenario you would create a virtual machine without a virtual disk. Firstly, you might prefer to create a virtual disk on the command-line using vmkfstools –c to take advantage of the advanced functionality offered there. Secondly, you might be delivering your guest operating system over-the-wire with PXE or other technology. In this case the VM is just an environment or an engine for processing rather than offering anything in the way of storage functionality.

**Figure C.36**




At the end of creating the new virtual machine, there is option to open the "Edit Settings" dialog of a VM, to make further modifications to the VMs setting such as attaching ISO or changing the VMs reservation settings. Figure C.37 shows this new option.

**Figure C.37**



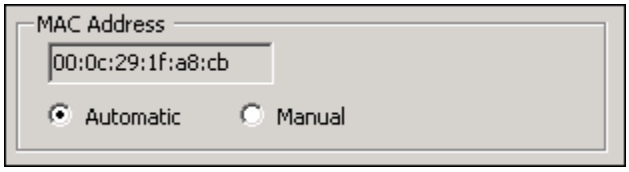

After installing your guest operating system to the VM the next step would be to install VMware Tools. The install and configuration of VMware Tools remains unchanged. At this stage the driver called "Deschedule Time Accounting" which is intended to improve clock accuracy in the VM is still only experimental supported. There is an additional driver for Wyse Multimedia Support which intended for use in VDI deployments where Wyse Terminals are used to connect the end-user to their virtual desktop. To access both drivers and enable them you must use the "custom" option in the VMware Tools installer.

## Editing the VMs Settings

There are couple of major changes to the "Edit Settings" dialog box. A quick look at the options on a VM will allow you to see the differences.

**Set a static MAC address:**
It is now possible to set a static MAC address on VM from the VI Client. Prior to this you need to edit the VMX file of a virtual machine to change the settings. You can change the MAC address of a VM under the Hardware Tab and the Network Adapter of a VM. Figure C.38 shows the change in the edit settings dialog box

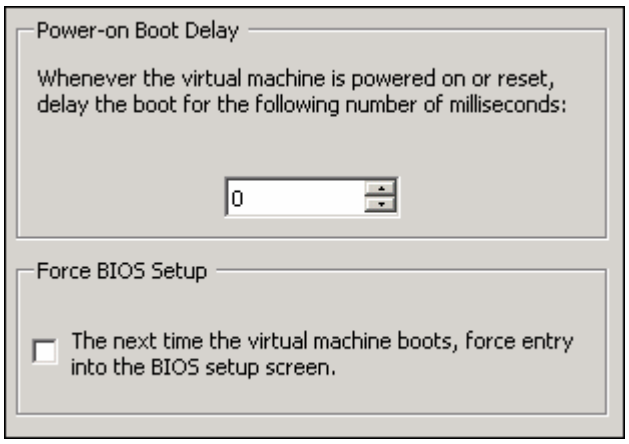
**Figure C.38**




**VMware Tools:**
There are two new options associated with VMware Tools held within Edit Settings, Options Tab, VMware Tools. This includes the ability to check if VMware Tools is the correct version before power on. Second option allows you set that VMware Tools synchronizes with the ESX host for time. Neither of these two options is currently enabled by default.

**Power-On Boot Delay:**
It is now possible to specify a delay to power on process and also force the VM to load the BIOS on the next reboot. Some people have found that the VM boots so quickly that they cannot press [ESC] or [F2] to adjust the BIOS settings. Figure C.39 shows the new options available

**Figure C.39**




**Paravirtualization (VMI) Support:**
Paravirtualization is a virtualization approach where the guest OS is recompiled so that it is VM aware. In other words the guest OS kernel knows it is running inside a virtual machine. This allows for enhancements in the performance of the guest OS. If you want to learn more about paravirtualization and VMware's support for it including its open-source VMI standard visit:

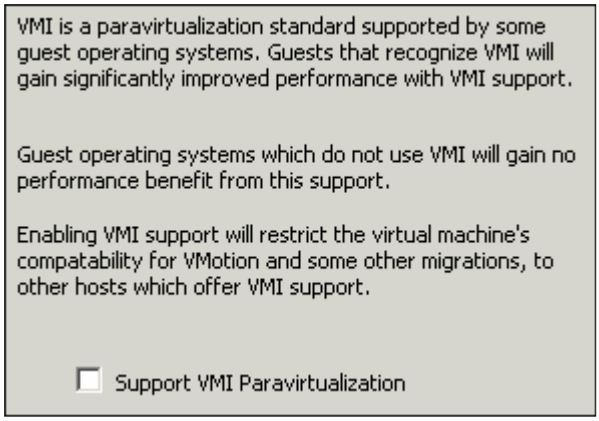
http://www.vmware.com/interfaces/paravirtualization.html

If you are looking for sample guest OS that support paravirtualization there are some downloads available here:

http://www.vmware.com/interfaces/techpreview.html

Right now the number of guest OS that are VMI aware is limited to mainly Linux distributions. Figure C.40 shows the tick off box that allows VMI to be enabled. Notice how this can introduce a possible VMotion incompatibility. At the moment ESX 3.0.2 and older do not support paravirtualization, so your ESX hosts would have to be upgraded to a higher release. It is possible to cold migrate a VM between releases but this could reduce performance if the VM arrives on a destination host which is not yet paravirtualization aware.

**Figure C.40**



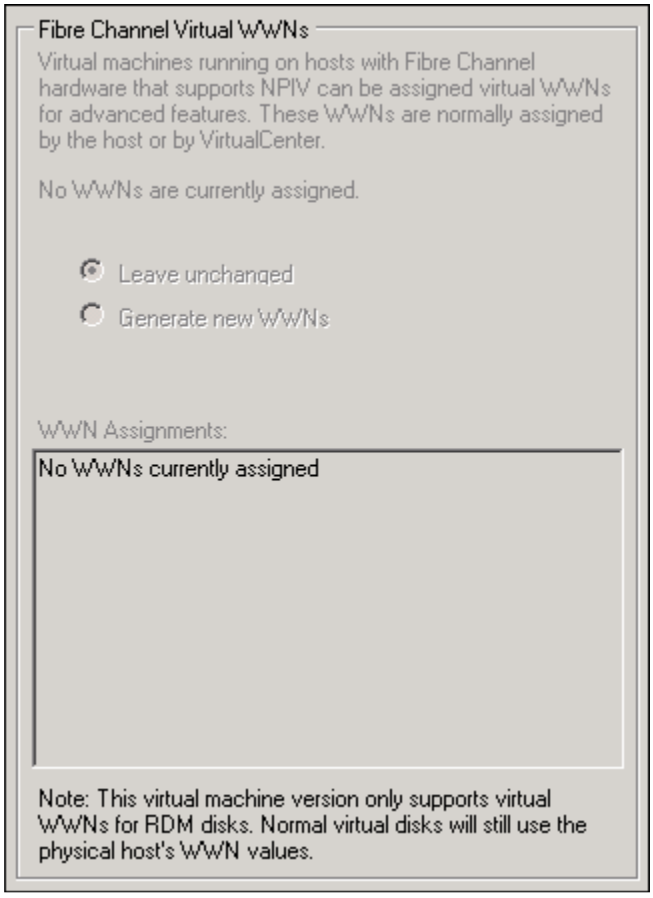
**Fibre Channel NPIV Support:**
Up until NPIV it was the ESX administrators tasks to make sure the right VM's saw the right LUNs when using the RDM (Raw Device Mapping) feature. Essentially, ESX is adding a layer of abstraction between the hardware devices (the VMkernel's fibre-channel device driver) and the VM.

N-Port ID virtualization allows supported fibre-channel devices to present a WWN to a VM. With NPIV the VM is returned to the state of physical machine, as it can have allocated it own WWN. This means the people who manage the SAN are able to leverage features of the SAN directly to the VM. This includes such things as masking and zoning. If you want to learn more about NPIV from a VMware perspective a good place to look is at the "Providing LUN Security" PDF on VMware's website.

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

Unfortunately, none of my servers support NPVI so I am unable to experiment or use this feature right now. Figure C.41 shows the configuration dialog box

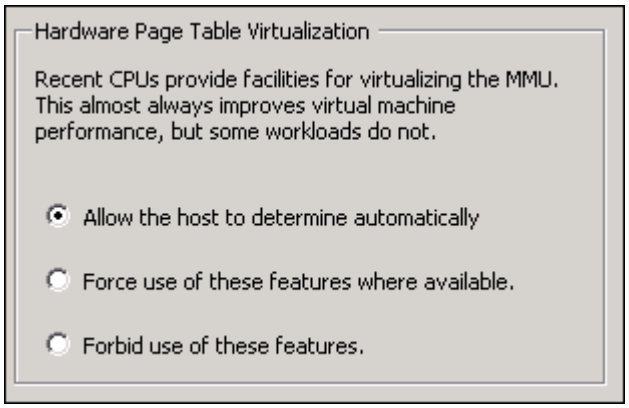
**Figure C.41**




**Virtualized MMU:**
MMU stands for Memory Management Unit. VMware has for a long time supported in the VMKernel a feature called "Page Tables". This is a mapping of memory of the VM to actual physical memory. This allows for enhanced features such as Transparent Page Sharing (TPS), where the VMkernel spots duplicate data within and between VMs – and produces as single read-only copy. Whilst this is a great advantage (as it reclaims "lost" memory and is often enough to than reduce any memory overheads experienced in virtualization) it clearly makes the VMkernel harder to maintain these page tables.

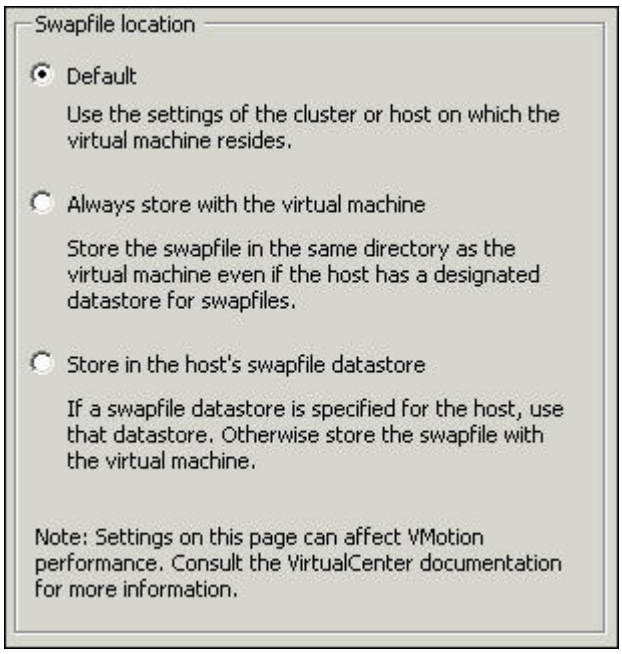
This function of the VMkernel has now been ported to the newer CPUs. You can regard the virtualized MMU as being akin to other process assists such as Intel-VT and AMD-V enhancements. This feature is enabled by default in VI-3.5. The default settings uses a discovery process and basically states – if the CPU supports the virtualised MMU attribute – then the ESX host will use it. Other options include to hardcode the feature on or off. Figure C.42 shows the dialog box options.

**Figure C.42**




**Swap File Location:**
AS mentioned earlier, along side the global setting to relocate the per-VM VMkernel Swap file we also now have the possibility to set this value for each individual VM. Figure C.43 shows the main options available

**Figure C.43**




**Resizing Virtual Disks:**
In previous releases if you want to resize virtual disk, you had to shutdown the VM and use the command-line tool vmkfstools –X to increase the size. This functionality has now been incorporated into the VI Client. You must shutdown the VM before changing its disk size. You will find the option to increase the size of virtual disk if you edit the settings of a VM, and click the appropriate disk. Once the virtual disk has been resized then you will need to use the guest

operating systems tools to resize the partition table(s) inside the virtual disk. In the case of Windows 2008 if you increase the size of the virtual disk for the boot partition it will automatically stretch the NTFS partition to take up the new space.

## VMware Tools

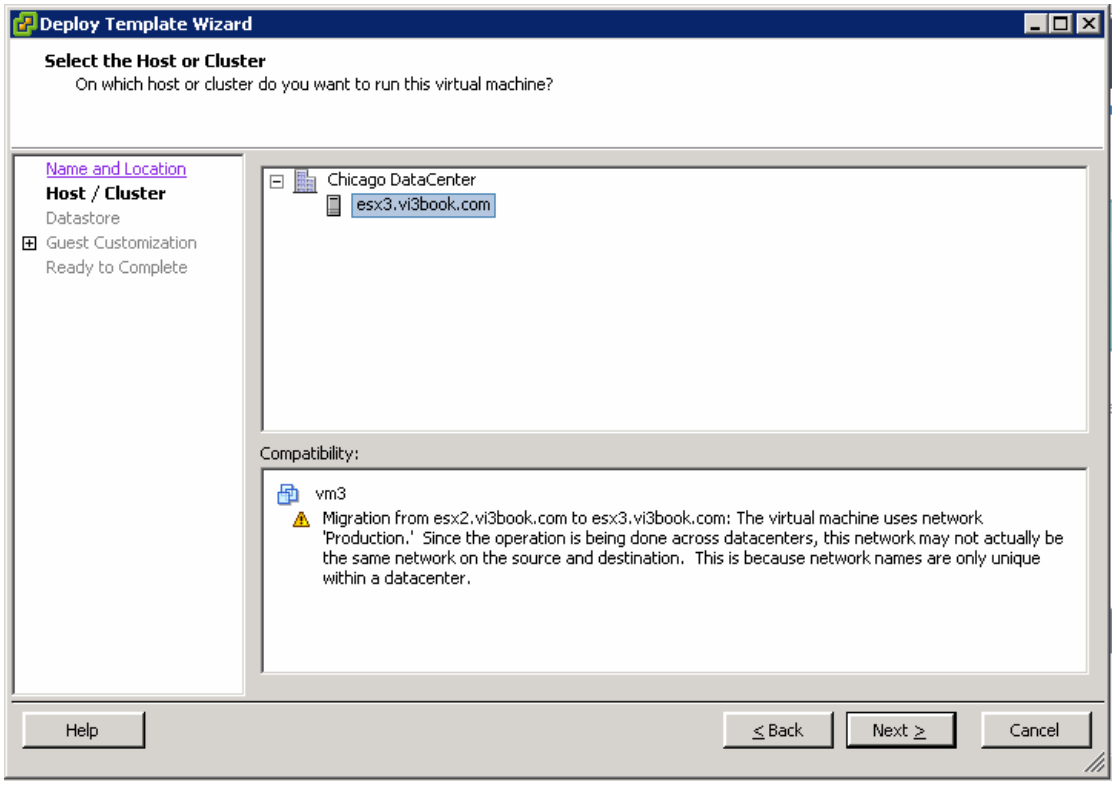
On surface VMware Tools has not change significantly in Vi3.5 except the return of a depreciated feature. VMware use the term "depreciated" to indicate that an option, feature, utility or process has either been completely removed or significantly reduced in functionality. When Vi3 first came out the "shrink" feature was depreciated. The shrink feature can be found in a Windows VM by double-click the VMware Tools icon in the tray. As you will see "shrink" is back!

What does this feature do and how it is used? You might want to use the shrink feature just before you convert the VMDK file from the "monolithic" format to the 2gb "sparse" format with either vmkfstools –I or with vcbmounter/vcbexport. The shrink feature will write out delete files with zero-bytes significantly reducing the real amount of data copied or backed up. As you probably know when you delete files in most guest operating systems the file it self is not physically deleted from the disk. What happens is files are "marked" for deletion, they don't actually get delete from the disk until a new file comes along and takes over the blocks the old file was consuming. This achieved in most operating systems by inserting a character into the file name is it know by the file system causing it to be an invalid file. Most disk cloning utilities such as Drive Image Pro or Ghost, look for these files and make sure they not included in any "images" you make. With VMware what we do is shrink the disk to remove these unwanted deletes prior to making a copy of the virtual disk – thus getting only the true data on disk.

# *Using Templates*

Creating templates and creating new VMs from them is largely unchanged. Historically, the templates resources of one datacenter have been unavailable to the ESX hosts in another datacenter. This meant you could not deploy a template registered with ESX host in one datacenter to another an ESX host in different datacenter. In practical terms this may still remain a barrier unless two datacenter share the same storage or your environment has advanced SAN replication technologies such as stretched-clustering. Where this feature is useful is where the datacenter object in VirtualCenter as a management unit rather than purely representing ESX hosts that share the same storage and network resources. If use this feature you will get warning as you select a template in one datacenter and try to use to create a VM in different datacenter. Figure C.44 shows the warning message. The concern is that the port group labels held in the template .vmtx file may not match the port group labels used in a different datacenter.

**Figure C.44**

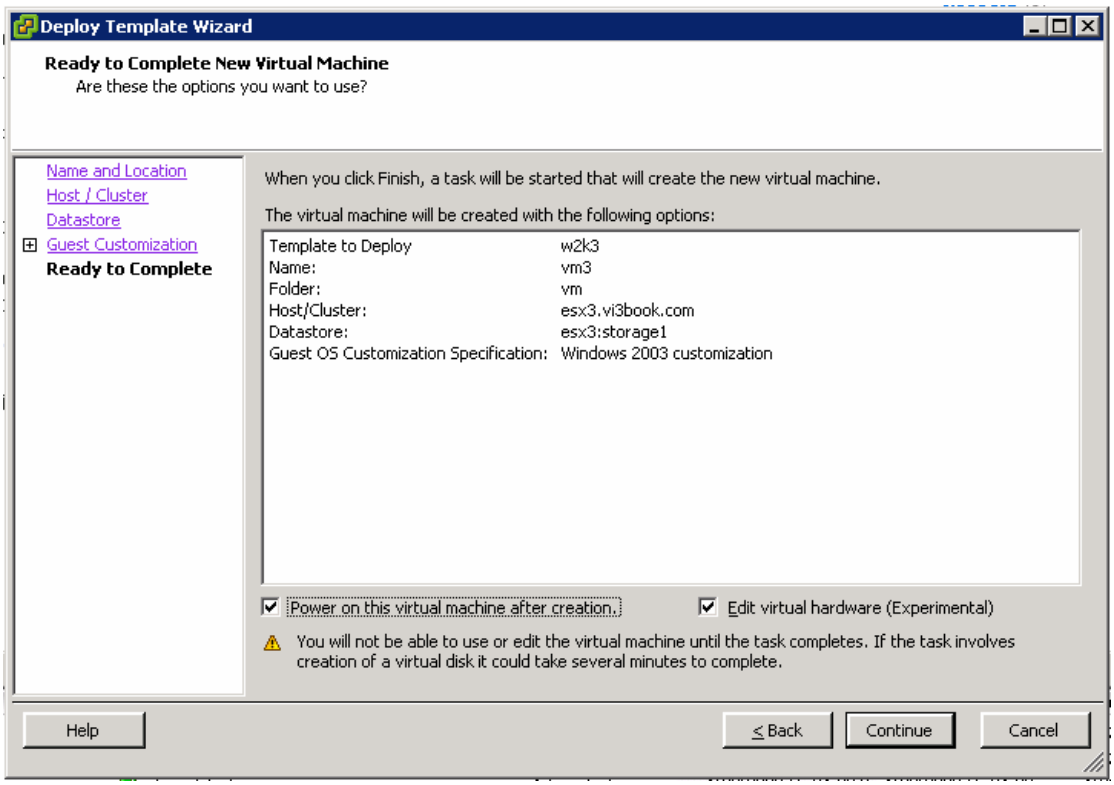



What is also new in templates is that 64-bit editions of sysprep are now supported. If you look at the directory structure for sysprep held in C:\Documents and Settings\ All Users\ Application Data\ VMware\ VMware VirtualCenter\ sysprep folder you will find folder location for the 64-bit versions of Windows 2003 and Windows XP Professional.

At the end of the wizard to "Deploy Virtual Machine from this Template" you will find there is an option to enter the "Edit Settings" dialog box shown in Figure C.45. Currently in the Release Candidate this option is marked as "experimental". The option to power on and edit the VMs settings are not enabled by default. If you enable both at the same time, the edit settings dialog appears first, then the VM is created and then lastly it is powered on after clicking OK in the "Edit Settings" dialog box.

There's an edit (experimental) option at the end of the guest customization

**Figure C.45**



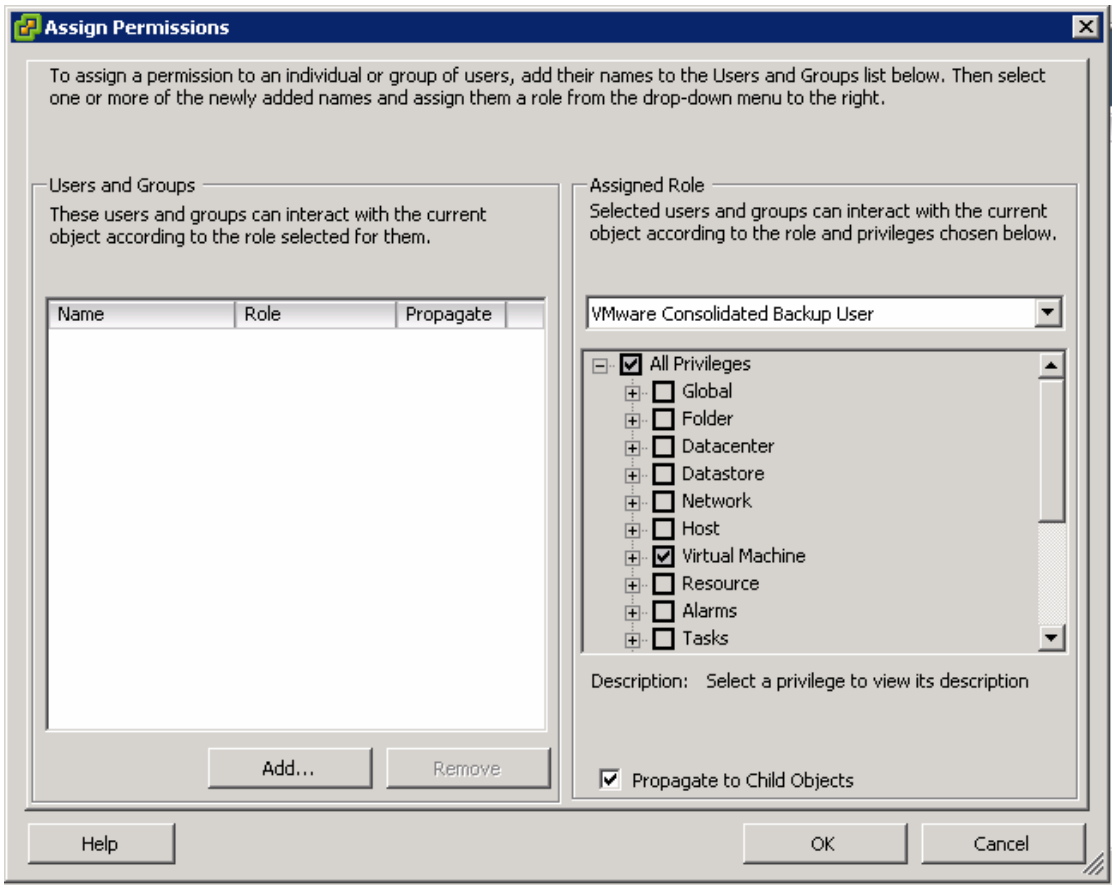

# *Access Control*

Access control is another word for setting permissions within the VirtualCenter environment. The structure of Access Control has not significantly modified. However, there is a new role type designed for setting the minimum permissions required for creating a dedicated user account required for using VMware Consolidate Backup. The role is called VMware Consolidate Backup User. This role is allocated the following virtual machine permissions:

- State: Create and Remove snapshot
- Configuration: Disk Lease
- Provisioning: Allow Read-Only Disk Access
  Allow Virtual Machine Download

Figure C.46 shows the new role in the "Assign Permissions" dialog box.

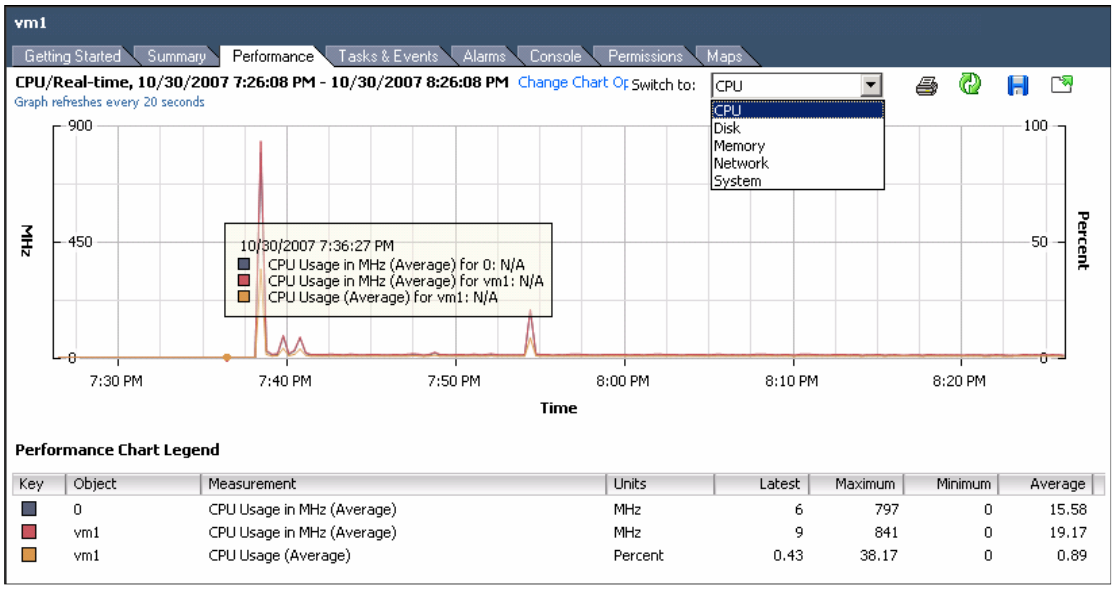
**Figure C.46**




# *Resource Monitoring*

Once again there are no significant changes to performance monitoring once again although there has been some finessing of the user interface. Figure C.47 shows that there is now a quick and easy way to switch between viewing different four core resources (CPU, Disk, Memory and Network) and the internal system resources (system)

**Figure C.47**

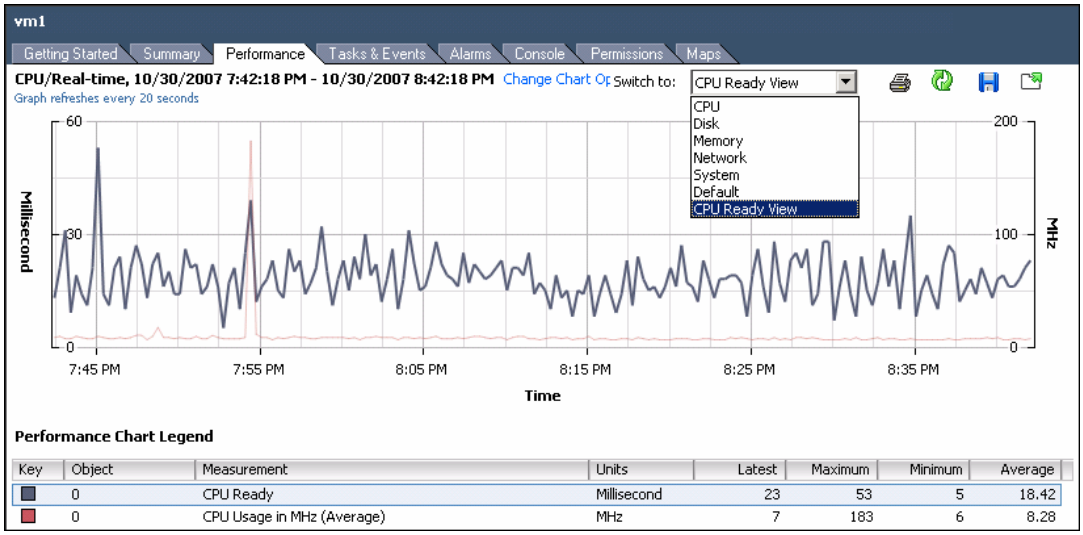


Different chart views are also available – and enables the quick switching from different views in the VI Client. This can be achieved by click the "**Change Chart Options**" button in blue. After changing your settings such as adding additional counters. The "Customize Performance Chart" dialog box has a "Save Chart Settings" dialog button and the top of the dialog box allows you to switch to various chart view. The following instruction will demo this feature to you.

1. Select a VM and the **Performance Tab**
2. Select the **Change Chart Options** link
3. Remove the tick under **Objects**, **Description** and **0**
4. Under **Counters** part of the dialog box enable the counter called **CPU Ready**
5. Click the **Save Chart Settings** button, and type in a name for this view in the dialog box – for example you could call it CPU Ready View

   Figure C.48 shows the resulting custom view in the VI Client

   **Figure C.48**



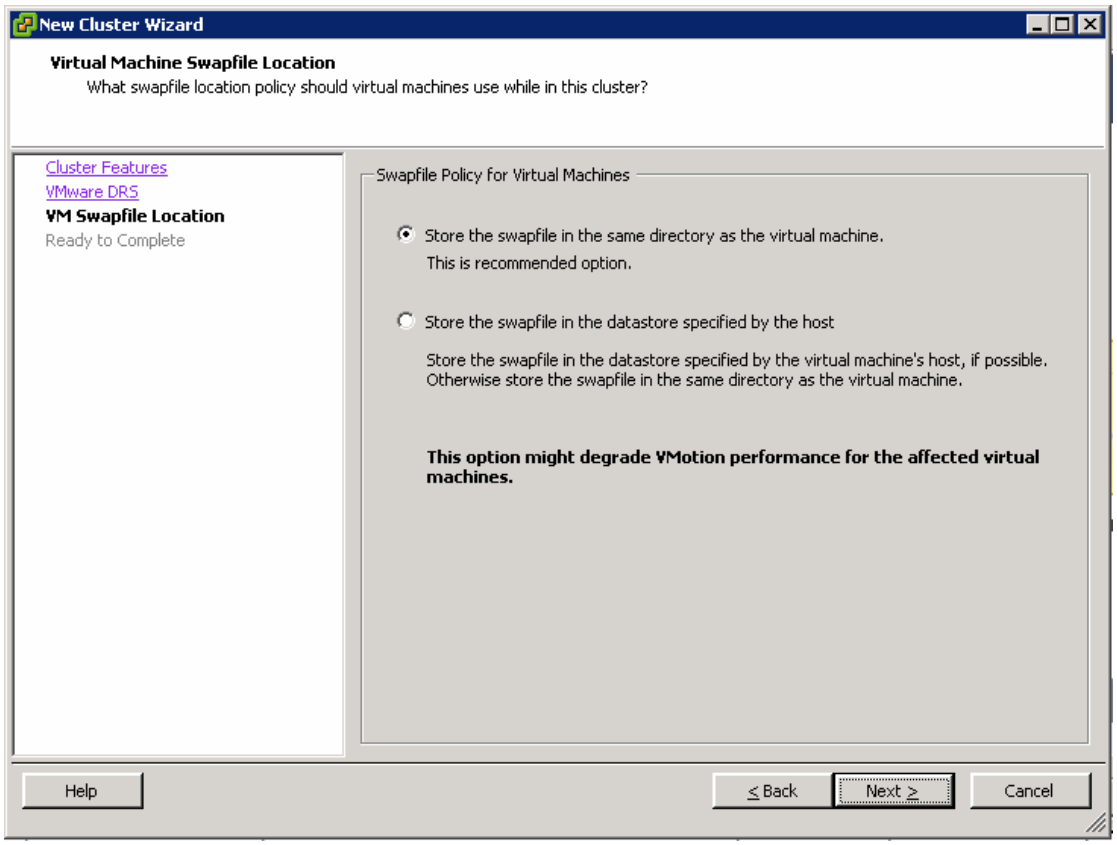

# *VMware DRS*

VMware have introduced a number of enhancements and improvements to both DRS and HA clusters not least increasing the number of ESX hosts allowed to be 32 for both DRS and HA.

## DRS and the Virtual Machine Swap File

As we saw in the ESX installation and the VM configuration options there are new options for where to store the VM's swapfile. This is also present running through creating DRS cluster wizard. Figure C.49 shows the dialog box in question which allows you set the swapfile to be created in the same directory as the VM, or in location specified in Configuration Tab of the ESX hosts. Again, the recommendation is store the swapfile in the same location as the VM, as locating it elsewhere could degrade performance.

**Figure C.49**




# DRS Recommendations

As you may know in manual or partial mode DRS works on system of "recommendations" a system of dialog boxes and tabs are available when you power on a VM or when DRS detects it would be appropriate to move VM to rebalance the cluster of ESX hosts for memory or CPU usage. There are new and improved dialog boxes if you operate your DRS clusters in either manual or full-automated mode. Figures C.50 and C.51 show the new power on dialog box and the DRS Recommendation Tab.

**Figure C.50**

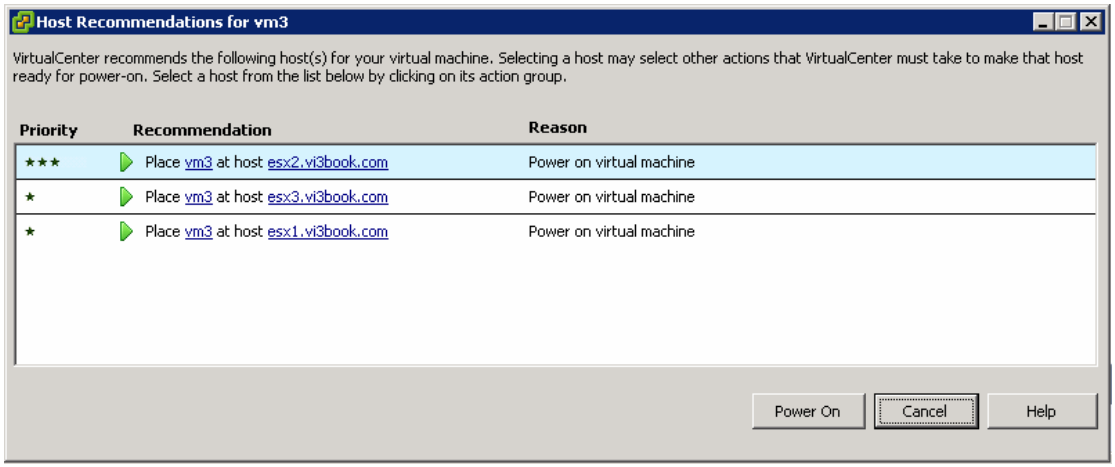
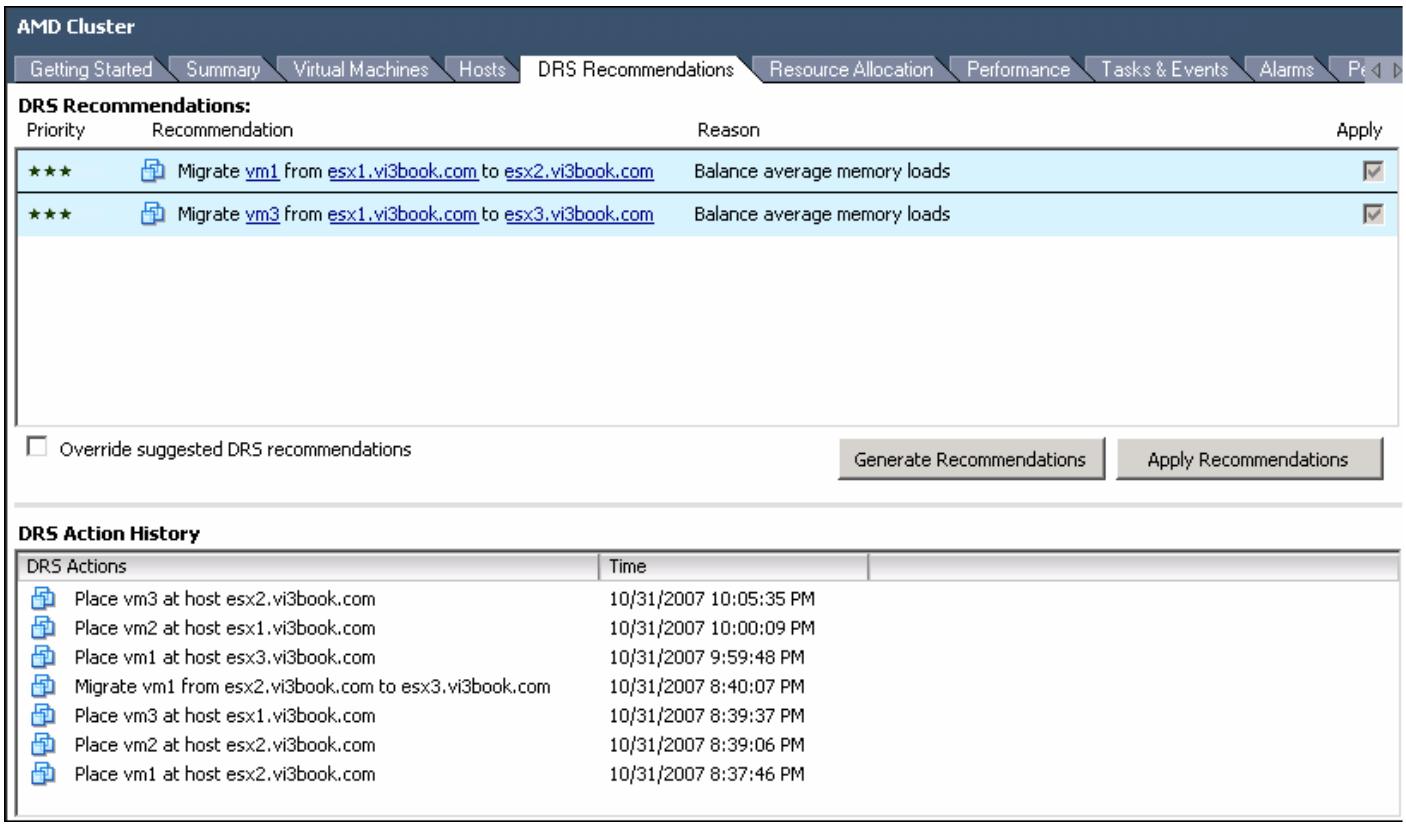


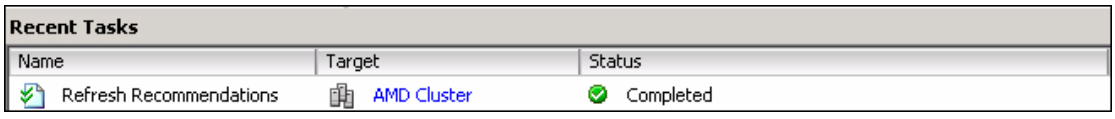

**Figure C.51**




More or less the functionality offered here is much the same as previous versions. However, you can probably spot the difference if you are already familiar DRS already.

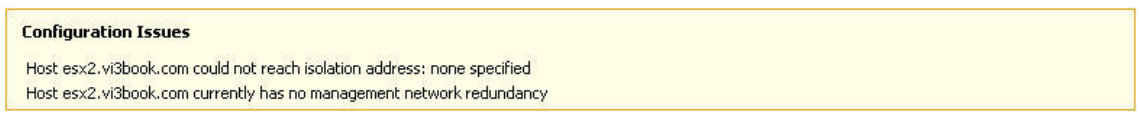
- The new "DRS Action History" gives you a much clear view of events that happened in the cluster
- The Apply option allows you to select the migrations you wish to migrate – prior to clicking the "Apply Recommendations" button. As you can see its dimmed in the screen grab. Enabling the option to "Override suggested DRS recommendations" turns on the apply column option
- The "Generate Recommendations" forces DRS to re-check the cluster for DRS cluster imbalances, rather than waiting the default which is every 5 minutes. Clicking this button will generate a "Refresh Recommendations" in the Recent Task bar. Figure C.52 shows this refresh occurring

**Figure C.52**




In addition to this improved status information you will also get alarms and alerts on ESX hosts which are similar to the alarms and alerts within clustering generally. You might find these more useful than the simpler "HA Agent Failed" to start messages. Figure C.53 shows a HA rather than DRS message.

**Figure C.53**



## DRS and Maintenance Mode

In VI-3.5 maintenance mode has been improved. When maintenance mode was triggered in the past it would only move VMs that were powered on. In this release maintenance mode will also move VMs which are powered off and suspended. Whilst this is an improvement, templates which are registered with an ESX host in maintenance mode are still unavailable, until maintenance mode has been exited. In the past maintenance mode in with manual or partial automated DRS would generate a whole list of 5-Star recommendations. This no longer happens and VMs are just moved automatically. It's assumed if you are entering maintenance mode you want to evacuate the ESX host of all VM's.  Figure C.54 and C.55 show the new maintenance mode prompts that indicate that suspended and powered VMs will be moved also.

**Figure C.54**

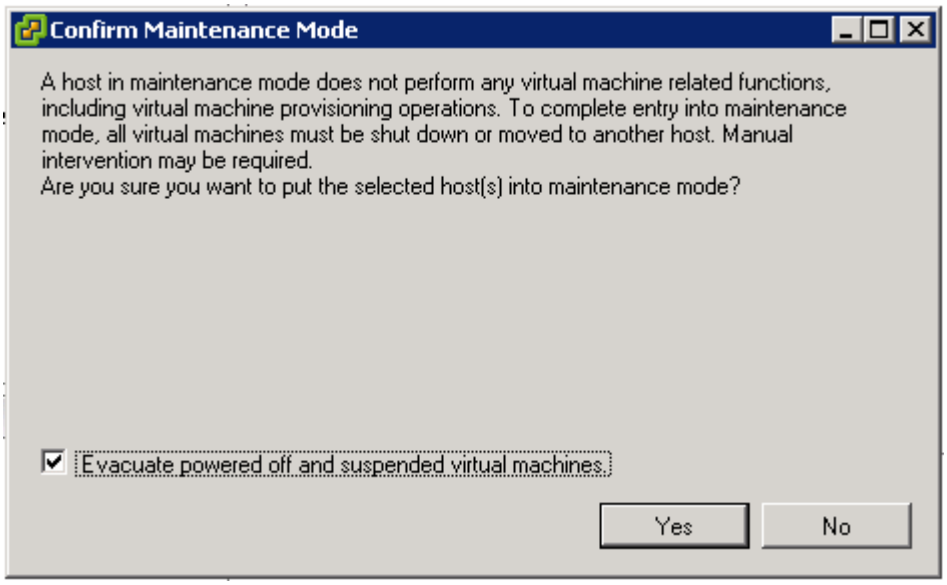



**Figure C.55**


# *Distributed Power Management (DPM)*

## What is DPM?

In recent years there has been much talk about creating a "Green DataCenter" – a drive to consume less power is intend to have both an economic and environmental impact. According to most independent analysis servers represent about a third of the power consumed with network and storage devices representing similar amounts.

Distributed Power Management (DPM) addresses this concern is integrated into DRS. Its job is monitor the clusters usage, and move VMs during non-peak usage to a fewer number of ESX hosts. The unneeded ESX hosts are put into a standby mode, so consume less power in the server room. DPM is integrated into DRS such that other rules such as reservations and affinity rules are obeyed. For some people the idea of VMware powering down and up their physical servers will be something they nervous about especially in their production environment. Like many I'm of the "old school" that believes once something is on, it should be left on – for fear it might not come on again! However, putting these worries aside, DPM may come into its own in environments where the "always on" approach is less significant. So in your test and development or DR environments it's extremely wasteful having servers powered on when they simply not needed.

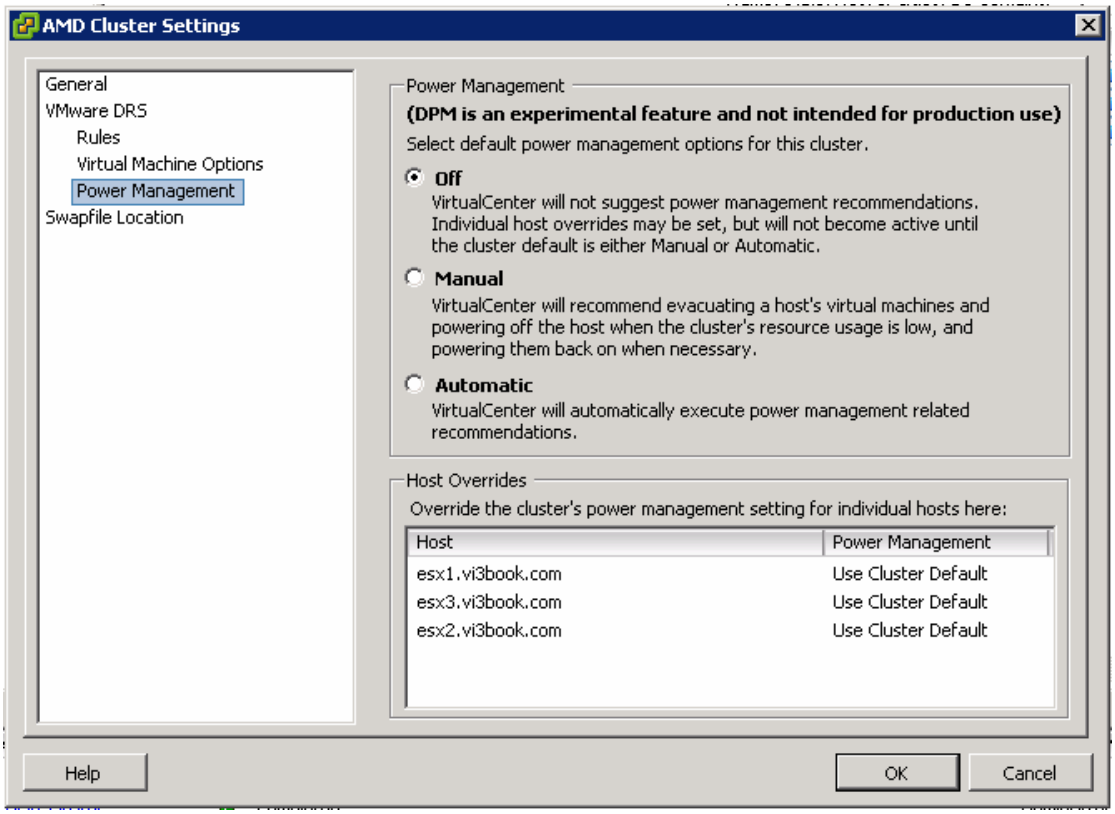
DPM maintains a lookup table for the amount of power consumption – and three main conditions are used to calculate DPM process. It monitors:

- Guest CPU and Memory usage
- ESX host CPU and Memory usage
- ESX host power consumption

Like DRS, the algorithm behind DRS is a conservative one, and here's some the reasons why. For a start DPM takes into account a load history over a twenty minute period for power off events. For power on events it checks every five minutes, after all you do not want to wait too long for an ESX host to be powered on if more resources are needed. Using DRS VMs are grouped into either highly loaded VMs or lightly loaded VMs. If DRS detects that the highly loaded group is using more 80% of the resources then this will trigger a power ESX power on event. If DRS detects that the lightly loaded group are using less than 45% of the resources then this will trigger a power off an ESX host. Using these two constraints DPM runs a number of "What if" simulations to work which are the best VMs to move, to allow the power off of the best ESX hosts. DPM also interacts with VMware High Availability so it does not power off that many ESX hosts that it breaks your rules for the number of ESX you tolerate in a failed state – or put another way whether you have +1, +2, +3 or +4 redundancy.

The DPM feature is enabled on the properties of DRS cluster and is by default switched off. As with DRS it can be configured in a "manual" mode where it offers recommendations which can be ignored or followed, or automatically where DPM carries a standby function automatically. Additionally, an option exists to exclude specific ESX hosts from the DPM process referred to as "Host Overrides". Figure C.56 shows the DPM configuration dialog box on the properties of a DRS cluster

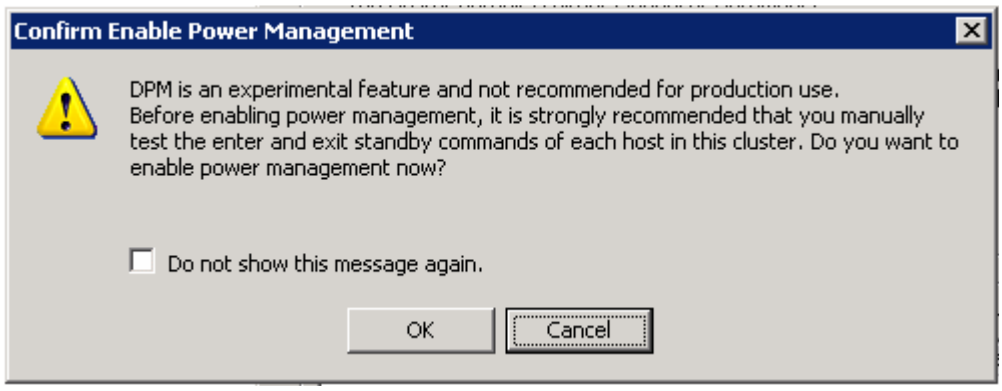
**Figure C.56**




## Confirm & Testing Standby Mode

When DPM is enabled with manual or automatic, a dialog box appears suggesting that the "standby" option is tested on each ESX host to confirm they support soft-power on. Figure C.57 shows this warning dialog box.

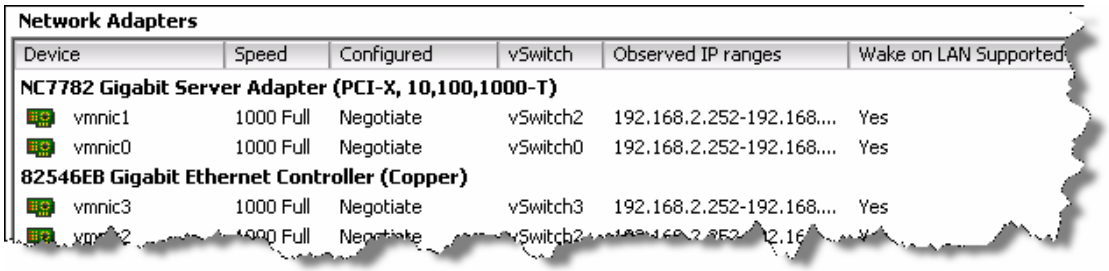
**Figure C.57**




The soft-power on is functionality is achieved by leveraging the "Wake on LAN" feature of most modern network cards and power supplies. You can confirm if this enabled on your ESX hosts by:

1. Select an ESX host
2. Click the **Configuration** Tab
3. In the **Hardware Pane**, select **Network Adapters**
4. As in Figure C.58 you should see in the "**Wake on LAN supported**" column the words "**Yes**" next to each NIC

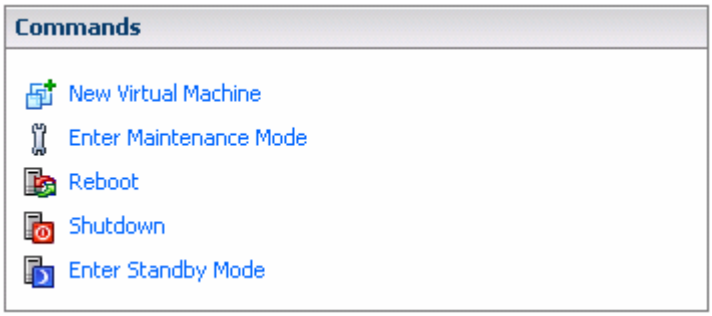
   **Figure C.58**




**Note:**
With or without DPM enabled, all ESX host have an additional power option available on the "Summary" tab and on the right-click menu of an ESX host in the VI Client. It is recommended that you test that each ESX host can enter and exit this standby mode correctly before enabling DPM. Figure C.59 shows the Summary tab and the new "Enter Standby Mode" option. As with maintenance mode this should trigger either five star recommendations or automatic VMotion events dependent on the level of automation you have selected for the DRS cluster.

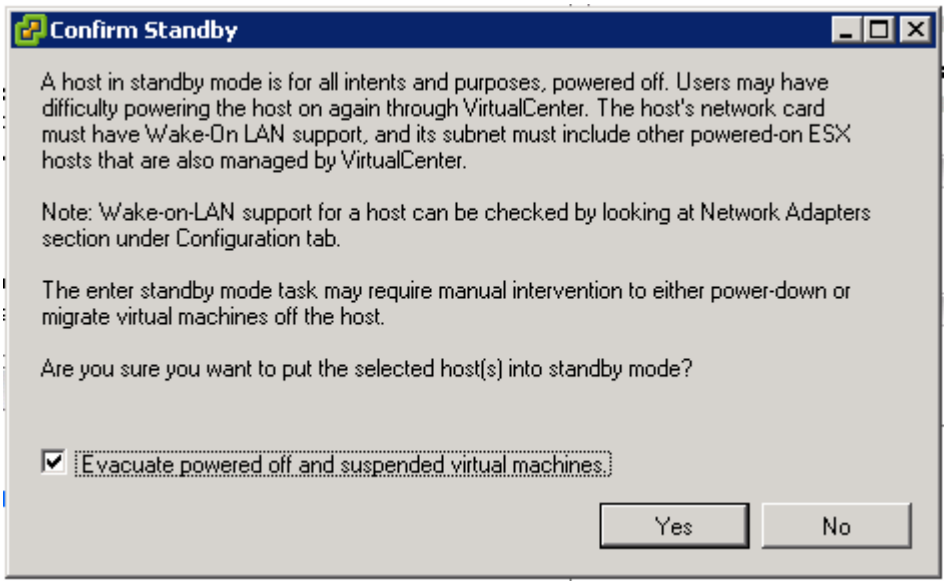
5. Select the **ESX host**, and click the **Summary Tab**
6. Select the option "**Enter Standby Mode**" as shown in Figure C.59

**Figure C.59**




7. Click **Yes**, to the **Confirm Standby** dialog box (Figure C.60)

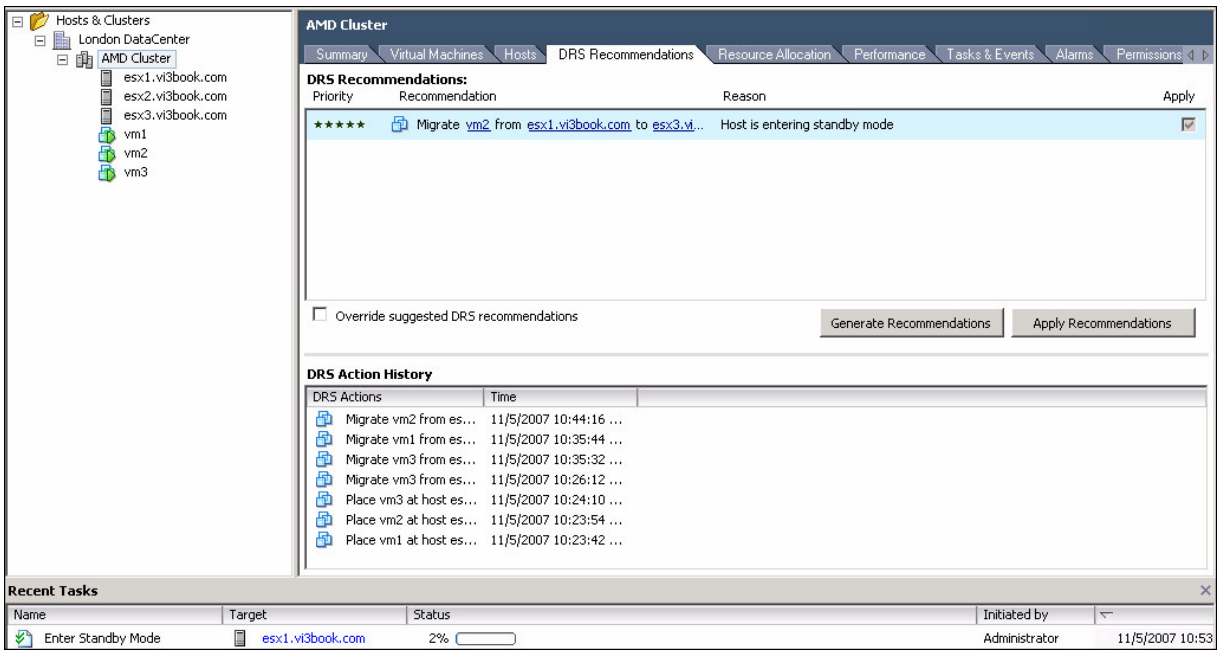
**Figure C.60**




**Note:**

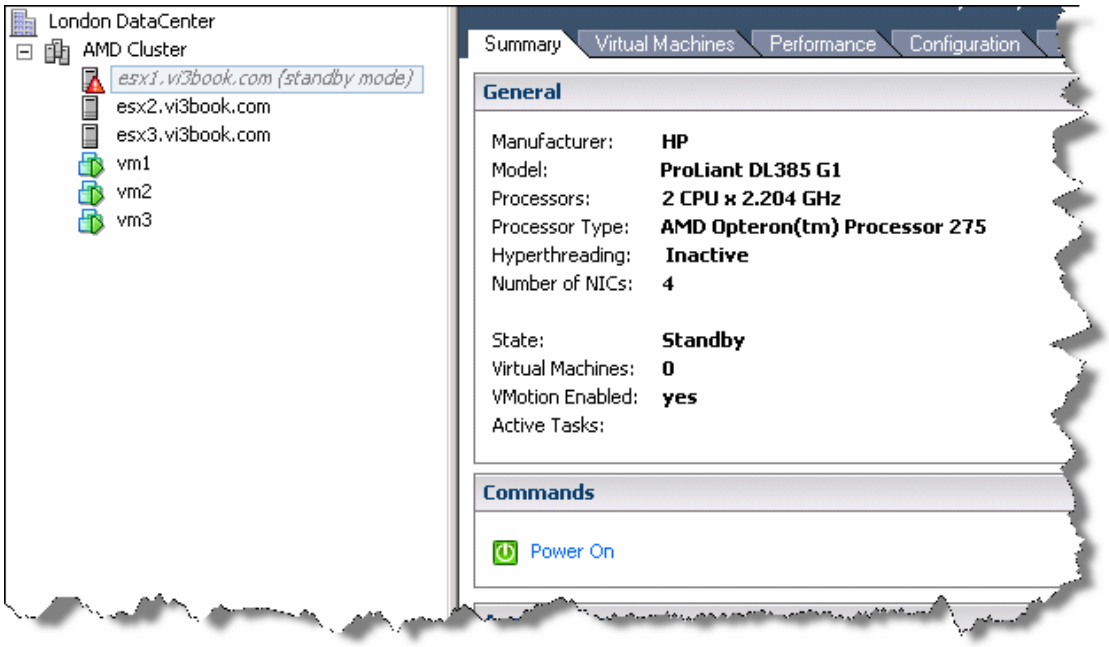
As with maintenance mode, standby mode can "hang" as it waits either for the operator to confirm the VMotion of VMs, or because a VM cannot be moved due to not meeting VMotion requirements. Figure C.61 shows the DRS Recommendation tab waiting to be confirmed. The recommendation is has five stars because it is a logical requirement to move the VMs before standby can complete. Note that the "Recent Task" bar shows "Enter Standby Mode" waiting on 2% as waits for the operator to accent the recommendation. If DRS is configured for fully-automated mode, the VM would be moved without these prompts.

**Figure C.61**




Once standby mode has completed the ESX host will appear dimmed in VirtualCenter with the words "Standby Mode" in brackets next to its name. This is very similar to status messages of "Not Responding" or "Disconnected" when a network or management agent error separates VirtualCenter from an ESX host. Additionally, the ESX host will only have one option available to it on its "Summary" tab which is to power it back on. Figure C.62 shows this new status information and the new power on button

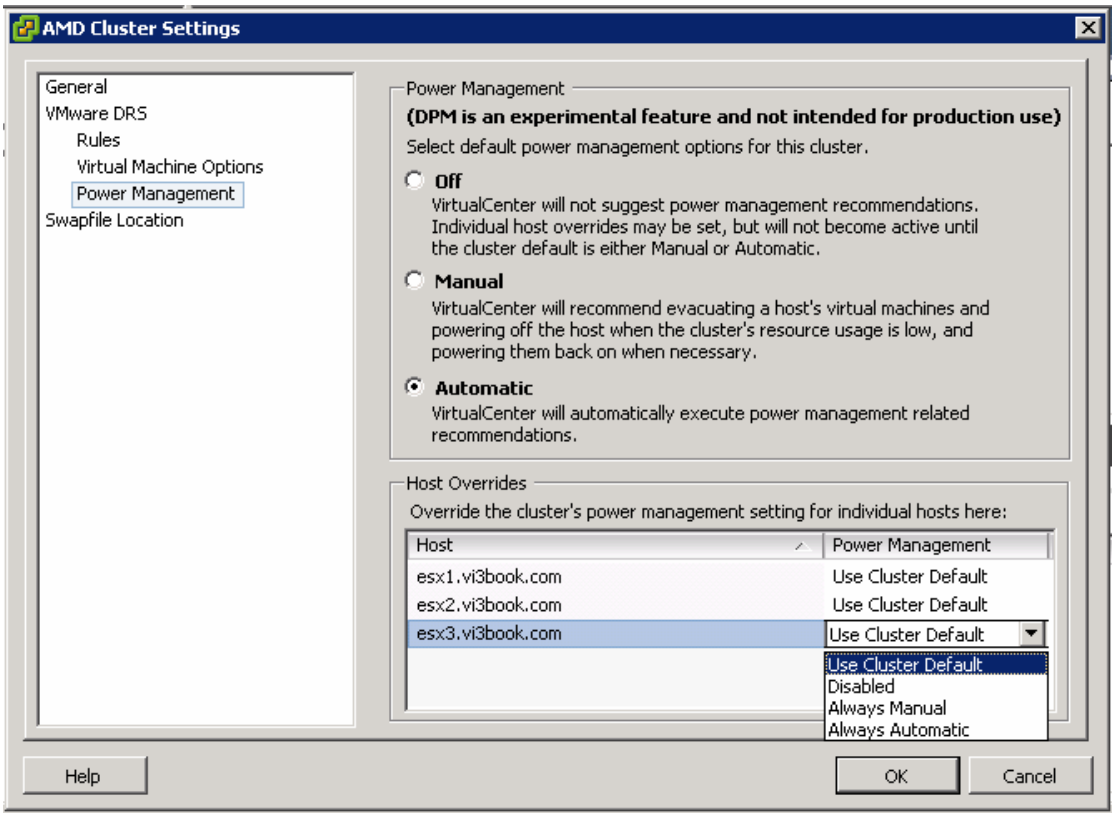
**Figure C.62**




## Enabling DPM on a Cluster

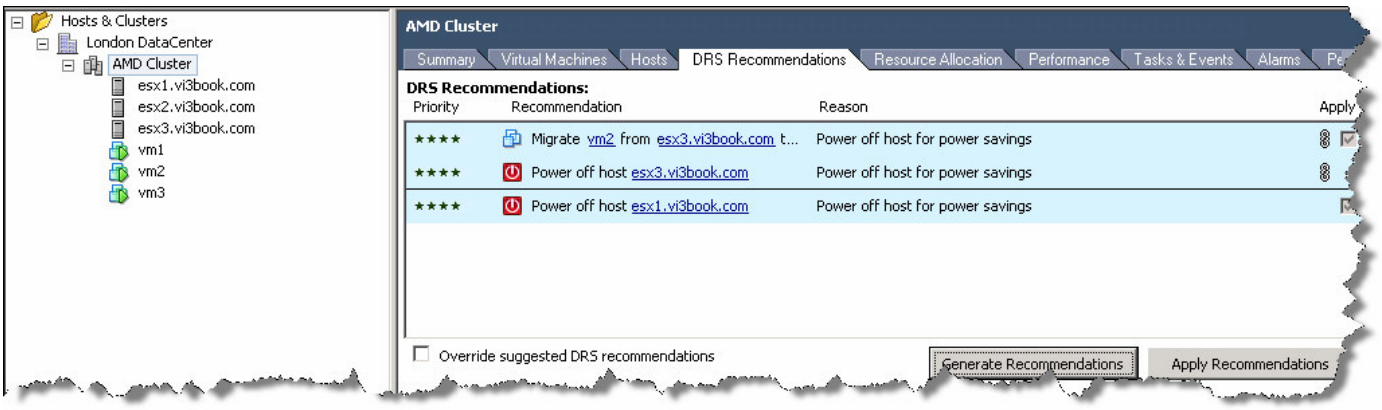
Once you are entirely convinced that entering and exiting standby mode is reliable, then it is possible to enable DPM on the cluster. As stated before your options are simple to either enable it in manual mode or automatic mode. Any configuration you can imagine can be configured depending on the policy of your organization. One reason to have "Host Override" is for ESX host that don't support the Wake On LAN feature or in your testing, you discover that they do not work reliably with the DPM feature. Figure C.63 shows a DPM cluster set to use automatic, with esx3.VI-3book.com about to be set with the option to disable DPM altogether (in fact esx3.VI-3book.com does work reliably with the DPM feature).

**Figure C.63**




If you decide to use the manual mode a new set of recommendations will appear when DRS and DPM decide that given the resource demands made by the VMs it would be power efficient to put some ESX hosts into standby mode. Figure C.64 shows the DRS Recommendation tab and the new four star recommendations generated under these circumstances.

**Figure C.64**



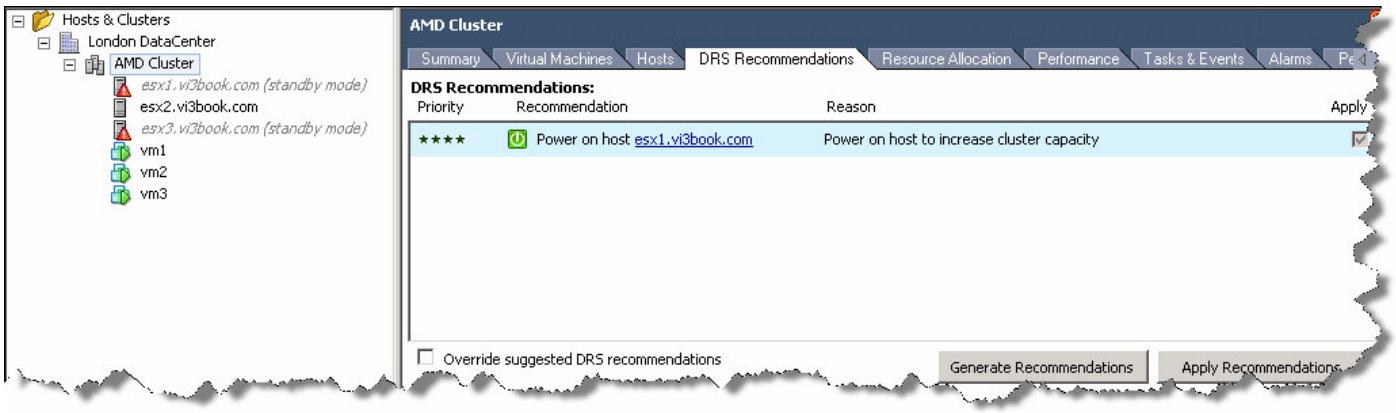

In this case I am running very few VMs which are doing very little in terms of workload. DRS and DPM has decided to move VM2 from esx3 to esx2, and put esx1 and esx3 into standby mode to save on power. In this case I would only have one ESX host running in the DRS cluster. These are the kinds of recommendations one would receive if you hadn't yet enabled VMware High Availability where at least two ESX hosts would be left powered on to maintain a minimum level of fault-tolerance.

**GOTCHA:**

By default this would generate to alarms for as there is an alarm condition created by default called "Host Connection State" unfortunately VirtualCenter is not aware yet that the reason for the disconnection is not a network failure but due to standby mode being triggered.

As you might expect – if you're VMs subsequently begin to demand more physical hardware resources such as CPU and RAM. Then DRS and DPM will together generate recommendations that ESX host should exit the standby state and be powered on again. Figure C.65 was generated by running a CPU intensive script inside one of the VMs, and by increasing the amount of memory allocated to two of my VMs.

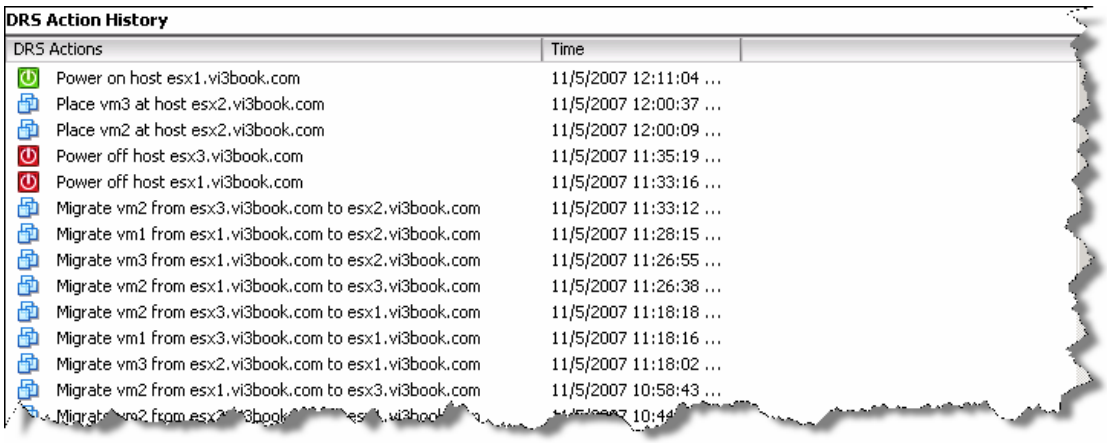
**Figure C.65**




Again these recommendation do not appear if DRS is in fully automated mode – ESX host are powered off and on-demand as and when the VMs need the resources during off-peak and peak hours. In future capacity planning exercises must be done upfront before going into production - unless you wish explain to your boss, why the thousands dollars worth of servers you have purchased spend most of their time powered off during the day!

As stated before the DRS Action history log does a much better job of tracking and tracing both VMotion and DPM events than in previous releases of VI-3. Figure C.66 shows the DRS Action History log with both VMotion and DPM activity

**Figure C.66**




# *VMware HA Clusters*

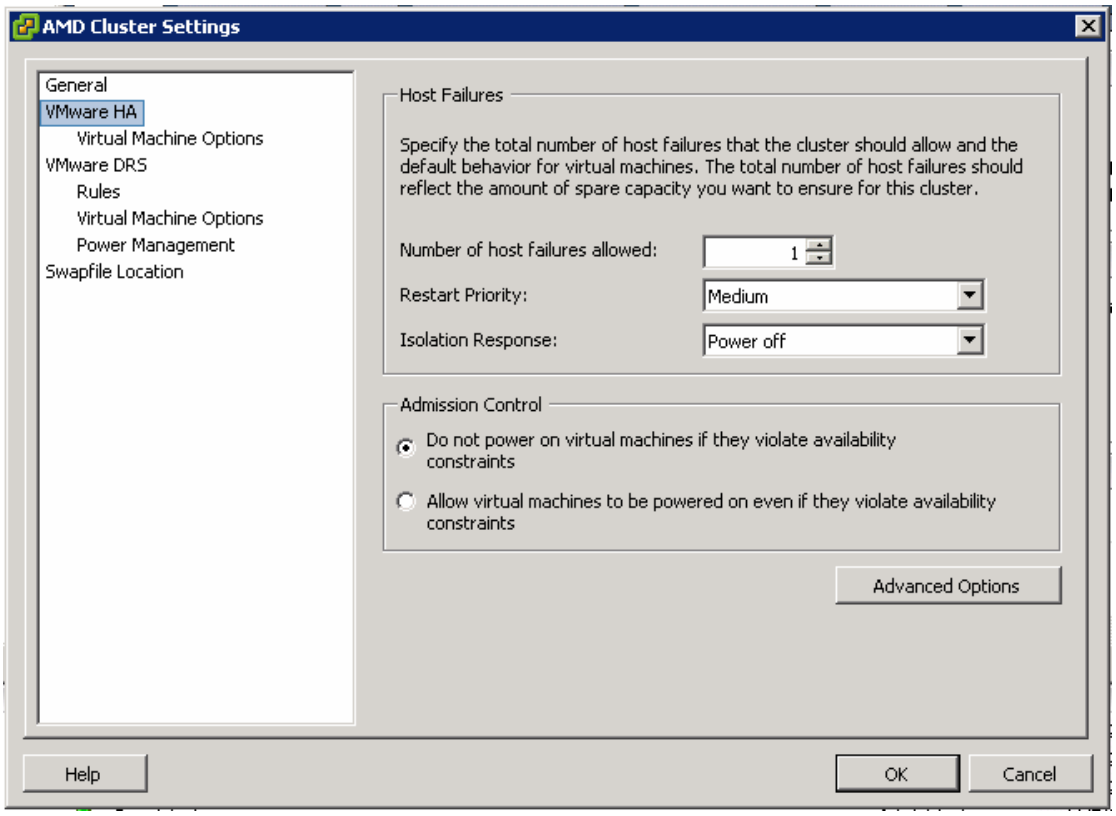
A number of critical enhancements have been introduced in VMware High Availability. In past the total number of ESX hosts in a cluster differed; DRS was tested up to 32 and HA was tested to 16 ESX host per cluster. This effectively makes the maximum number of ESX nodes in a cluster 16

as most customers would configure both DRS and HA features. In VI-3.5 the number of ESX host per cluster is now the same for both DRS and HA – 32 ESX host per cluster.

The logic of HA has been improved as well. In the previous release, when an ESX host failed virtual machines were powered on the remaining ESX hosts. The algorithm for power on was quite simple. The ESX host selected for the VM power on event was select by host name (esx1, esx2, and so on) and based on that hosts ability to meet any reservation settings. In the VI-3.5 release VMs are powered on the ESX host with the largest amount of free CPU and memory resources. In the other words the best ESX host is selected.

Lastly, VMware HA has new options on the main page where it is configured. Figure C.67 shows how the new configuration dialog box allows you configure global settings for start-up priority and isolation mode.

**Figure C.67**




**GOTCHA:**
Remember it is entirely possible to manually enter an ESX host into the Standby Mode regardless of the HA settings. This is similar to maintenance mode. This allows the shutdown down of ESX host; even with a two node HA cluster.

## Per VM Failures

In the past VMware HA could only deal with the failures of the ESX host. In this release VMware monitoring the VM looking for a failure of the guest operating system or the VM itself. If the is detected then VMware will restart the VM automatically.

## Per VM Heartbeat Alarms

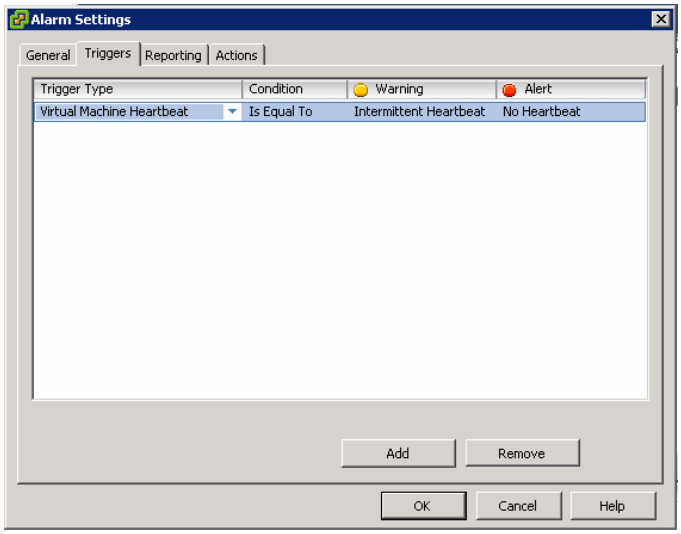
In the new release it is possible to monitor the guest operating system, and restart it if it has stalled. Additionally it is possible to automate reboots after a configured interval for VMs that

have a reputation for predictable failures such as applications that exhibit memory leaks. In fact this functionality was once part of VirtualCenter 1.x.x and ESX 2.x.x but was "lost" in Vi3.

The feature is essentially part of the Alarms and Alerts feature and is very easy to enable:

1. Select the container "**Host & Clusters**" and Choose **Alarms**
2. Click the **Definitions** button
3. **Right-click anywhere in the Window** that lists the current definitions, and select **New Alarm**
4. **Type a new alarm name** such as "Virtual Machine Heartbeat Status"
5. In the dialog box under "**Alarm Type**" choose to "**Monitor a virtual machine**"
6. Next, click the **Triggers** tab and select the **Add** button
7. **From the pull down list** select "**Virtual Machine Heartbeat**" as the Trigger type. Figure C.68 shows configuration box at this point

   **Figure C.68**




8. Next select the **Actions Tab** and Click the **Add button**
9. **In the pull down list**, change **Action** to be "**Reset a VM**"

   **Note:**
   Ensure the condition is "From yellow to red"

# *ESX on the Command-Line*

## Configuring NTP

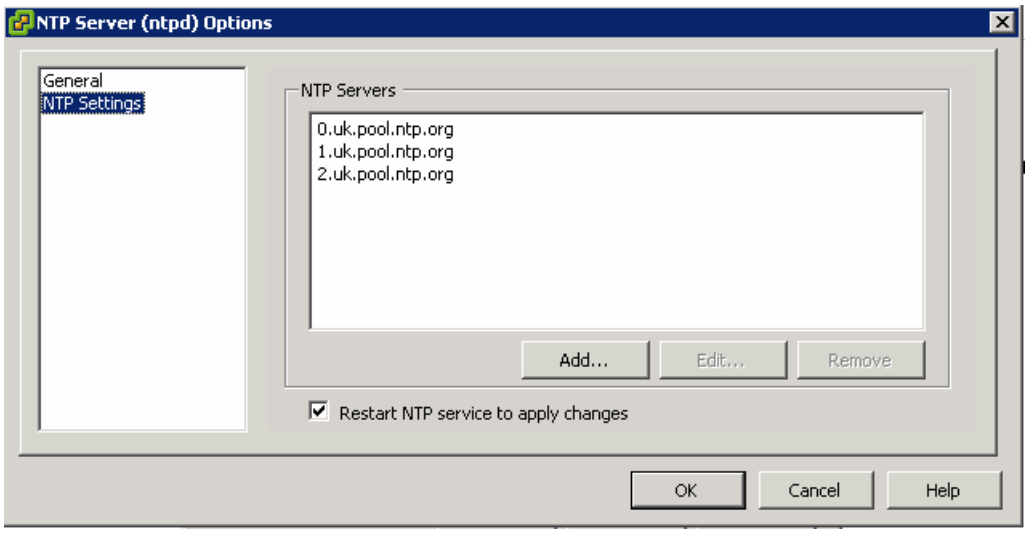
The vast majority of the command-line tools are unmodified in ESX 3.5. In fact some of the configuration that normally was only available at the command-line is now available from the VI Client. A case in point is the configuration of the NTP Service. This can all be done without resorting to text editor such as VI or nano.

1. Select the **Configuration Tab**, and in the **Software pane** choose option **Time Configuration**
2. Click **Properties…** option on the right-hand side of the VI Client
3. In the **Time Configuration** dialog box select the **Options…** button
4. In the **NTP Server (noted) options dialog**, select **General** and click the **Start** button
5. In the **NTP Server (noted) options dialog box** choose **Add**
6. **Type in the FQDN or IP addresses of the NTP services** you wish to synchronize with

7. Lastly **enable the option** to "**Restart the NTP Service to apply changes**" and Click **OK**

   **Note**:
   Figure C.69 shows the NTP Server NTPD options box

   **Figure C.69**




## Using the Remote CLI

In Appendix B: ESX3i we showed how it is possible to enable a "physical" console for the ESX3i product and also how it is also possible to download via the virtual machine importer tool a VM which acts as the CLI for ESX3i. With the release of the full VI-3.5 toolset a third option has been created. It is possible to install a Remote CLI tool to your management PC to manage an ESX3i and 3.5 host. The Remote CLI works with Windows or Linux systems. Once installed Remote CLI does not differ in functionality where you run the commands on a Window or Linux management PC.

In the Beta/Release Candidate I found after installing the Remote CLI tools that neither the path to the tools or the Active Perl Toolkit upon which it was dependant were set as environmental paths. This means at the command-line you will receive either "'…is not recognized as an internal or external command, operable program or batch file" messages or message stating that libxml2.dll is missing. To remove these annoyances add these paths to your windows environmental variables:

C:\Program Files\VMware\VMware VI Remote CLI\bin
C:\Program Files\VMware\VMware VI Remote CLI\Perl\bin

You can see an entire list of all the Remote CLI commands in the C:\Program Files\VMware\VMware VI Remote CLI\bin directory. You can receive help by using a command together with the command together with -?. Additionally, sometimes the CLI commands have a "perl document" created for them – this not unlike the "man" utility that is available in the Service Console – so issuing the command perldoc svmotion.pl would print the help information on the storage VMotion command. However, I would be for the moment very cautious with some of the examples given with the Remote CLI utilities – as occasionally often they are wrong!

The syntax used to list the vSwitch on an ESX host directly would be

**esxcfg-vswitch.pl -l --username** root **--password** VMware **--server** esx1.VI-3book.com

to do this via VirtualCenter you would use the equivalent vicfg command

**vicfg-vswitch.pl -l –-username** VI-3book\administrator **--password** vmware **-h** esx1.VI-3book.com

# *Storage VMotion*

**Note:**
At the time of writing this document I had some difficulty getting Storage VMotion working non-interactively. It threw up a number of internal errors. However after some effort I was able to make the non-interactive method work. This said an "interactive" Storage VMotion from the command-line was always successful and easy to follow.

Storage VMotion is a new feature which you may have already used in the migration process from ESX 2.x.x to ESX 3.0.1. Since ESX 3.0.1 we have been able to move running ESX 2.x.x VMs from VMFS2 to VMFS3 volumes. The feature back then had a community name of "DMotion" and was intended to offer zero downtime for upgrades. This term "DMotion" is not an official VMware term, but comes from the fact that the delta files created during the VMotion process have name "DMotion" in them.

This feature has been extended to allow the movement not of a VM from one ESX host to another, but from one datastore to another – in fact the VM is kept on the *same* ESX host while the VMs are "moved" to another datastore. Storage VMotion can relocate the entire VM, or just individual virtual disks using the –-disk option. The advantages of Storage VMotion are many and include:

- Free up space in VMFS volumes that are full or part of a general storage/LUN reconfiguration
- Cope with future upgrades where the VMware File Systen has changed
- Disk Performance optimization by re-blending VMs to reduce disk contention
- Solve disk location problems where users have created VMs on local storage rather than shared storage

Storage VMotion has some key requirements and limitations. Right now the feature is only available from the Remote CLI although VirtualCenter already has the option to move a VMs files during using the cold-migration wizard. VMware do plan for the feature to be integrated in VirtualCenter in future releases. We hope this will be the case once VI-3.5 has become GA.

As with VMotion there are virtual machine and ESX host restrictions. This list is quite extensive

- Virtual machines with snapshots cannot be migrated
- Virtual machine disks must be in persistent mode or be RDM's
- The host on which the virtual machine is running must have sufficient resources to support two instances of the virtual machine running concurrently for a brief time.
- Only one migration can occur per datastore at any one time
- The host on which the virtual machine is running must have access to both the source and target datastores.
- VMotion must be setup and licenced the host
- You can't move a VM with NPIV enabled
- You can't VMotion whilst performing a Storage VMotion
- If you have a VM with more than one VMDK stored on different VMFS volumes – and you move it without using the "—disks" option – it will take all the VMDKs and put them in a single VMFS volume

The reasons behind these restrictions are obvious once you know how Storage VMotion works. Firstly, the VM cannot have snapshot currently applied to it, this is because the Storage VMotion feature uses snapshots to "unlock" the files of the VM thus allowing them to be "moved" to another VMFS volume. Secondly, the ESX host needs free memory and CPU resources of the

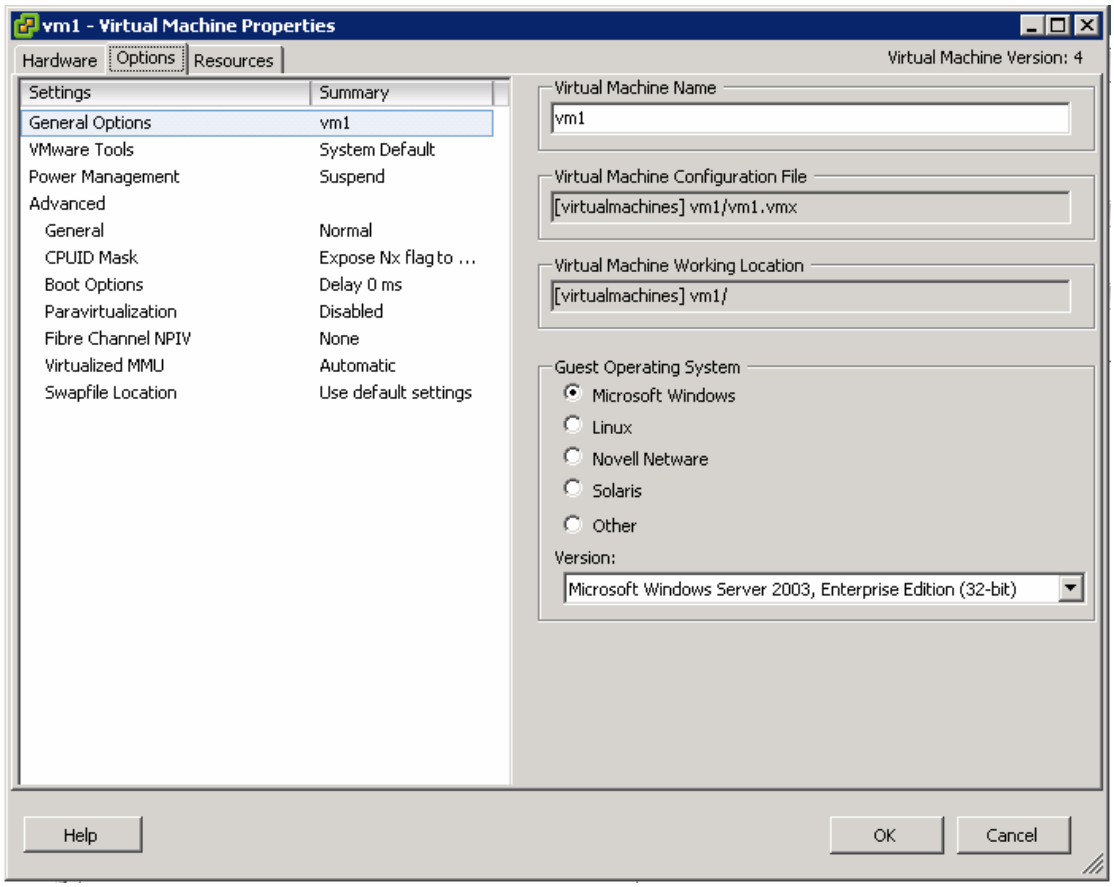
same amount as the VM being relocated – this is sometimes referred to as "self-VMotion" by VMware. The internal Storage VMotion creates a hidden copy of the VM which is similar to the hidden VM used within VMotion. This allows a seamless switch over to the VM which has been duplicated in a different storage location from the original VM on the original storage location. For this reason the requirements of VMotion extended to Storage VMotion – for example VMotion must be enabled and licensed.

The Remote CLI utility "svmotion.pl" can be used interactively (it prompts you for the required options) or non-interactively. It's worth using the utility interactively once to become familiar with the required variables before using the tool straight at the command-line with switches. Before you begin the Storage VMotion you will need to know the path to the VMX file. This is not specified as you would at the Service Console (for example: /vmfs/volumes/virtualmachines/vm1/vm1.vmx) but in a syntax you see only in VirtualCenter which looks like this:

[virtual machines] vm1/vm1.vmx

You will find this syntax when if choose to Edit Settings of a VM, and select the Options Tab under "General Options". Figure C.70 shows the information required

**Figure C.70**




**Storage VMotion - Interactively**

**Warning:**

svmotion.pl like other command-line tools is case-sensitive. This includes passwords; datacenter names; the path to the VMX file; destination datastore

1. Open a CMD prompt on the system you have installed the Remote CLI

2. Type the command:

   **svmotion.pl –-interactive**

   **Note:**
   The CLI will then print the response

   Entering interactive mode.  All other options and environment variables will be ignored

3. Next provide the name or IP address of the VirtualCenter server

   Enter the VirtualCenter service burl you wish to connect to
   (e.g. https://myvc.mycorp.com/sdk, or just myvc.mycorp.com): virtualcenter.VI-3book.com

4. Next provide your username and password to connect to VirtualCenter

   Enter your username: administrator
   Enter your password: vmware

   **Note:**
   VMotion will then respond with the message:

   Attempting to connect to https://virtualcenter.VI-3book.com/sdk.
   Connected to server.

5. Next type the **name of the datacenter**

   Enter the name of the datacenter: London DataCenter

   **Note:**
   You do not need to provide speech marks represent spaces, but VMotion is case-sensitive hence the capital L and D and C in London DataCenter in my example

6. **Using the syntax found on the settings of the VM, provide the path to the VMX** file

   Enter the datastore path of the virtual machine (e.g. [datastore1] myvm/myvm.vmx):
   [esx1:storage1] vm1/vm1.vmx

7. **Supply the name of the destination datastore,** in my case the VMFS volume is labeled virtualmachines

   Enter the name of the destination datastore: virtualmachines

   **Note:**
   You do not have type in square [angle brackets]

8. If you wish to move the entire virtual machine to a different location, then choose No, to the question about moving just the virtual disk

   You can also move disks independently of the virtual machine.  If you want the disks to stay with the virtual machine, then skip this step..
   Would you like to individually place the disks (yes/no)? no

   After confirming this last question, you will then see progress bars, as the VM is moved from one VMFS volume to another

```
Performing Storage VMotion.
0%     |------------------------------------------------------------------------|
100%
       ##########################
```

**Storage VMotion – Non-Interactively**
It is possible to supply all this command-line information as single string. It's tricky to get every aspect of the syntax correct so be persistent. Below is example of a Storage VMotion with all the parameters provided. The example has been "wrapped" for readability

svmotion.pl –-server=virtualcenter.vi3book.com --username=administrator --password=vmware

--datacenter="London DataCenter"

--vm="[esx1storage1] vm1/vm1.vmx: virtualmachines"

**Warning:**
In the release candidate svmotion was is very particular about syntax. Firstly, notice the use of "double quotes" on the command-line. Secondly, notice that VMFS volumes "esx1storage1" does NOT have any colon : in the name. If you have a VMFS volume which includes a colon, then the storage VMotion command returns the error "Argument to --vm is not in the correct format".

Unlike the interactive method where you receive progress bars – at the command-line no progress is given. You will receive a "Relocate Virtual Machine Storage" message in the Vi Client.

**Storage VMotion – Moving Virtual Disks**
It is also possible to move individual virtual disks from one location to another. The syntax of this command is a little bit tricky as it is not the most obvious. The Storage VMotion command does need the location of the disk followed by the new location. You can see what I mean if I give you sample Storage VMotion command for moving a virtual disk. In this example I want to move a virtual disk from local storage (esx1storage1) to SAN based storage (sanlun2). The first part of the syntax is pretty straight forward, as they are merely the credentials to the VirtualCenter server

svmotion.pl --server=localhost --username=administrator --password=vmware --
datacenter="London DataCenter"

The next part of the syntax below indicates the current location of the VM's VMX file, followed by the destination I would like it to have. You see I can't move a virtual disk, without also moving the VMX file at the same time.

--vm="[sanlun1] vm1/vm1.vmx: sanlun2"

This line indicates I would like to leave the vm1.vmdk in its current location sanlun2, whereas the second part indicates the virtual disk called vm1.vmdk on esx1storage1 is to be moved to sanlun2

--disks="[sanlun1] vm1/vm1.vmdk:sanlun1, [esx1storage1] vm1/vm1.vmdk:sanlun2"

The net affect of this command is that first disk (vm1 on sanlun1) would stay in its current location and that the VM (and its smaller files) together with vm1.vmdk on esx1storage would be relocated on sanlun2. Notice the comma after --disks="[sanlun1] vm1/vm1.vmdk:sanlun1, this allows you to specify the location of multiple disks.

If I wanted to move the VMs smaller files back to sanlun1. The syntax would be as follows

svmotion.pl --server=localhost --username=administrator --password=vmware --

datacenter="London DataCenter"

--vm="[sanlun2] vm1/vm1.vmx: sanlun1"
--disks="[sanlun1] vm1/vm1.vmdk:sanlun1, [sanlun2] vm1/vm1.vmdk:sanlun2"

Here you can see this command is very similar to the previous command – in fact I merely used the cursor keys to retrieve the original command, and modified the critical elements, which I've highlighted in bold. So in the first line (beginning with –-vm) I'm requesting the VM's smaller files to be relocated back on sanlun1 (remembering the previous command relocated them to sanlun2). The second line (beginning with –-disks) shows I would now like to keep vm1.vmdk on sanlun2 on sanlun2. This is the same as line as vm1.vmdk on sanlun1. By setting the source and destination location to be the same we are affectively instructing the system not to move these files.

# *VMware Update Manager (VUM)*

Update Manager comes in two flavors – a stand-alone application that is used for stand-alone ESX hosts, and as plugin extension into VirtualCenter.

VMware Update Manager is brand new feature to VI-3, and its main job is patch ESX hosts and Virtual machines. In its VirtualCenter format, it allows you set a baseline level for patches, and to scan the VirtualCenter DataCenter or folder to see if VMs meet this corporate baseline. VMware Update manager can be set to manual or schedule scanning – and this can be achieved with the VM being online or offline. Additionally, the system can be configured to offer away of rolling back a VM should the patch process itself introduce more problems than it remedies using the VMware snapshot feature.

VMware Update Manager integrates with the DRS feature and can orchestrate the entire patch process. Working in conjunction with DRS, Update Manager will put the ESX host into maintenance mode triggering the evacuation of the VMs from the ESX host using DRS. Then Update Manager will then patch the ESX host, and force the ESX host to exit maintenance triggering DRS to re-balance the cluster.

Updates are managed in a three-stage process:

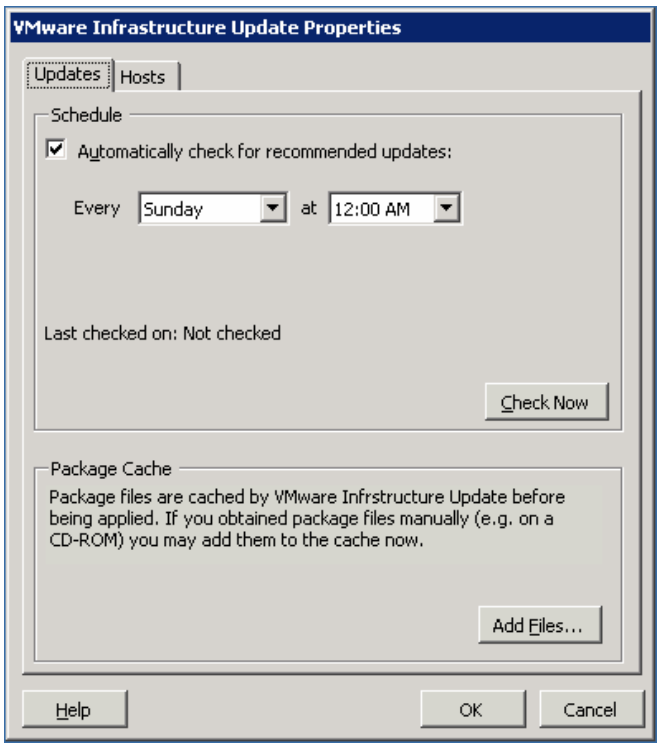
- Baseline – A list of patches that form a "company standard" for ESX hosts and VMs
- Scan - Checks against the baseline for compliance
- Remediation - Patch ESX host and VMs which fail to meet baseline

VMware will continue to support the older "esxupdate" command-line tool that has been used in the past script the installation of patches.

## Stand-Alone VMware Update with ESX 3i

1. Choose **Start, Programs**, **VMware** and Select **VMware Update Services**
2. The **Updates tab** enable "**Automatically check for recommended updates**" and set a schedule that you feel comfortable with
3. In the **Host tab** enable the option to "**Check all hosts**"
4. Return to the **Updates tab**, and to trigger a manual update click the "**Check Now**" button. Figure C.71 shows the Update dialog box

   **Figure C.71**




**Note:**
After a short while this should bring up the VMware Infrastructure Update dialog box. Click the **Install Updates** button. Figure C.72 shows the update dialog box; Figure C.73 shows the pretty download status bars and Figure C.74 shows the process in the VI Client

**Figure C.72**

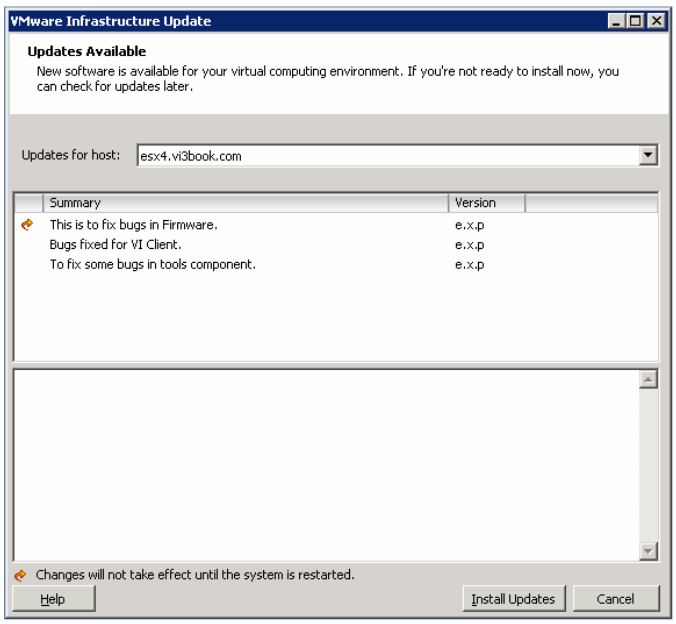



**Figure C.73**

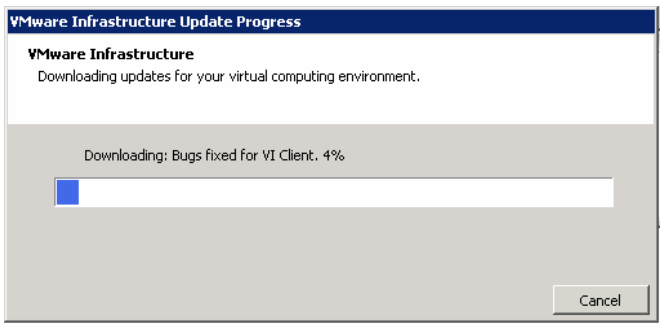
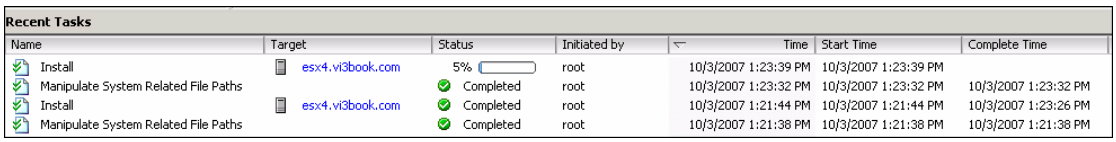



**Figure C.74**




5. At the end of the download process – you must authenticate to the ESX host. As you can see from figure C.74 if there is major change in the Firmware (ESX3i itself) then a reboot is required to allow the update take affect

## Configuring Microsoft SQL Server for Update Manager

As with VirtualCenter, VMware Update requires a database to track and trace your baselines, scans and remediation data. Additionally, before you begin the installation of Update Manager create a System DSN to communicate to this database. As our installation will be to Update Server which is separate from my VirtualCenter installation, its worth checking that the Update Server can communicate to VirtualCenter by IP address and/or hostname. During the installation VMware Update will want to communicate to VirtualCenter to complete the installation. Lastly, I would add a second disk to your Update Server purely for storing the updates themselves they can get large and could easily fill the Windows partition.

1. At the **SQL Server**
2. Open **Enterprise Admins**, and Expand **+ Microsoft SQL Servers, + SQL Server Group, + (Local) (Windows NT)**
3. **Right-click the Database folder**, and choose **New Database** and type: **vum-db** (or something similar/appropriate) – and choose **OK**
4. Expand the **+ Security** tab, and **right-click Logins**, and choose **New Login**
5. **Browse with … button** to select the account created for VirtualCenter database…
6. Choose the option **SQL Server Authentication** and type in the password for the VirtualCenter Database User
7. and set the **Default Database** to be the database created at point 2
8. Click the **Database Access** tab, **Permit** access for the database, for VirtualCenter Database User, also enable the permission **db_owner** – and choose **OK**
9. Click **OK**, and Confirm the password again

   **Note:**
   Repeat this process for the Update Manager Service database, perhaps calling vmware-updateDB. I used the same database user account for both databases

## Configuring Update Manager with Microsoft DSN

Previous VirtualCenter installations had a button in the installer to load the Data Sources (ODBC). This Microsoft Management tool is used to configure DSN settings to allow the VirtualCenter to "speak" the Microsoft SQL Database. Prior to starting the VMware Update installation these settings need to pre-configured.

1. At the **VMware Update Server**
2. Open **ODBC Data Source Administrator** from Administrative Tools on the Start, Programs menu
3. In the **ODBC Data Source Administrator** choose the **System DSN** tab
4. Click the **Add** button
5. From the end of the list choose **SQL Server**, and select **Finish**
6. In name field of the **Create a New Data Source to SQL Server** dialog box, type **VMware Update Manager**

   **Note:**
   The VMware Update Manager installation assumes this name

7. From the drop-down list **select your SQL server** and click **Next**
8. Select "**With SQL Authentication…**" and type in the user account and password for the database set up in SQL and click **Next**
9. Enable "**Change the default database to**" and select the VMware Update Database you created earlier
10. Click **Next** and **Finish**

    **Note:**
    You should be now able to confirm all the dialog boxes associated with the ODBC setup – and also test that you have connectivity to the database server. This test is nearly always successful. It does *not* test your user account credentials.

# VMware Update Manager Installation

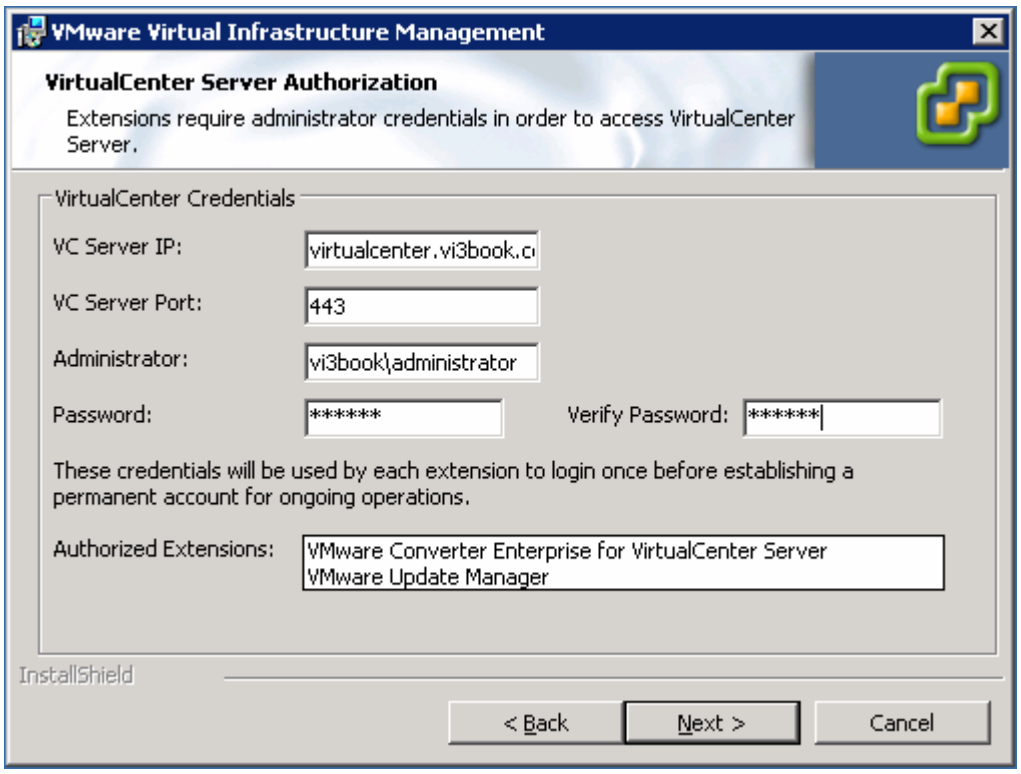
**Note:**
In this case we have assumed your VMware Update Manager is connected to the internet. If for security reasons it is not, it is possible to install the VMware Update Manager Download Service. This allows an internet connected service to download the updates, and relay the management information to the Update Manger. You will find the Update Manager Download service in the UMDS folder on the VirtualCenter CD. If your Update Manager has internet connectivity, VMware UMDS is not required.

1. Start the Autorun
2. **Next your way through the usual install suspects** – Welcome dialog box, EULA, Username and Organization

3. After wadding through these dialog boxes you will make your way to the **Installation Type dialog box**

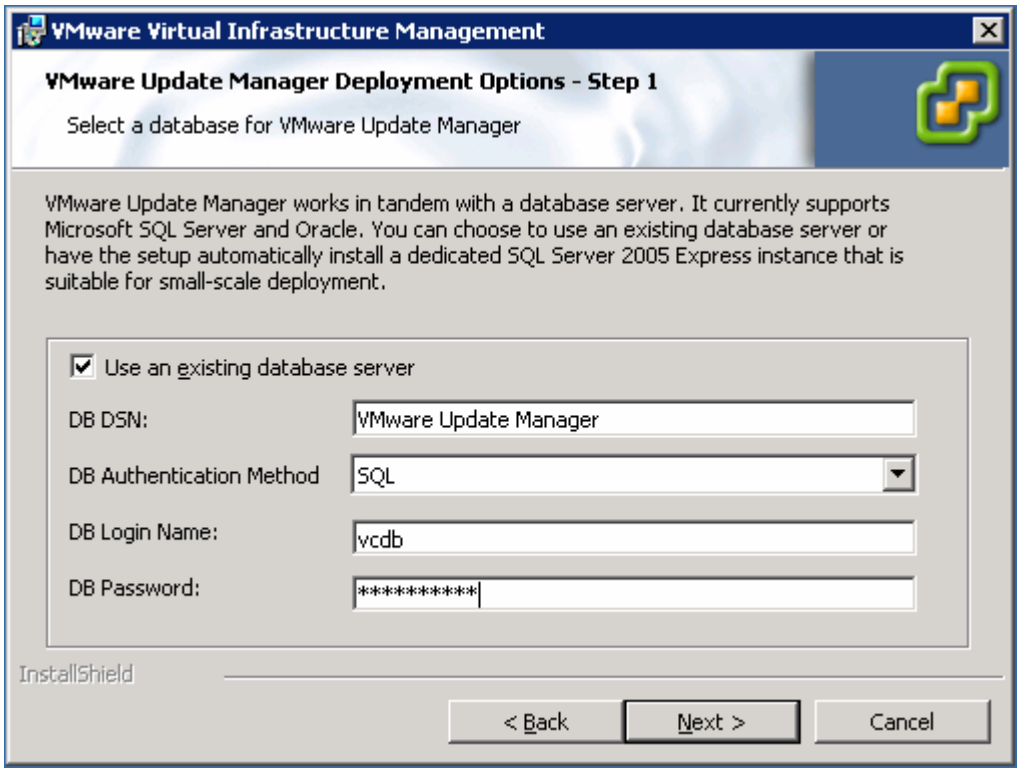
4. Choose **Custom**
5. Choose **VMWare Update Manager**
6. Complete the **VirtualCenter Server Authorization** dialog box. Figure C.75 show the dialog box in question. The "VC Server IP" field defaults to the VMware Update server's IP address and will need changing to either IP address or FQDN of the VirtualCenter Server

   **Figure C.75**



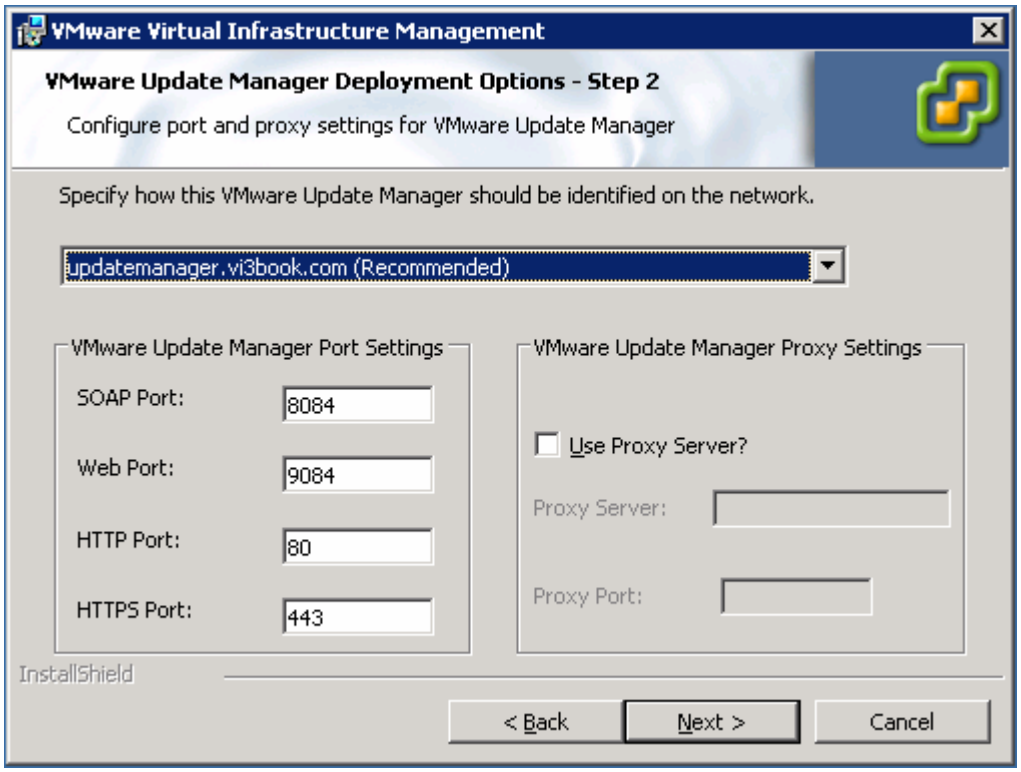

7. Next complete the **Update Deployment Options – Step 1 dialog box**. This allows you to set the database credentials for the VMware Update Database. Figure C.76 shows the dialog box in question, and I used the same credentials for VirtualCenter for my Update server

**Figure C.76**



8. Next **set the communication paths for VMware Update**. I accept the default for the VMware Update port numbers, in here you can also set your proxy server settings (if needed) to allow the VMware Update service to communicate to the internet for downloading patches.

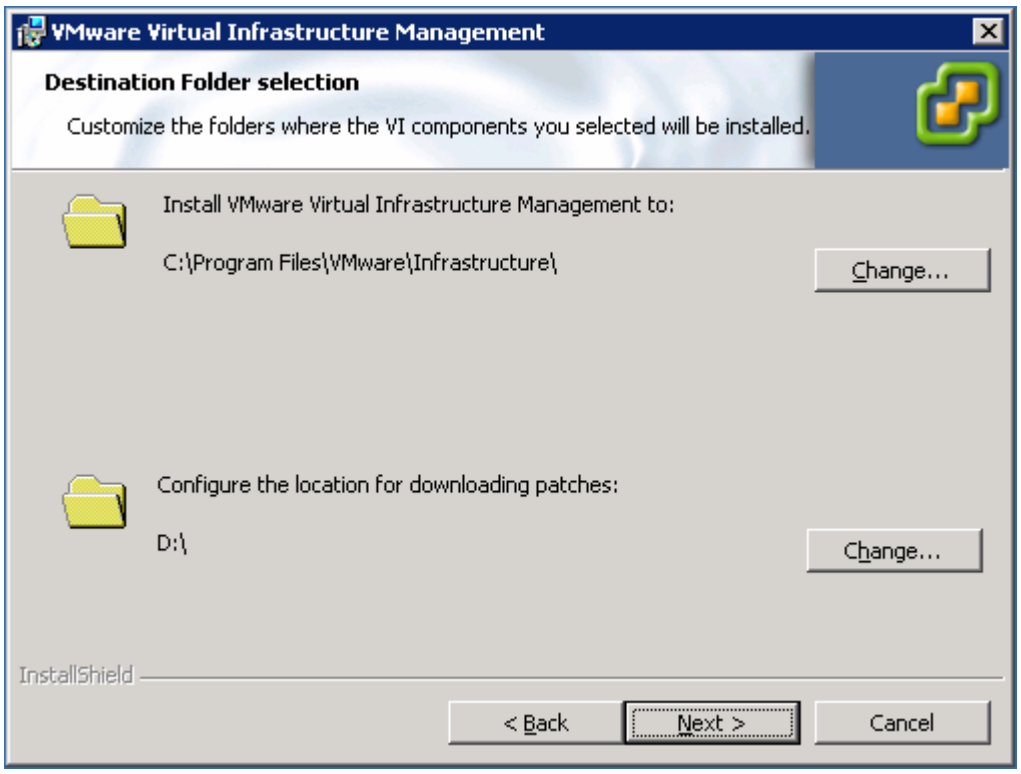
   **Figure C.77**




9. Finally, the last thing you are asked are the default locations for the VirtualCenter Installation, and where you would like to download the VMware Update files. **We feel that like Windows Update its perhaps best practice to dedicate a dedicated disk to this to avoid filling the root of C:**

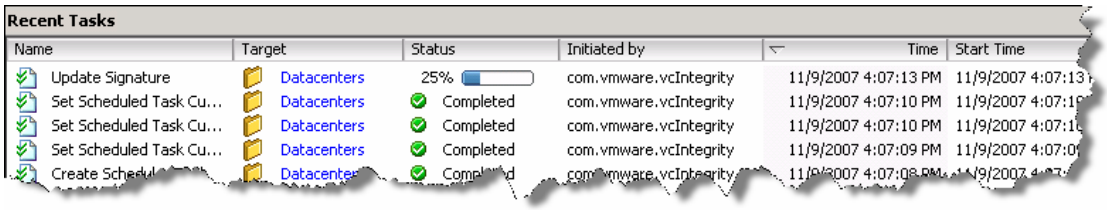
   Figure C.78 shows me changing the default drive for VMware Update Manager to D: for downloading patches. In fact as I run my VirtualCenter and Update Manager in a VM, I added a disk while the VM was running and used an RDM to store the patches.

   **Figure C.78**



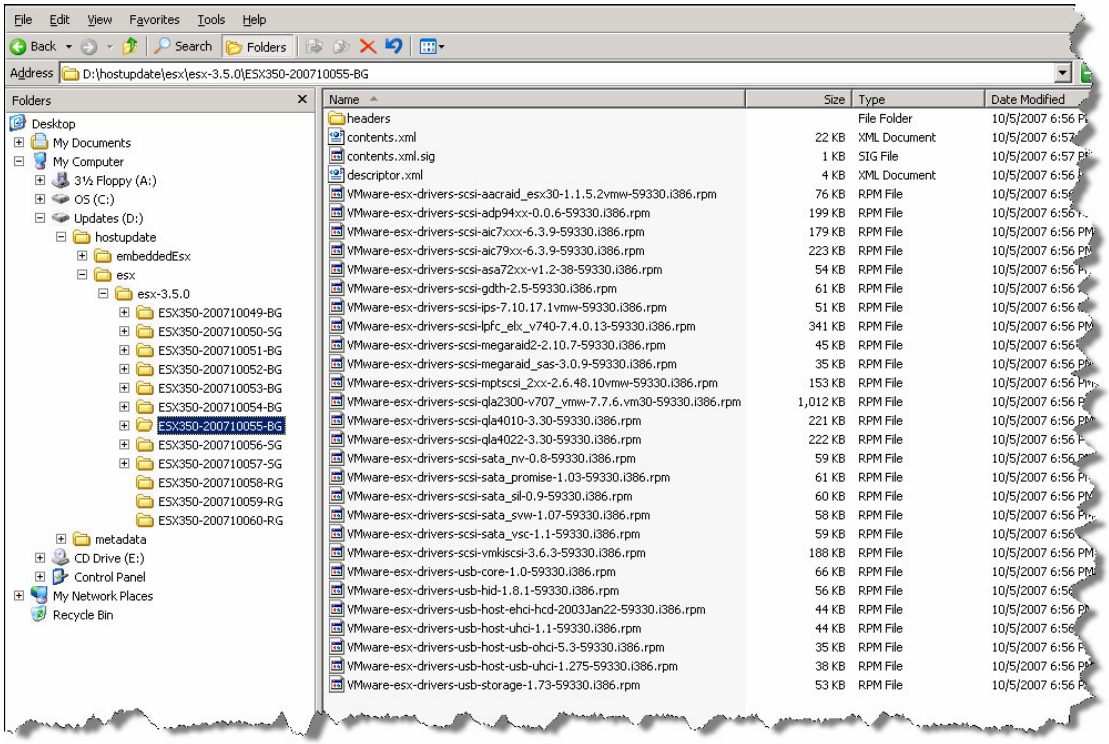

**Note:**
After the Update Manager has started you will see this progress bar in VirtualCenter change as it downloads new signatures from the internet. Figure C.79 shows the progress of downloading the signatures. VMware Update Manager checks both VMware and Shavlik to find and download updates. Shavlik monitors a range of different guest operating systems and the software they contain

**Figure C.79**




During this download process you will see this kind of directory structure (Figure C.80) being created on the VMware Update server. You can see that in the particular patch that has been downloaded for ESX there are a number of RPM (Redhat Package Management) files that will patch various drivers on the ESX host. VMware Update Manager by default download ESX host updates, but does not download Windows or Linux updates. Instead it download tools that allow it to compare the latest bullet-ins to your Windows and Linux guests. The download of Windows or Linux patches on begins at the "remediation" phase, and only the patches that apply are download. In other words, Update Manager does not download patches needless then, when they are not being installed to the guest operating system in question.

**Figure C.80**




Whilst your waiting for this process to complete we can press on with installing and enabling the VMware Update Client Plugin.

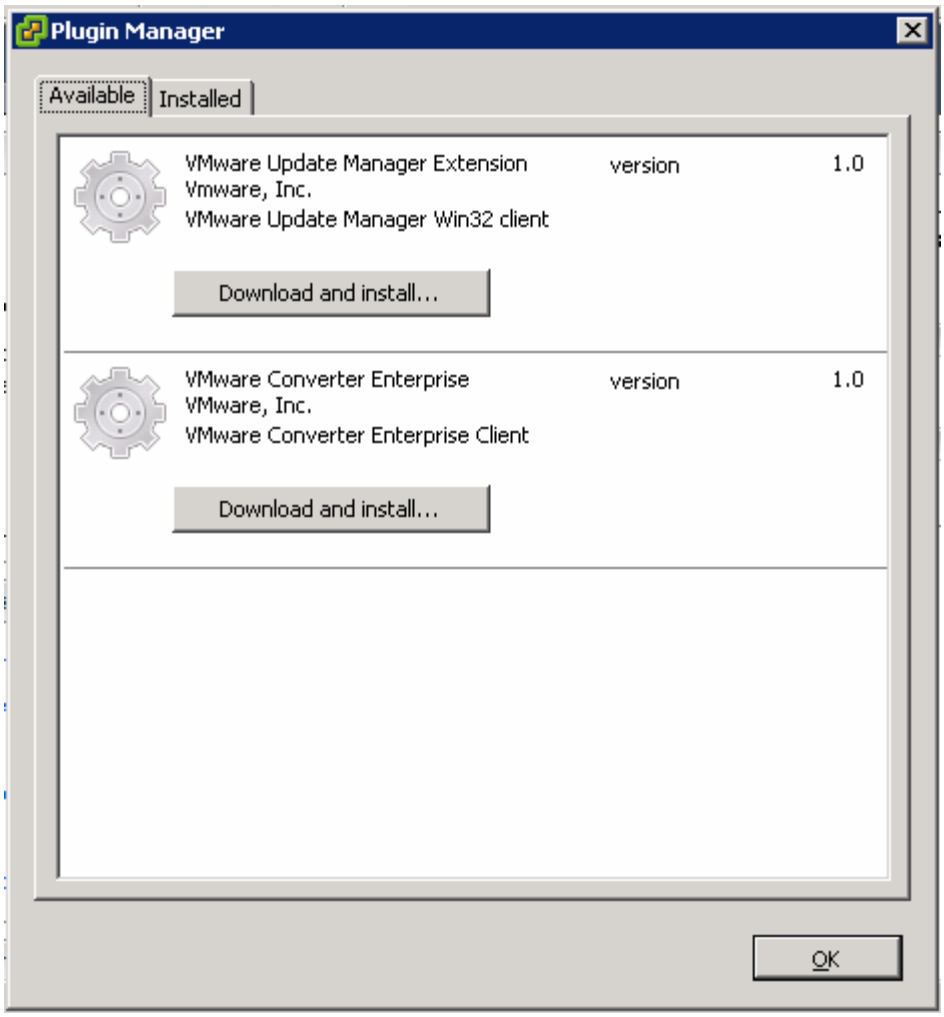
# VMware Update Client/Plugin Installation

**Warning:**

In the Beta/Release Candidate I found the "Plug-ins" section of the VI Client were blank. This problem was fixed by running repair on the installation using the Control Panel's "Add & Remove Programs". The main error you will see with plugins is if you incorrectly set either login details or the communication between VirtualCenter and system that allows plugins to be added. This error only happened when I was attempting to install VirtualCenter and Update Manager on the *same* instance of Windows. I did not have this problem when Update Manager was installed to a separate Windows instance after the VirtualCenter install has completed.

1. In the VI Client menu choose **Plugins** and **Manage Plugins**
2. In the **Plugin Manager** dialog box, click the **Download and Install** button for **VMware Update Manager Extension**

**Figure C.81**

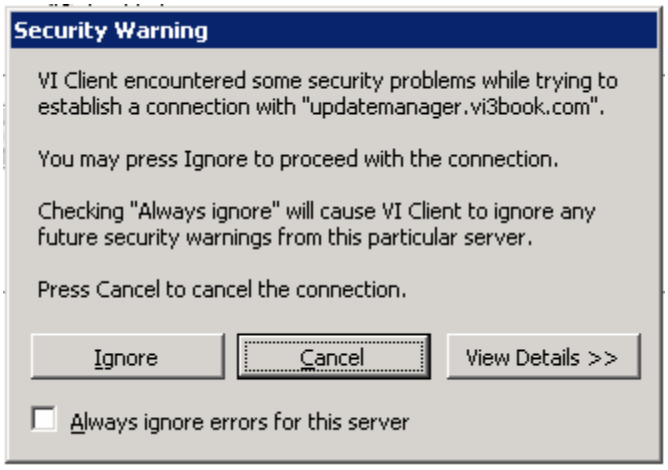



**Important:**
After running through the installation restart the VI Client. It can take sometime for a plugin to register itself on the installed tab.

3. In the VI Client menu choose **Plugins** and **Manage Plugins**
4. In the **Plugin Manager** dialog box, select the **Installed** tab
5. **Enable** the **VMware Update Manager Client**

**Note:**
When you enable the VMware Update Manager client – you will have to confirm another SSL certificate. This is the SSL certificate that proves the identity of the VMware Update Server. Additionally, you will receive a prompt from the VI Client about the untrusted nature of these certificates. As you can see in Figure C.82 this does validate the identity of the VMware Update server

**Figure C.82**




**Note:**
This should add a number of extensions to the VI Client it adds "Update Manager" button to the main toolbar (Figure C.83) and Scan/Remediate options in the right-click menus (Figure C.84)

**Figure C.83**

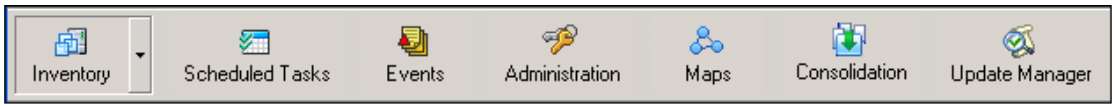
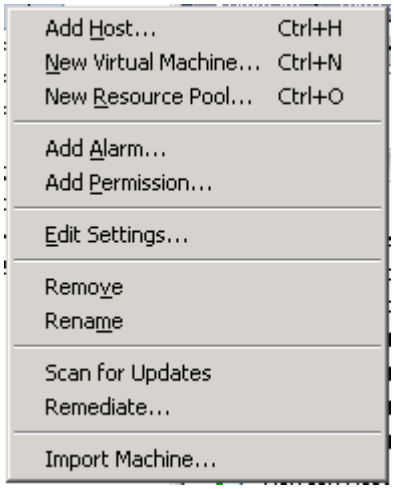


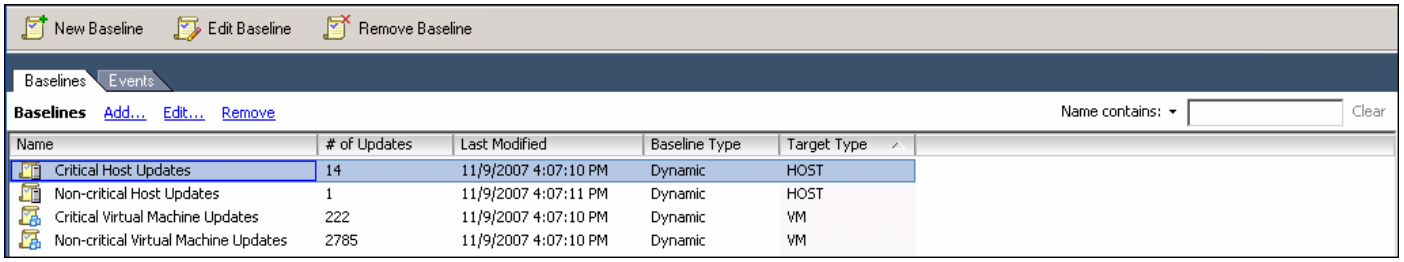

**Figure C.84**




## Understanding & Viewing Baselines

If you click the VMware Update Manager view button at the top of the VI Client you will see four default baselines create by the install procedure (Figure C.85)

**Figure C.85**




As you recall baselines are basically lists of possible vulnerabilities and are used in the scanning process to see if an ESX host or VM meets your baseline. We can many different baselines, and attach those baselines to any number of datacenters, clusters, ESX hosts, Virtual Machines or a folder of VMs. So might decide that baseline X is applied to folder A, but baseline Y is applied to folder B. ESX host or VMs that fail these baselines can be fixed in a process that VMware calls "remediation".

There are two types of baseline for either ESX hosts or for VMs. So you could decide to only use VMware Update to maintain the ESX software, and use other existing patch management systems to maintain your guest operating systems.

Baselines are further sub-divided into either critical or non-critical updates. VMware uses a categorization system and Shavlik's to determine if an update is critical or non-critical. The baseline then builds a list of updates to add or not add to a baseline.  In figure C.86 we can see that there 14 Critical Updates for ESX hosts, but only 1 non-critical update.

Additionally, baselines can either be dynamic or fixed. Dynamic baselines are automatically maintained by the update system and they are updated as new vulnerabilities appear. The automatically create in the baseline exclusions and inclusions of the patch based on the categories of non-critical and critical. It is possible to permanent exclude items manually from the dynamic baseline. Additionally, with fixed baselines which are manually specified by the administrator you can create any combination of non-critical or critical patches suited to your organizations policy.

That seems all very simple. However, first glace the dialog boxes for baselines might not seem very intuitive, but with a little explanation to do make perfect logical sense. Figure C.86, C.87 and C.88 show the configuration dialog boxes of the "Critical ESX Hosts Updates" baseline

**Figure C.86**

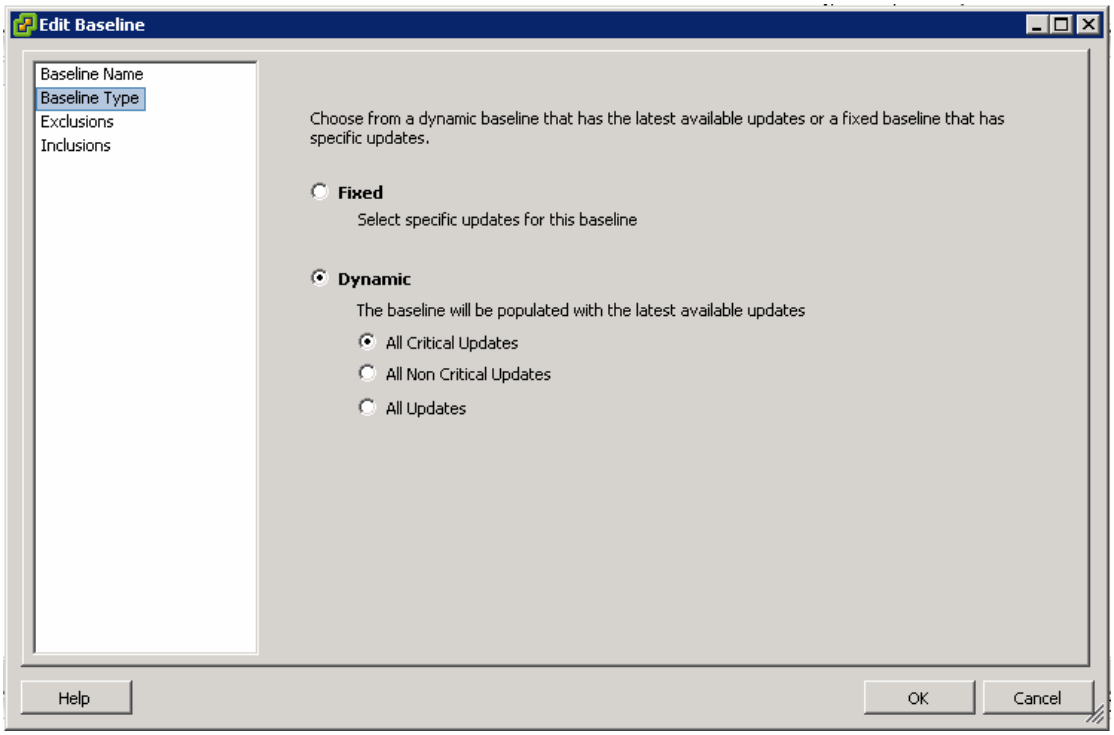



Figure C.86 shows that the baseline is dynamic and configured to only look for All Critical Updates.

**Figure C.87**

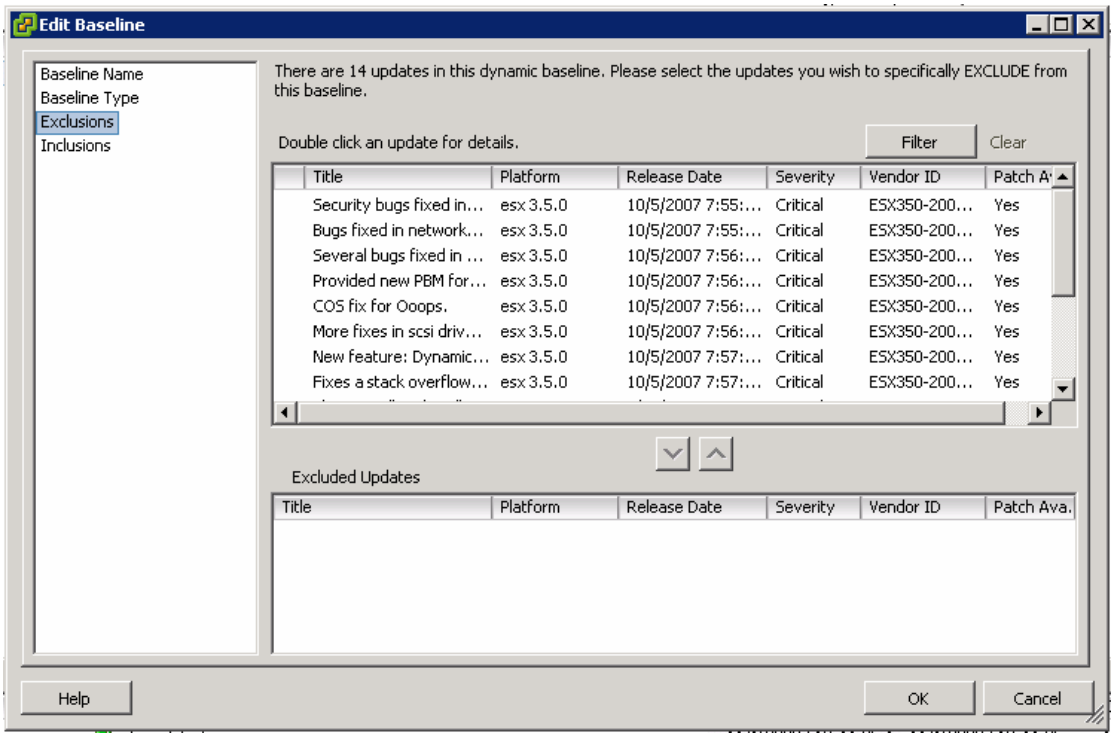



Figure C.87 shows that there are 14 updates that can be applied, and that some of them could possibly be excluded. Notice how they are all categorized as being "Critical". Ironically, this despite list being labelled "exclusions" these vulnerabilities would be used in a scan! The upper part of this dialog is list of patches that would be applied, the lower part allows you as the administrator to override this and specifically exclude a critical patch.

**Figure C.88**

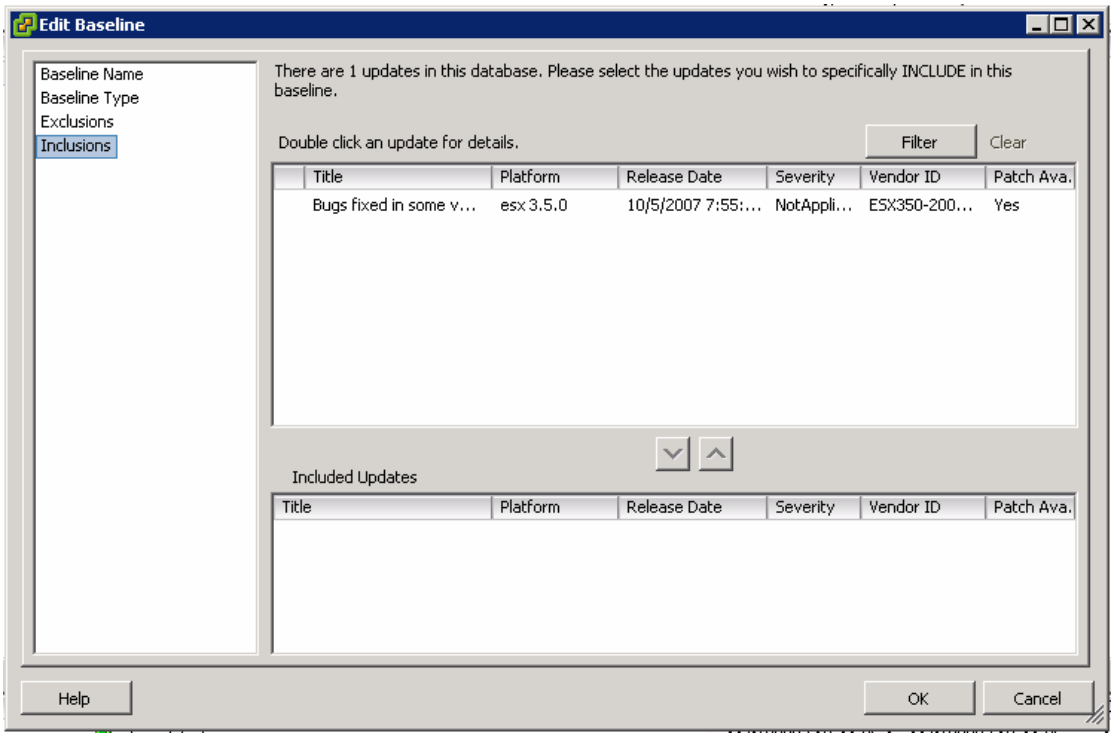



Figure C.88 shows just one update has severity level of "Not Applicable". As such it does not become added to the baseline, because it is not critical. Ironically, this list labelled "inclusions" this vulnerability would NOT be used in a scan. Unless you use the up and down arrows in the dialog box to over-ride the baseline to include non-critical updates. This would be a little bit illogical. What would be the point of a baseline called "Critical Updates" that included a non-critical updates?

**IMPORTANT:**
The way to understand these interfaces – is to see the exclusion list as way of excluding critical vulnerabilities you do NOT wish to check your ESX or VM against. For example I could decide out of the list of 14 critical vulnerabilities that the update that fixes problems with SUSE guest operating system drivers does not affect me because I do not run SUSE as my Linux distribution. Using the "exclusion" dialog box I could double click at the vulnerability (Figure C.89) to find more information about it, and use the down arrow to add it to the exclusion list (Figure C.90)

**Figure C.89**

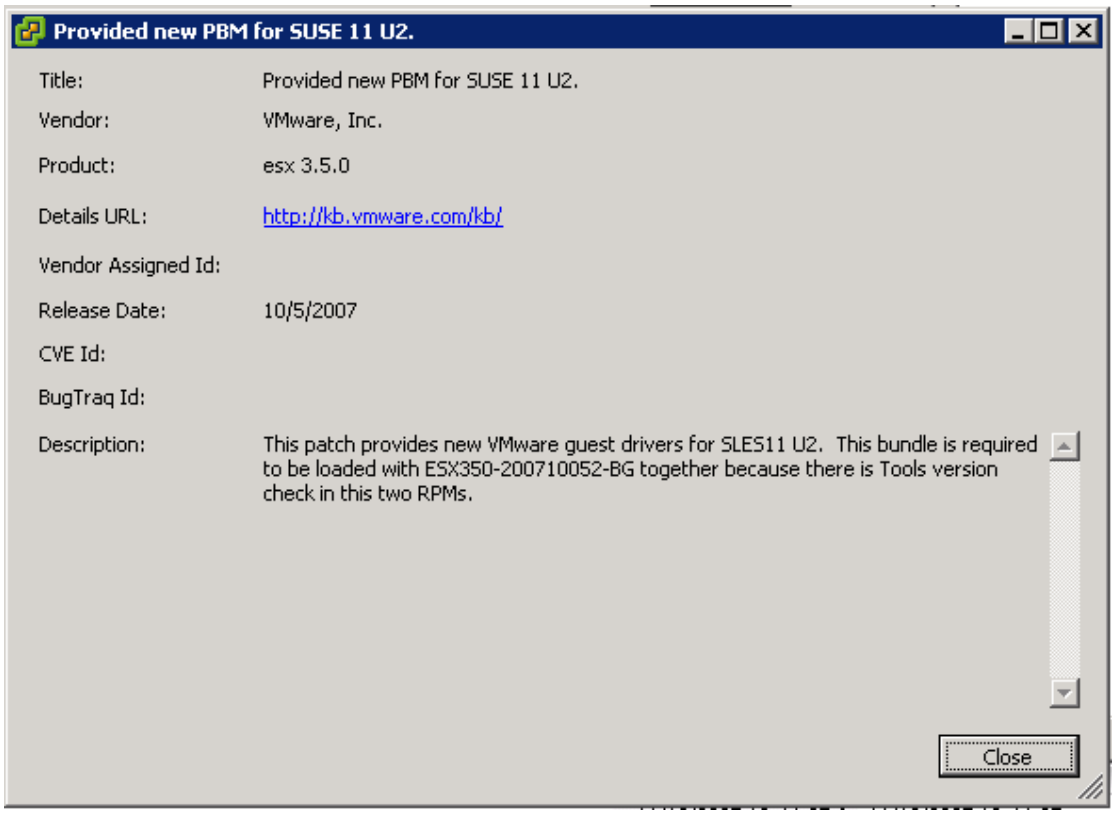
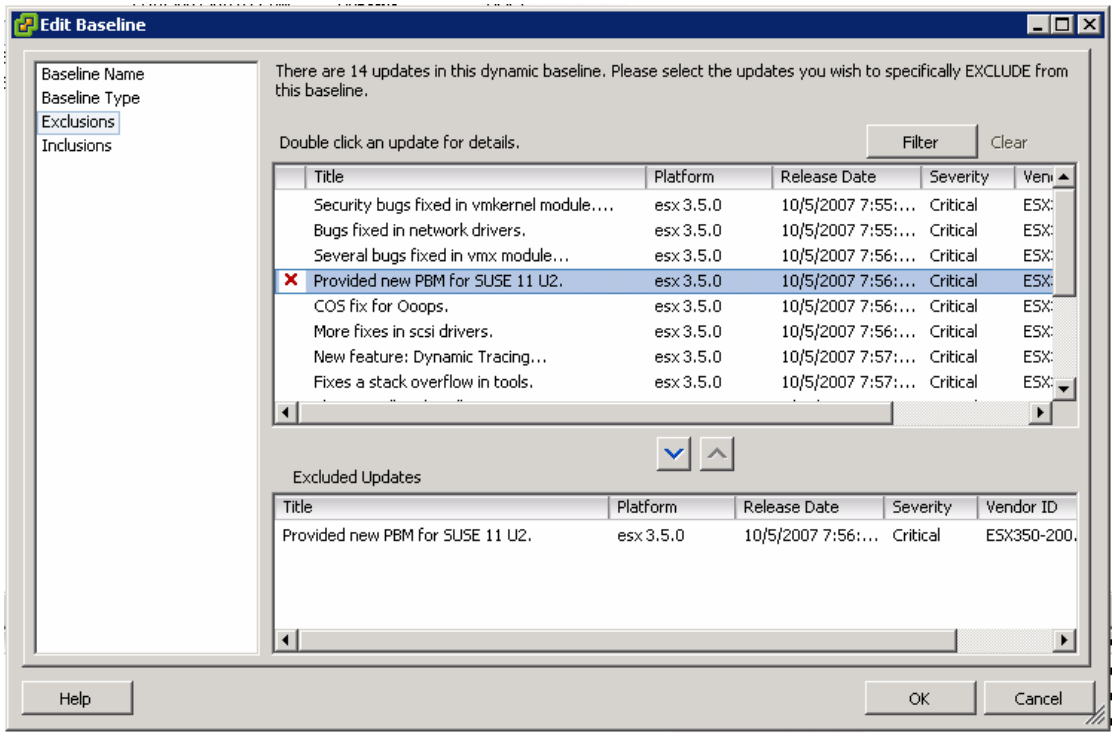
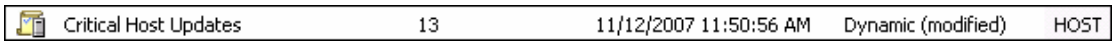



**Figure C.90**




As I make changes to the default dynamic baselines, the Update Manager will update its information to show my changes. Figure C.91 shows that I now only have 13 updates instead of my original 14, and that it has been modified.

**Figure C.91**



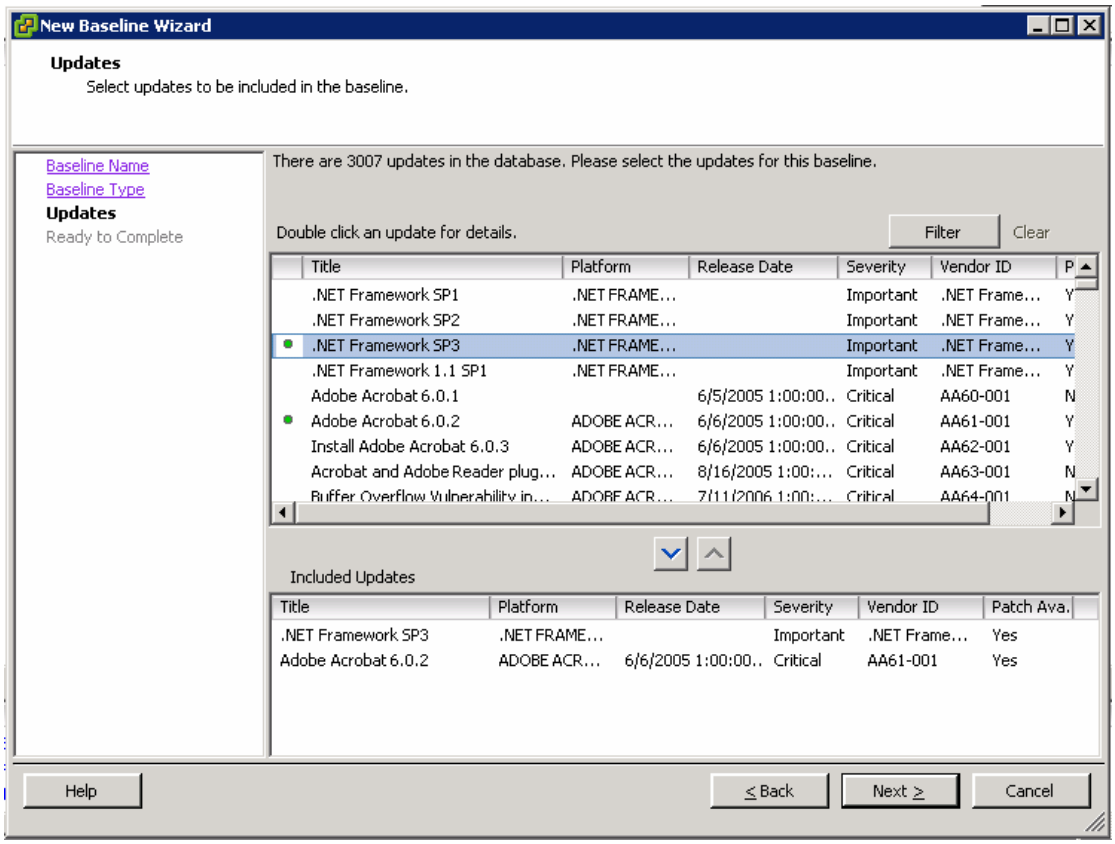

**Note**:
The number of updates does not categorically tell you how long the scan or remediation process would take. After all you have lots of vulnerabilities that can be patched with 1K file, and a couple of vulnerabilities that 100MB in size. This said, as general rule of thumb the more patches the long the scan/remediation process with take. As you might expect scanning hundreds of VMs with thousands of updates, takes considerably long than scanning a much small number of ESX hosts with just couple of vulnerabilities. As ever the severest vulnerabilities generally really lies within the scope of the guest operating system, not with VMware ESX server. You can substantial reduce the patch management of ESX by adopting ESX 3i, as most of the vulnerabilities in ESX 3.5 affect the "Service Console" piece of the platform.

## Creating Fixed Baselines

It is possible to create your own baselines (fixed or dynamic) which conform to your own internal standards. The information below is here just to guide you through the process. There is no need or requirement for you own fixed baselines to make Update Manager work except if the default baselines do not fit to the requirements within your organization.

1. In the **Update Manager** window
2. Click the **New Baseline** button
3. **Type in a friendly name for the baseline** such as: **Corp Standard – Virtual Machine Critical Updates**
4. **Select a baseline target** such as **Virtual Machines/Guest OS Updates** and Click **Next**
5. Choose the **Fixed** baseline option
6. **Select the updates you wish to include**, with the **downward arrow button**. Figure C.92 shows me including just two updates/fixes

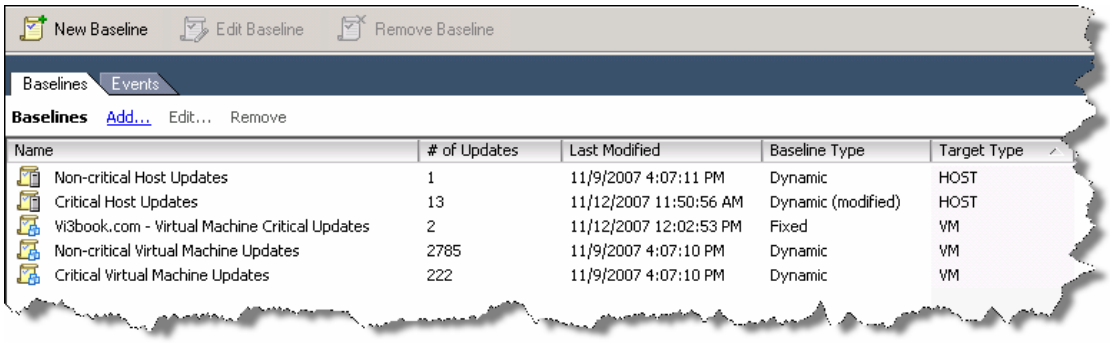
   **Figure C.92**




7. Click **Next** and **Finish**

   **Note:**
   Again the main VMware Update manager window would refresh showing a mix of the default dynamic baselines and the manual fixed baseline created in the above procedure.

   **Figure C.93**




## Attaching Baselines & Scanning for Updates

Using these baselines we can now scan the inventory to produce a report on whether our ESX hosts or VMs meet our baseline. We can trigger a scan in nearly all the major nodes within VirtualCenter including:

- In the **Virtual Machine & Templates** View
  - On the Virtual Machine & Templates container itself – therefore scanning every VM and Template
  - Folders containing VMs

- Single VMs
- Templates

- In the **Hosts & Clusters** View

  - On the Host & Cluster container itself – therefore scanning every datacenter, cluster and ESX host
  - DataCenters
  - Clusters
  - Hosts

**Note:**
We cannot currently attach a baseline to the resource pool object. Additionally, if you wish to attach a baseline to a VM or a folder of VMs, you must switch to the Virtual Machine & Templates View.

**Scanning All the ESX hosts in a DataCenter:**

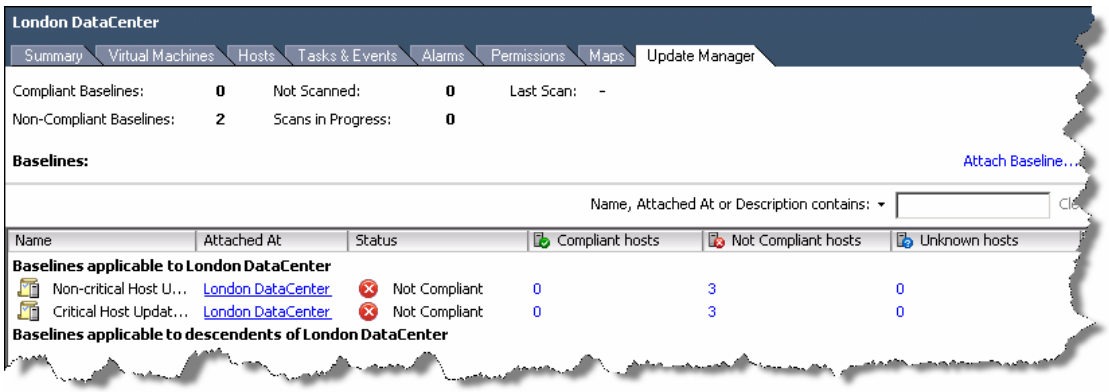
1. In the **Hosts & Clusters** View
2. Select a **DataCenter**
3. Select the **Update Manager** tab
4. Click the **Attach Baseline…** link
5. **Select the Baselines you wish to scan** with and click **OK**

   **Note:**
   Notice how VM baselines are hidden in this dialog box

6. Click the **Scan** button on the toolbar, or right-click the datacenter and chose Scan for Updates.
7. Choose **Yes** to the dialog box, to scan all the ESX hosts

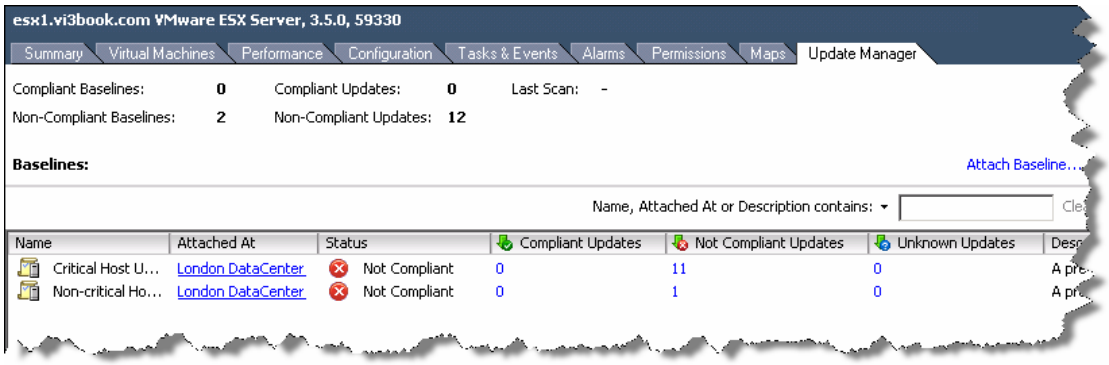
   **Note:**
   After the scanning process completes a report is generated at the point it was triggered – in my case the DataCenter view. Figure C.94 shows that none of my ESX host meet the baseline currently because they are clean installations of ESX 3.5 that have never been patched or updated. As such they a flagged up with red X marks indicating that they do not meet my requirements (my baseline) for ESX.

   **Figure C.94**




If I select an ESX host and look at its update manger tab, it will give me a report. For example Figure C.95 shows the report the ESX host called esx1.VI-3book.com

**Figure C.95**




**Scanning all the VMs in a datacenter:**

1. In the **Virtual Machine & Templates** view
2. Select a **DataCenter**
3. Select the **Update Manager** tab
4. Click the **Attach Baseline...** link
5. **Select the Baselines you wish to scan with** and click **OK**

   **Note:**
   Notice how ESX host baselines are hidden in this dialog box

6. **Right-click the DataCenter** and choose **Scan for Updates**
7. Choose **Yes**, to scan all the VMs in the datacenter

   **Note:**
   After the scanning process completes a report is generated at the point it was triggered – in my case the DataCenter view. Figure C.96 shows that none of my VMs meet the baseline currently because they are clean installations of either Windows 2003 (SP1) or Windows 2000 Advanced (SP4) that have never been patched or updated. As such they a flagged up with red X marks indicating that they do not meet my requirements (my baseline) for VMs.

   As with ESX host scanning, you receive similar compliant and non-compliant reports

**Warning:**
Occasionally, you might see in the Update Manager report window the word "unknown" and count of "unknowns". These are known unknowns, which are unknown because no scan has yet to take place, once these unknowns are known, they then known to the system – and these unknowns are removed. How's that for Donald Rumsfield speak?

# Remediation of ESX host & VMs

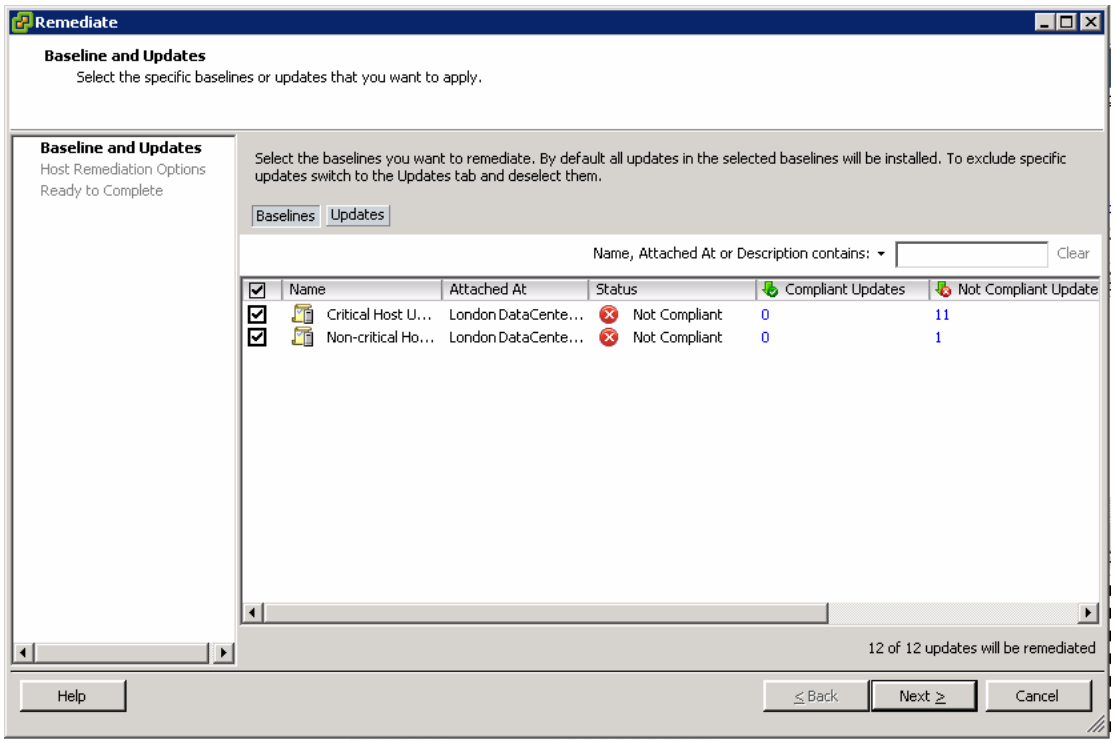
The term remediation is a rather fancy term for applying a patch, as with scanning remediation can be done at same levels of the VirtualCenter inventory. One especially neat feature is the way VMware Updates is integrated with DRS, as it can orchestrate the VMotion of VMs off an ESX host that is about to be patched, trigger enter/exit of maintenance mode. There is also the option to configure what happens if maintenance mode cannot be achieved. For example of such VMs are those running Microsoft Clustering Service which need to be configured with local VMFS storage in order to meet VMware support requirements. As a consequence they cannot be moved by DRS as they break one of the main requirements of VMotion – shared storage.

**Remediation of an ESX Host:**

1. **Select an ESX host** and click the **Update Manager** tab

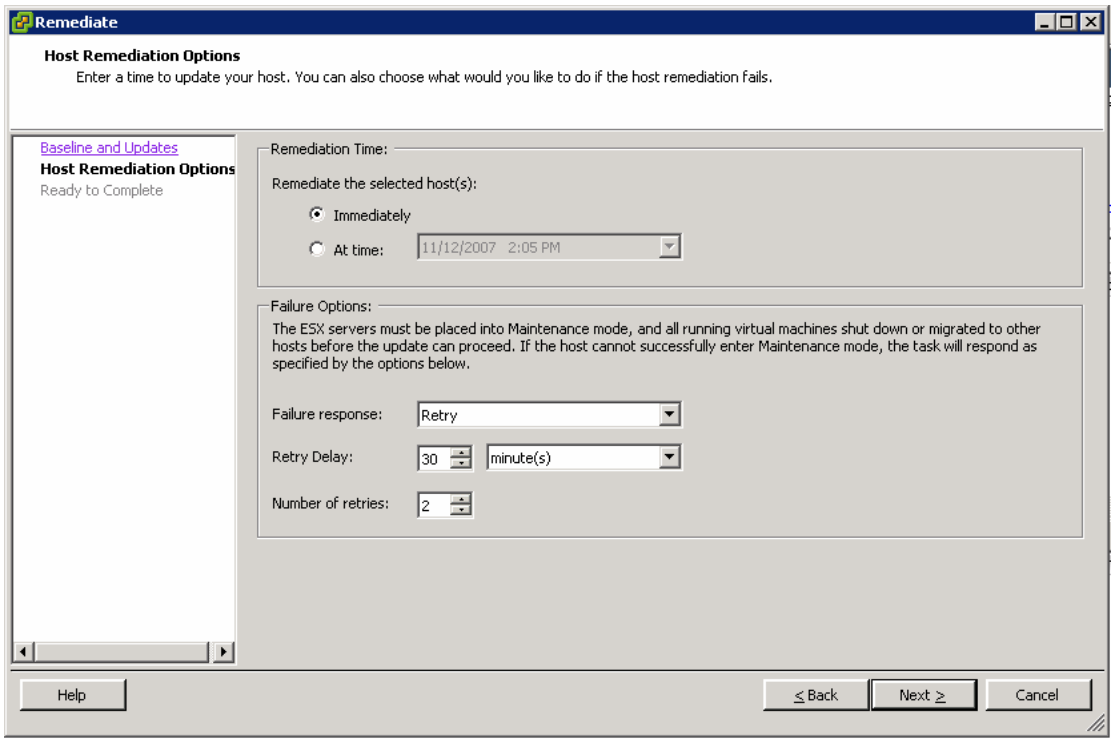
2. Click the **Remediate** Button, or right-click the ESX host and choose Remediate
3. **Select the baselines which will form the basis of your remediation**. Figure C.96 shows the dialog box, until you have selected some kind of baseline, you will not be able to select the update tab to see the updates that will be applied

**Figure C.96**



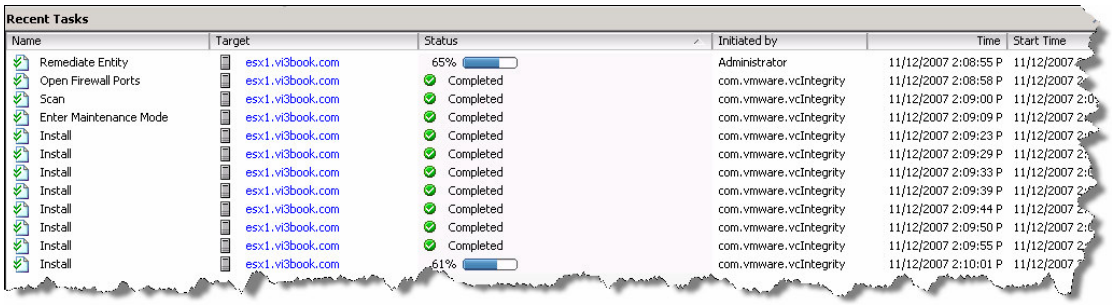

4. The next dialog box (Figure C.97) allows you configure when the remediation will happen, and also what to do if maintenance mode cannot be achieved

**Figure C.97**




**Note:**
If you have selected immediately, the process will begin right away, and the "recent tasks" view will give you progress information as shown in Figure C.98

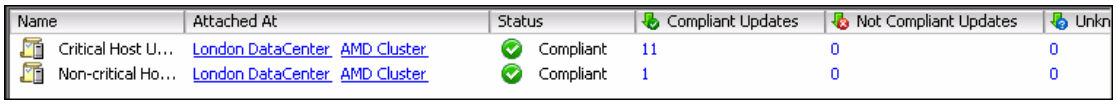
**Figure C.98**




**Note:**
The "Remediate Entity" give you an entire view of the process with each of the "Install" entries being a patch that has been applied. The "Remediate Entity" will also include the time taken to reboot an ESX host, and for maintenance mode to be exited. You should expect your ESX host to be flagged as "Not Responding" at some stage during the remediation process.

After the remediation process is over there is no need to manually re-scan an ESX host to confirm that it now meets the baseline – this task is automated. The update manager tab for a patch ESX host should change its status from non-compliant to compliant as shown in Figure C.99.

**Figure C.99**




Additionally, in the datacenter or cluster views you would see the column listing the number of compliant and non-compliant hosts update as well.

**Note:**
If you trigger remediation at high-level than an ESX host (Hosts & Clusters, DataCenter or Clustering) the Update Manager manage will patch each ESX host serial this is to ensure as many ESX host are online as possible during the remediation process.

**Remediation of a Virtual Machine(s):**
**Warning:**
The remediation of VMs automatically creates a snapshot. Beware of patching large numbers of VMs simultaneously that have not been patch managed previously. You may run out of disk space for the delta files that make up a snapshot.

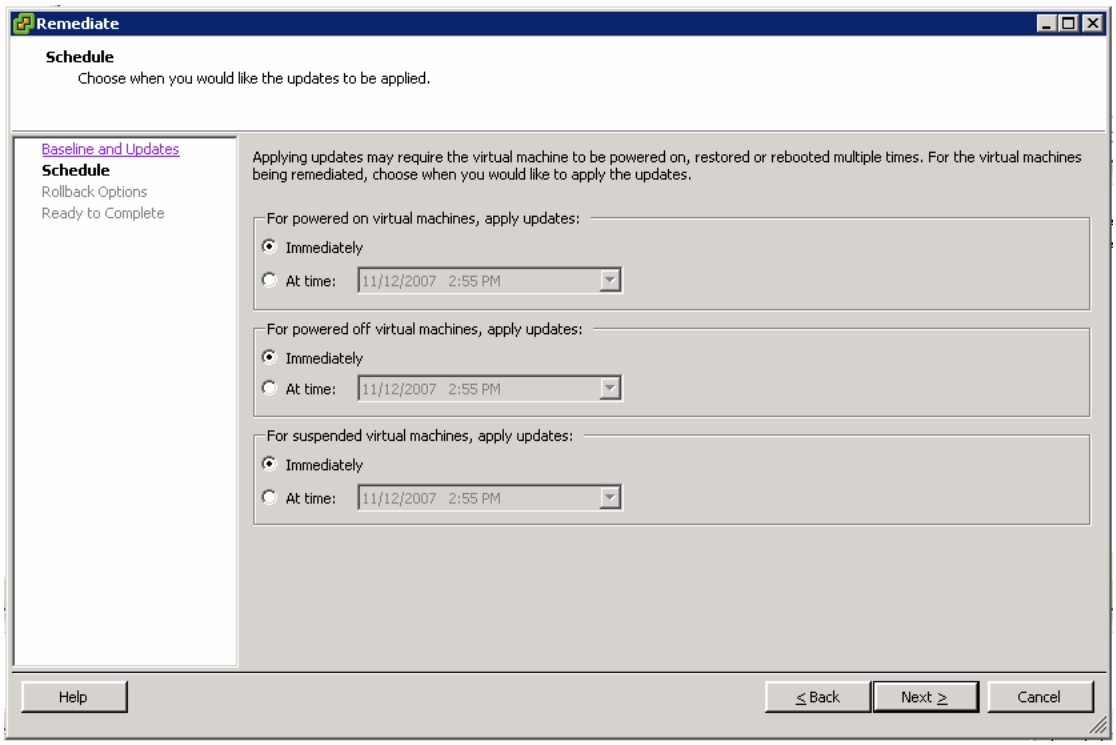
Remediation of a VM works in a very similar way except you have the chance to control when powered on, powered off and suspended VMs are patched. With suspended VMs, Update Manager powers those VMs back on, patches them and then re-suspends them.

During the patching process VMware will apply and retain a snapshot of the VM to allow the rollback of VM prior to the patching process in case a patch causes more problems than it fixes. We have a number of options to manage the snapshots such as:

- Applying a standard name and description for the snapshot which is applied to every VM affected.
- Not deleting the snapshot – and managing its removal manually
- Retaining the snapshot for a number of specified hours
- Taking a snapshot of memory

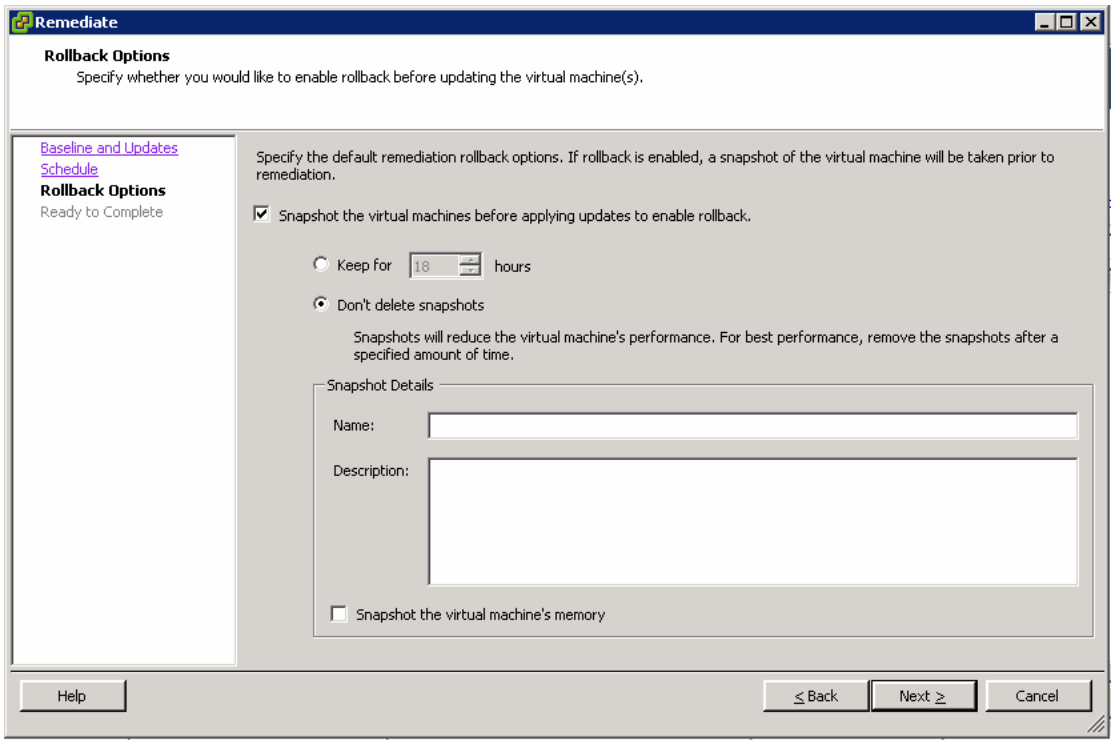
1. Select a VM or folder of VMs and click the Update Manager tab
2. Click the **Remediate** Button, or right-click the VM/Folder and choose Remediate
3. **Select the baselines which will form the basis of your remediation**
4. **Set your preferences** for the **Schedule** (Figure C.100)

**Figure C.100**



5. **Set your preferences** for **Snapshots (Figure C.101)**

**Figure C.101**




**Note:**
During this process the VMware Update Manager Guest Agent is installed for the first time to the VM.

I found monitoring the progress of a large VM remediation tricky. Unlike the installation of ESX patches, where each update has event entry of "install", no such progress information of that detail exists for VM patches. So unless you have VMs which are read patched up to hilt already expect the "Remediate Entity" status bar to be on screen for sometime. In my case with just Windows 2003 (SP1) and Windows 2000 Advanced Server (SP4). It took a long time to download all the patches and then apply them.

## Configuring VMware Update Service Settings

Some of these settings that control the remediation defaults can be modified from the VMware Update menu (Plugins, Update Manager, Settings). If you wish to modify the behaviour for failed maintenance and VM Snapshots you can change them under the menu of Plugins, Update Manager and Settings.

As you might have saw in the ESX remedial dialog boxes you have 4 options on what to do if maintenance mode is unsuccessful they include:

- Retry N times in N minutes
- Fail Task
- Power off VMs and Retry
- Suspend VMs and Retry

## Update Manager Intervals & Scheduling Scans

VMware Update manager also extends the functionality of the Schedule Tasks. There is a default schedule task which is used to control how frequently Update Manager checks for new updates. There is two way to control this scheduled task, either from the Schedule Task interface, or from

the menu under plugins, Update Manager, Schedule Update Download. The Update Schedule by default checks for updates for ESX hosts, Windows and Linux VMs. This is triggered every week on Saturday and 9.01am. This is started relative to your time zone. Additionally, you can request the schedule task to send an email if you so wish. If you wish the email feature to work remember to set your SMTP settings in Administration, VirtualCenter Management Service Configuration.

In addition to the built-in scheduled tasks to download updates. There is the option to create scheduled tasks to both scan and remediate both ESX hosts and VMs. The interface is very easy to use, and anyone familiar with a typical task scheduler should be easily able to automate this types events. I don't intend to cover them here.

It is perhaps worth at this point listing the new tasks that can be scheduled – as VI-3.5 extends about the default 8 to a list of 12 tasks. The new tasks include:

- Scan for Updates
- Remediate
- Export a virtual machine
- Import a virtual machine

# *Guided Consolidation*

Guided Consolidation is not really new product as such; however the close integration of parts of VMware's Capacity Planner and Converter into VirtualCenter is certainly new. Essentially, "Guide Consolidation" combines a much slimmed down version of VMware's Capacity Planning tool with VMware Converter. The Guided Consolidation is not intended to replace VMware Capacity Planner.

The Guide Consolidation wizards lead you through the process of analyzing existing physical hosts to assess the virtual hardware required to make them run efficiently. Currently, the Guide Consolidation only allows the conversion of Windows physical machines, and is dependant on browsing feature to locate them on the network. This can be somewhat slow, and there is currently is no method to manually add a physical machine by NETBIOS name or IP address with the Guide Consolidation wizards. However, it is still possible to trigger the use of VMware Convert from the right-click menus of VirtualCenter, thus missing out the "discovery and analysis" phase of Guide Consolidation. Additionally, in the Beta/Release Candidate there is no interface to select on which datastore your imported machine will be copied to. In my tests I found the system preferred to use shared storage VMFS volume over my local VMFS volume which had more free space in them. For these reason you might still prefer to use the VMware Converter tool without the Guided Consolidation Wizard.

## Enabling the VMware Converter Plug-in

1. In the VI Client menu choose **Plugins** and **Manage Plugins**
2. In the **Plugin Manager** dialog box, click the **Download and Install** button for **VMware Converter Enterprise**

   **Important:**
   After running through the installation restart the VI Client

3. In the VI Client menu choose **Plugins** and **Manage Plugins**
4. In the **Plugin Manager** dialog box, select the Installed tab
5. **Enable** the **VMware Converter Enterprise Client**

   **Note:**
   From this point onwards you have two options. You can use the VMware Converter tool manually, by right-clicking an ESX host or cluster and choose the Import Machine option. This brings up the standard API's for using VMware Converter.

Alternatively, you can use the Guide Consolidation Wizard

## Configuring Analysis and Conversion Authentication

In order for guided consolidation to work the correct user account(s) and user rights must be first configured. The account must have the following the privileges to work successful:

- A member of the local administrators group on VirtualCenter
- Rights to "Logon as Service" to the VirtualCenter's the local security policy
- A domain account with read rights to the domain
- Administrative rights over the physical machines to gather performance data (this user can be different from the accounts)

In the simplest configuration you can create one user account that carries out all of these tasks – however, you will probably face security restrictions that prevent this. Security and correct authentication is probably the biggest issue in using the guide consolidation feature. VirtualCenter does not se these additional privileges for you and it is worth ensuring them before using guided consolidation

## Performing an Analysis and Conversion

1. Click the large "**Consolidation**" button at the top of the VI Client
2. Click the **Start Analysis** button
3. Click **Next**
4. Configure Service and Default Credentials in dialog boxes. Figures C.68b and C.68c show the dialog boxes

**Figure C.102**

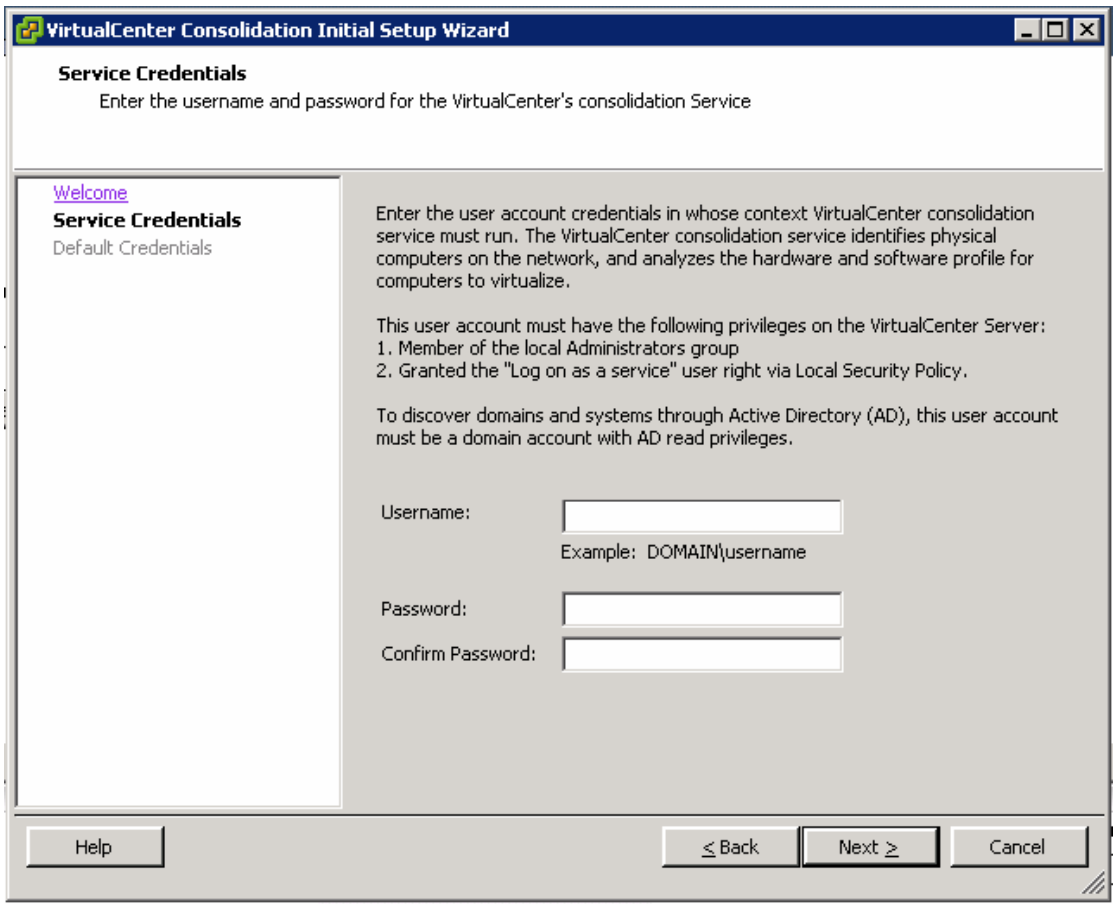
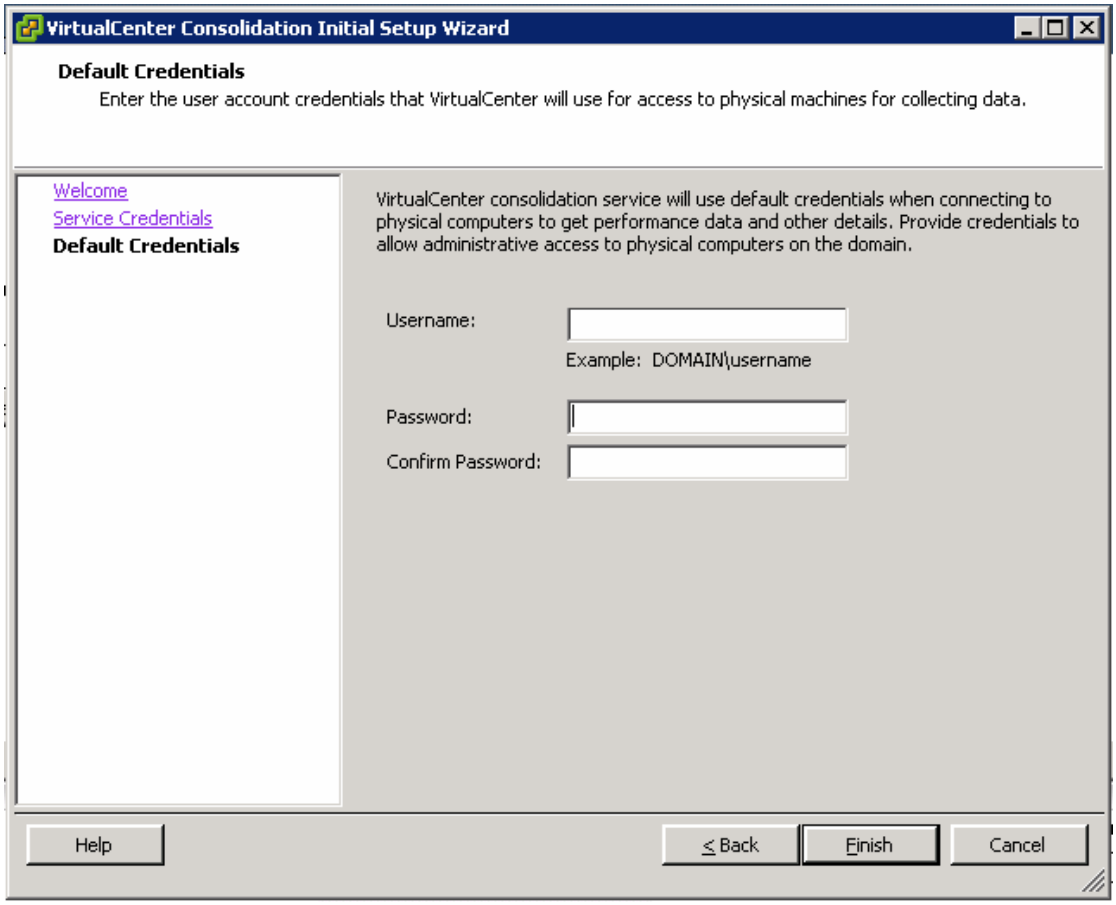


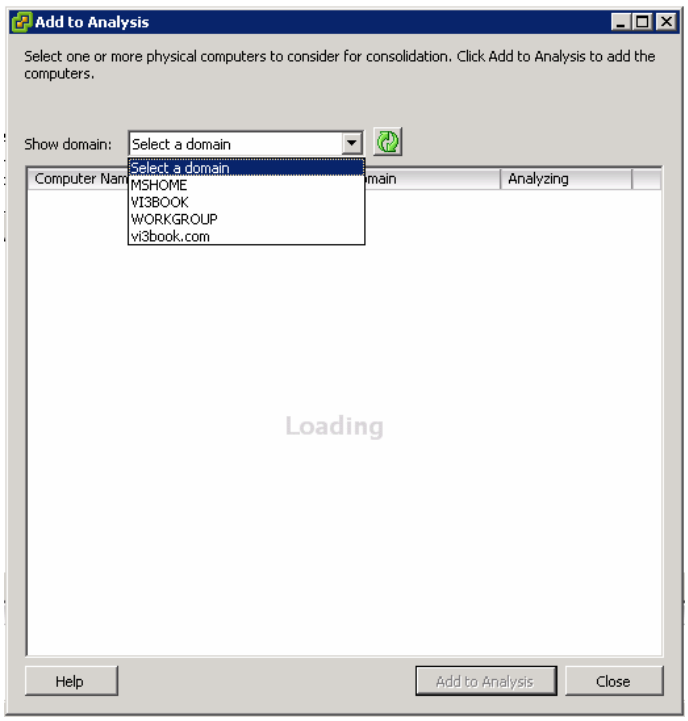
**Figure C.103**




**Note:**
Credentials must be supplied using the older domain\username format rather than the UPN (VI-3book.com@username) format. If you need to adjust or change these default credentials they can be modified under the administration menu

5. In the **dialog box** (Figure C.104) **select the domain or workgroup you wish to locate physical machines**

**Figure C.104**

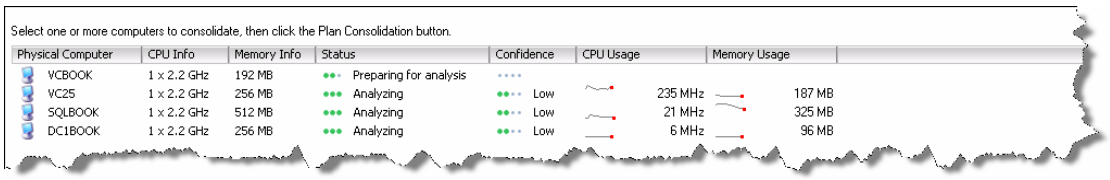



6. **Select the physical machine** you wish to analyze, and click the **Add to Analysis** button
7. In the **Set Authentication** dialog box**,** select **Use the Configured default credentials**

**Note:**
Figure C.105 shows the analysis window. The physical machines should appear in the analysis tab and will go through three main stages

Collecting System Information…
Preparing for analysis…
Analyzing…

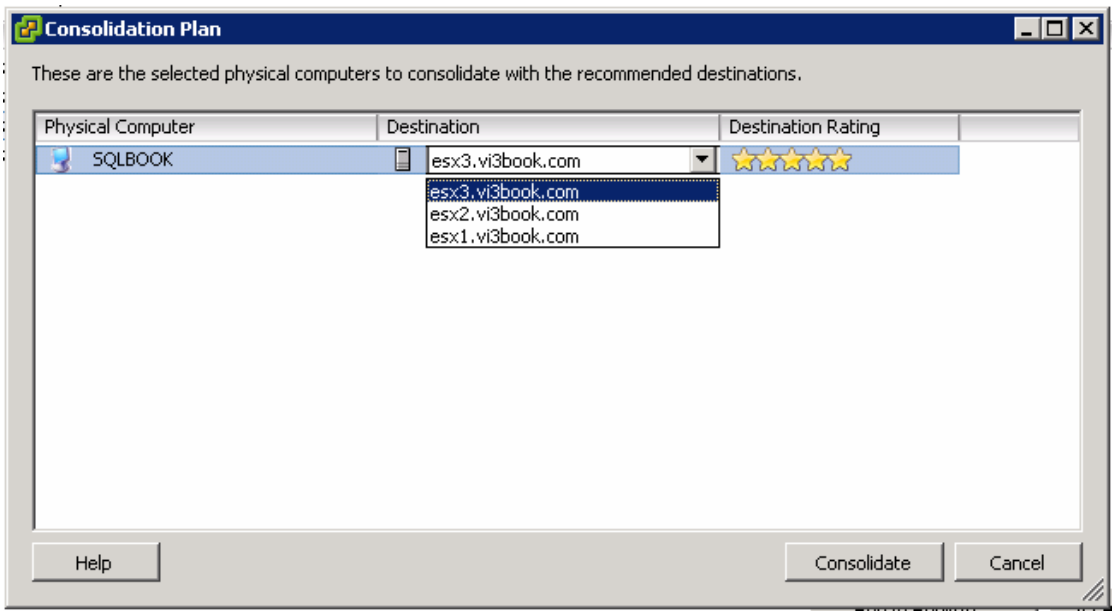
**Figure C.105**




**Note**:
To trigger the conversion process you select a physical machine (multiple selection is supported), and click the Plan Consolidation button. You will not able to convert a physical machine until has reached the "Analyzing" stage

8. **Select the physical machine(s)** and click **Plan Consolidation button**. This should generate the consolidation plan dialog box with recommendation for the destination physical host with star rating for the destination. Figure C.106 shows the recommendation dialog box and the fact you can override the recommendations suggested

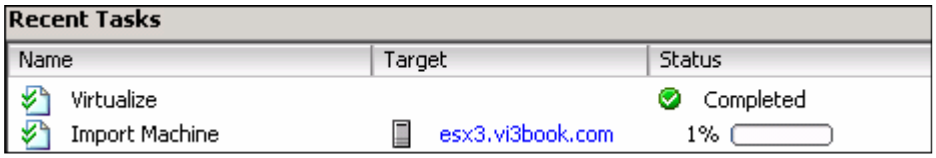
**Figure C.106**




9. Select the **physical machine(s)** and click the **Consolidate button**

   **Note:**
   This should trigger the virtualization and importing process

   **Figure C.107**




# *Importing & Exporting Virtual Machines*

## Importing a Virtual Machine

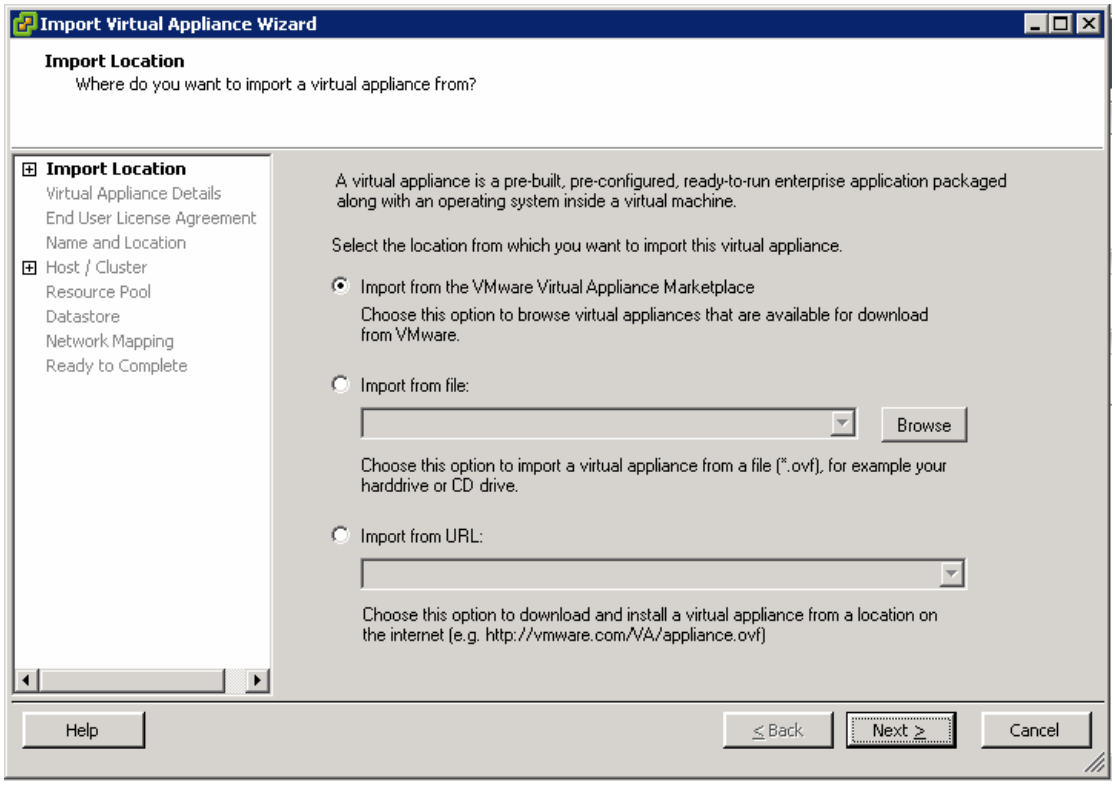
As shown in Appendix B on ESX 3i there is a new "import" feature that allows you to bring in VMs from external sources. These include the

- VMware Virtual Appliance Market Place
- From a hard drive or DVD a VM in the Open Virtual Machine Format (.ovf)
- From a URL the .OVF format

One sample Virtual Appliance runs old DOS style games, and I've selected it because the time it takes download is very small. This said the welcome message for Virtual Appliance can and do change.

1. In the menu choose
2. **File, Virtual Appliance** and **Import**
3. Choose **Import** from the **VMware Virtual Appliance Market Place**

   **Figure C.108**

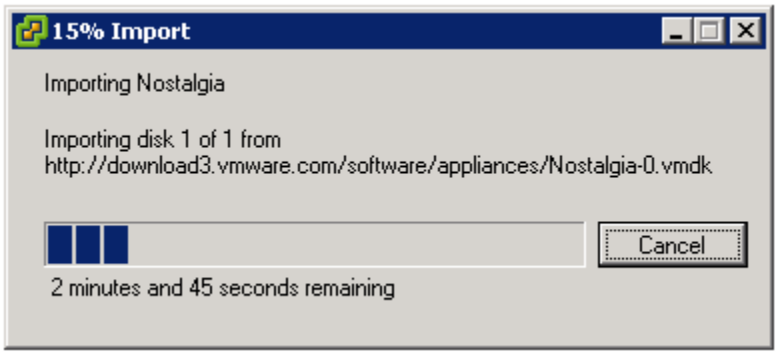



4. Select from the list

   **Nostalgia – 6.3MB**
   Ancient DOS Games, ready to play!

   **Note:**
   The remainder of the Import Wizard asks you to select a virtual machine, name, VirtualCenter location, ESX Host/Cluster and DataStore location. Figure C.109 shows you download progress bar

   **Figure C.109**




   **Note:**
   VMware Tools has not been installed to nostalgia, and please do not contact us for instructions on the keystrokes or the best strategy to win with the flight simulator game FII7!

## Exporting a Virtual Machine

It is also possible to power off one of your VMs in the VirtualCenter Inventory and exports them to an external source. This can be to the local disk of the VirtualCenter server or network

resource. The file is export in the 2gbsparse format (which means just the data is exported, not the free space in the disk) together with an .ovf file. Therefore they can be used to re-import a VM from one VirtualCenter to another or the original VirtualCenter.

1. **Select the VM** you wish to Export
2. Choose in the menu, **File, Virtual Appliance and Export**
3. Use the **Browse button** to select your destination

   **Note:**
   Similar dialog boxes are generated during the export process. The ovf file is an XML file which contain descriptor fields similar to the VMs VMX file. Below is a sample ovf file

```
      <?xml version="1.0" encoding="utf-8"?>
<ovf:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:ovf="http://www.vmware.com/schema/ovf/1/envelope"
xmlns:vssd="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/CIM_VirtualSystemSettingData"
xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/CIM_ResourceAllocationSettingData" ovf:version="0.9">
    <References>
        <File ovf:id="file1" ovf:href="vm1-disk1.vmdk" ovf:size="404860928" />
    </References>
    <Section xsi:type="ovf:DiskSection_Type">
        <Info>Describes the set of virtual disks</Info>
        <Disk ovf:diskId="vmdisk1" ovf:fileRef="file1" ovf:capacity="2147483648"
ovf:format="http://www.vmware.com/specifications/vmdk.html#sparse"
ovf:populatedSize="930742272" />
    </Section>
    <Section xsi:type="ovf:NetworkSection_Type">
        <Info>List of logical networks used in the package</Info>
        <Network ovf:name="Production">
            <Description>The "Production" network</Description>
        </Network>
    </Section>
    <Content xsi:type="ovf:VirtualSystem_Type" ovf:id="vm1">
        <Info>The virtual machince "vm1"</Info>
        <Section xsi:type="ovf:OperatingSystemSection_Type" ovf:id="79">
            <Info>Guest Operating System</Info>
            <Description>Microsoft Windows Server 2003, Enterprise Edition (32-
bit)</Description>
        </Section>
        <Section xsi:type="ovf:VirtualHardwareSection_Type" ovf:required="true">
            <Info>276 MB , 1 CPU, 1 disk, 1 nic</Info>
            <System>
                <vssd:InstanceId>0</vssd:InstanceId>
                <vssd:VirtualSystemIdentifier>system
id</vssd:VirtualSystemIdentifier>
                <vssd:VirtualSystemType>vmx-04</vssd:VirtualSystemType>
            </System>
            <Item>
                <rasd:Caption>1 virtual CPU</rasd:Caption>
                <rasd:Description>Number of Virtual CPUs</rasd:Description>
                <rasd:InstanceId>1</rasd:InstanceId>
                <rasd:ResourceType>3</rasd:ResourceType>
                <rasd:VirtualQuantity>1</rasd:VirtualQuantity>
            </Item>
            <Item>
                <rasd:Caption>276MB of memory</rasd:Caption>
                <rasd:Description>Memory Size</rasd:Description>
                <rasd:InstanceId>2</rasd:InstanceId>
```

```
                <rasd:ResourceType>4</rasd:ResourceType>
                <rasd:AllocationUnits>MegaBytes</rasd:AllocationUnits>
                <rasd:VirtualQuantity>276</rasd:VirtualQuantity>
            </Item>
            <Item ovf:required="false">
                <rasd:Caption>Floppy Drive 1</rasd:Caption>
                <rasd:Description>Floppy Drive</rasd:Description>
                <rasd:InstanceId>3</rasd:InstanceId>
                <rasd:ResourceType>14</rasd:ResourceType>
                <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
                <rasd:AddressOnParent>0</rasd:AddressOnParent>
            </Item>
            <Item ovf:required="false">
                <rasd:Caption>CD/DVD Drive 1</rasd:Caption>
                <rasd:InstanceId>4</rasd:InstanceId>
                <rasd:ResourceType>15</rasd:ResourceType>
                <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
                <rasd:Parent>7</rasd:Parent>
                <rasd:AddressOnParent>0</rasd:AddressOnParent>
            </Item>
            <Item>
                <rasd:Caption>Network Adapter 1</rasd:Caption>
                <rasd:Description>PCNet32 ethernet adapter on
"Production"</rasd:Description>
                <rasd:InstanceId>5</rasd:InstanceId>
                <rasd:ResourceType>10</rasd:ResourceType>
                <rasd:ResourceSubType>PCNet32</rasd:ResourceSubType>
                <rasd:AutomaticAllocation>false</rasd:AutomaticAllocation>
                <rasd:Connection>Production</rasd:Connection>
                <rasd:AddressOnParent>7</rasd:AddressOnParent>
            </Item>
            <Item>
                <rasd:Caption>Hard Disk 1</rasd:Caption>
                <rasd:Description />
                <rasd:InstanceId>6</rasd:InstanceId>
                <rasd:ResourceType>17</rasd:ResourceType>
                <rasd:HostResource>/disk/vmdisk1</rasd:HostResource>
                <rasd:Parent>8</rasd:Parent>
                <rasd:AddressOnParent>0</rasd:AddressOnParent>
            </Item>
            <Item>
                <rasd:Caption>IDE 0</rasd:Caption>
                <rasd:Description>IDE Controller</rasd:Description>
                <rasd:InstanceId>7</rasd:InstanceId>
                <rasd:ResourceType>5</rasd:ResourceType>
                <rasd:BusNumber>0</rasd:BusNumber>
            </Item>
            <Item>
                <rasd:Caption>SCSI Controller 0</rasd:Caption>
                <rasd:Description>LsiLogic SCSI Controller</rasd:Description>
                <rasd:InstanceId>8</rasd:InstanceId>
                <rasd:ResourceType>6</rasd:ResourceType>
                <rasd:ResourceSubType>lsilogic</rasd:ResourceSubType>
                <rasd:BusNumber>0</rasd:BusNumber>
            </Item>
        </Section>
    </Content>
</ovf:Envelope>
```

# *Conclusions*

As you can see VMware have once again added new functionality to both ESX and VirtualCenter at no additional “upgrade” cost. Additionally, there has been some significant finessing of existing features which make the administration of VI-3.5 easier. The core product remains the same despite the introduction of DPM, VUM and Guided Consolidation. So anyone reading the VI-3book will still find lots of useful and relevant material between its covers. The authors of the VI-3book will continue to maintain and updates its content as the VMware Infrastructure 3 evolves. These updates will supplied as free PDF files which can be downloaded from VI-3book.com. However, it seems like the next big release for VMware will be VMware Infrastructure 4.

See you there!