# VMware vSphere™ 4 Competitive Reviewer's Guide

WHITE PAPER

vmware®

## Table of Contents

# Getting Started

## About This Guide

The purpose of this guide is to support a self-guided, hands-on evaluation of VMware vSphere™ 4 by press reviewers, technology analysts, and IT professionals who wish to compare vSphere to competing virtualization products such as Microsoft Hyper-V and Citrix XenServer. This guide can also be used by reviewers without hands-on access to a live vSphere installation. You will find the key VMware competitive advantages called out in the "VMware Differentiators" section associated with each key feature.

## Intended Audience

This guide is intended to cover competitive evaluation cases that are suitable for reviewers and IT professionals who:

- Want a guided description of the key features in vSphere
- Want a detailed explanation of the differentiation provided by vSphere features compared to competing virtualization products
- Want scenario-based examples of the business and operational advantages vSphere features provide over Microsoft Hyper-V and Citrix XenServer

Readers are encouraged to follow the Document Structure section to select the self-contained sections that are appropriate for their evaluation requirements.

## Accessing the vSphere Reviewer's Hands-on Lab

If you are a qualified press or analyst reviewer, VMware can provide you with remote access to a fully operational VMware vSphere 4 installation and a companion Lab Guide. The Reviewer's Hands-On Lab allows live access to a vSphere enviroment where you can familiarize yourself with vSphere and try all its key new features. The companion "VMware vSphere Competitive Reviewer's Hands-On Lab Guide" provides step-by-step instructions for every feature.

To arrange access to the Reviewer's Hands-on Lab, contact Melinda Marks of the VMware Public Relations team at mmarks@vmware.com.

## Assumptions

To successfully use this guide it is assumed that:

- All hardware has been validated against the VMware Hardware Compatibility List (HCL);
- VMware vSphere ESX™ or ESXi has been installed on the physical servers designated for this evaluation;
- VMware vCenter™ Server and vSphere Client have been installed in the environment to manage the VMware ESX hosts;
- Shared storage (i.e. a SAN infrastructure) exists for evaluation of vSphere Availability features;
- Virtual machines have been pre-configured and installed with proper Guest Operating Systems.

For detailed information regarding installation, configuration, administration, and usage of VMware vSphere, please refer to the online documentation: http://www.vmware.com/support/pubs/vs_pubs.html.

| TASKS | DOCUMENTS |
|---|---|
| Install vCenter Server and vSphere Client | ESX and VirtualCenter Installation Guide<br>VMware ESXi Installable and vCenter Server Setup Guide<br>VMware ESXi Embedded and vCenter Server Setup Guide |
| Install ESX 4.0<br>Install and Configure VMware ESXi 4.0 Installable<br>Install and Configure VMware ESXi 4.0 Embedded | ESX and VirtualCenter Installation Guide<br>VMware ESXi Installable and vCenter Server Setup Guide<br>VMware ESXi Embedded and vCenter Server Setup Guide |
| Deploy virtual machines | vSphere Basic System Administration |
| Obtain and install licenses | ESX and VirtualCenter Installation Guide<br>VMware ESXi Installable and vCenter Server Setup Guide<br>VMware ESXi Embedded and vCenter Server Setup Guide |

## Document Structure

The purpose of this document is to support a self-guided, hands-on competitive review of VMware vSphere. The document has three sections as outlined below, starting off with basic virtualization features and concepts and moving through to the more advanced virtualization features and concepts in Section 3.

| | SCALE OF DEPLOYMENT | CONTEXT AND PURPOSES |
|---|---|---|
| Section 1 | Small scale deployment with 2 to 3 VMware ESX hosts | Basic configuration of virtualization platform in areas of networking, storage (iSCSI) and cluster. In this section, evaluators will experience VMware vSphere features of:<br>• High Availability (HA)<br>• VMotion |
| Section 2 | Small to medium scale deployment with 4 or more VMware ESX hosts | Intermediate configuration of virtualization platform, including Host Profiles and Fibre Channel storage. In this section, evaluators will experience VMware vSphere features of:<br>1. Distributed Resource Scheduling (DRS)<br>2. Distributed Power Management (DPM)<br>3. Fault Tolerance (FT)<br>4. Storage VMotion™ and Thin Provisioning<br>5. Update Manager |
| Section 3 | Medium to large scale, multi-site deployment with 4 or more VMware ESX hosts per site | Advanced configuration and management topics of virtualization platform:<br>1. Multi-site management using LinkedMode<br>2. vNetwork Distributed Switch (vDS)<br>3. Private VLAN<br>4. Dynamic Storage Management (e.g. growing a dynamic datastore)<br><br>In addition, evaluators will experience VMware vSphere features of:<br>• Hot Add<br>• Custom Alarms (e.g. for network access)<br><br>For hardcore IT administrators who desire to programmatically manage their vSphere environments, this section provides exercises in using the vSphere CLI interfaces:<br>1. Management Assistant (vMA)<br>2. PowerCLI |

## Reference Setup Environments

*Note: Reviewers with access to the Reviewer's Hands-On Lab system will see a slightly different pre-configured setup than the one shown below. Those reviewers should refer to the "VMware vSphere Competitive Reviewer's Hands-On Lab Guide" for details.*

Evaluators will need to provision the necessary hardware for the exercises included in this guide. In this section, details will be provided for a sample environment used for this vSphere evaluation in the lab. Below you will find architecture diagrams that illustrate the following setup in this lab:

- Active Directory, DNS, and DHCP services
- Sample vSphere Evaluation Set
- Logical network setup

### Active Directory, DNS, and DHCP services

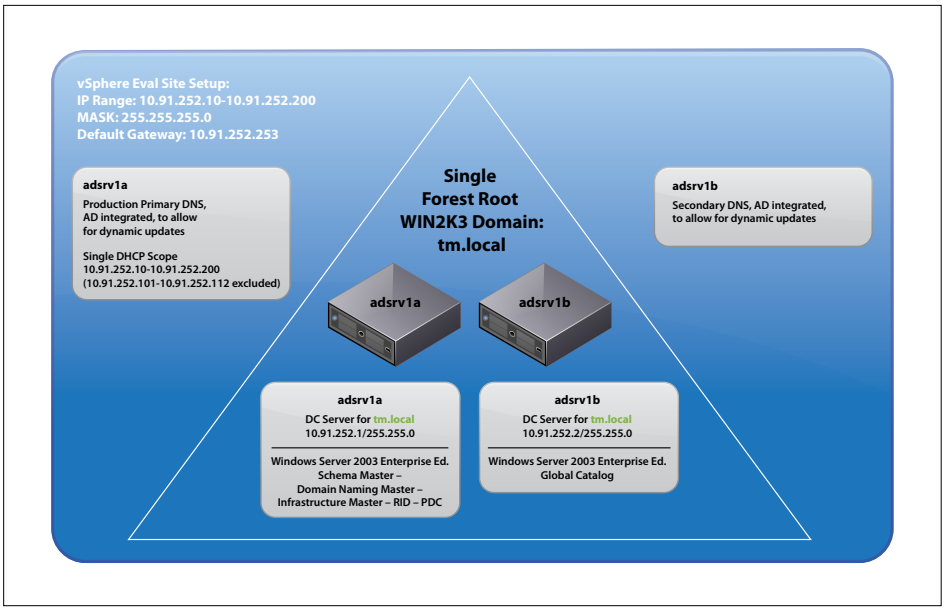



**Diagram A** - Active Directory, DNS, and DHCP services in reference setup environment

## Sample vSphere Evaluation Set

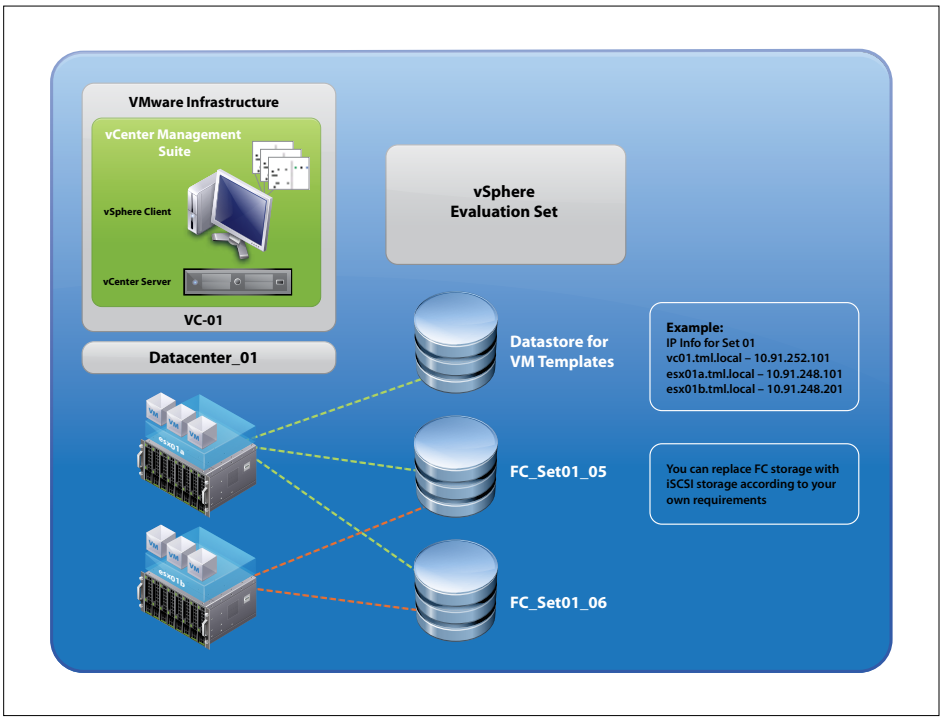



**Diagram B** - Sample vSphere Evaluation Set

## Logical Network Setup

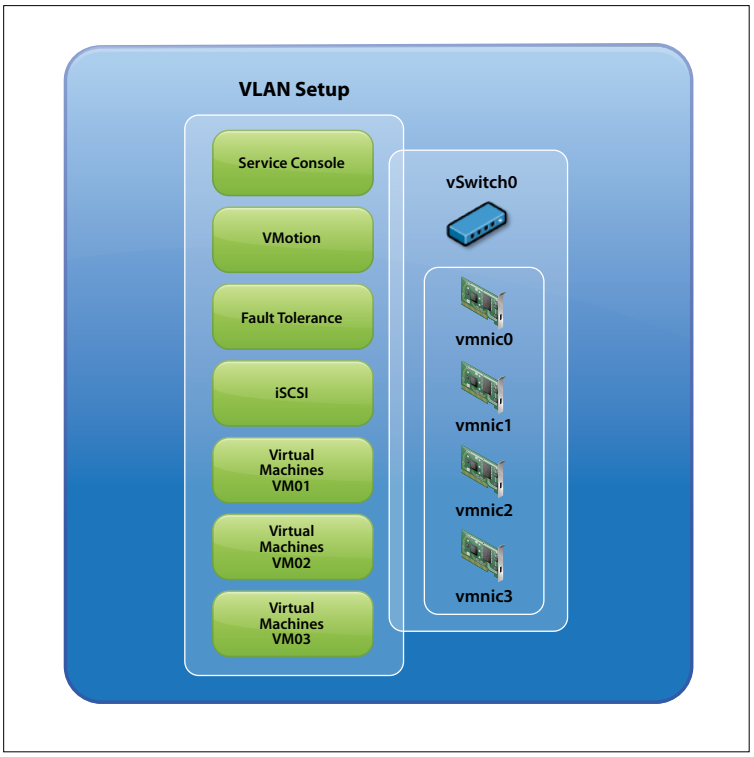



**Diagram C** - VLAN Setup

## What Will Be Covered

The content includes an overview of vSphere virtualization features, configuration options, and key use cases in order to demonstrate the tremendous benefits that vSphere provides to a datacenter. In the tables below, sections of the vSphere review that include competitive differentiators are marked with an asterisk (*).

*Note: The time estimate is an approximation, which may or may not necessarily reflect your time exact spent in each task.*

*Section 1 Summary:*

| CATEGORY | FEATURES | WHAT WILL BE COVERED | TIME ESTIMATES |
|---|---|---|---|
| Infrastructure Setup | vNetwork Standard Switch Configuration* | 1.1 Configure an existing vNetwork Standard Switch according to typical enterprise configuration with VLANs and NIC teaming<br><br>1. Add Port Groups to Standard Switch<br>2. Configure NIC Teaming | 30 minutes |
| Infrastructure Setup | iSCSI Storage Configuration | 1.2 Configure iSCSI Storage to house virtual machines<br><br>1. Confirm iSCSI SW initiator has been configured on VMware ESX<br>2. Create a new iSCSI datastore | 10 minutes |
| Infrastructure Setup | ESX Host Cluster Setup | 1.3 Create a new cluster of ESX hosts<br><br>1. Create a new cluster<br>2. Add ESX hosts to the cluster | 10 minutes |
| Availability and Capacity | High Availability* | 1.4 VMware HA detects server failure and restarts virtual machines on another host<br><br>1. Turn on VMware HA on a cluster<br>2. Set Admission Control and additional VMware HA options | 10 minutes |
| Availability and Capacity | VMotion* | 1.5 Allows the migration of running virtual machines from one ESX host to another.<br><br>1. Migrate a running virtual machine from one host to another host | 10 minutes |

*Section 2 Summary:*

| CATEGORY | FEATURES | WHAT WILL BE COVERED | TIME ESTIMATES |
|---|---|---|---|
| Infrastructure Setup | FC Storage Setup | 2.1 Create a second FC datastore<br><br>1. Create a new VMFS Volume/Datastore | 10 minutes |
| Infrastructure Setup | Host Profiles* | 2.2 Use host profiles to automate host provisioning and configuration:<br><br>1. Add two new hosts and re-configure their DNS and NTP settings<br>2. Create a host profile from a reference host<br>3. Attach host profile and check for host compliance<br>4. Apply host profile and re-check for host compliance | 30 minutes |
| Availability and Capacity | Distributed Resource Scheduling* | 2.3 Load balances resource utilization across a cluster using VMotion.<br><br>1. Turn on VMware DRS for a cluster<br>2. Set automation level for DRS cluster<br>3. Set automation level for each virtual machine | 10 minutes |
| Availability and Capacity | Distributed Power Management* | 2.4 Monitors the CPU and memory resource utilization of a cluster and decides whether to power off ESX hosts to reduce power consumption<br><br>1. Turn on VMware DPM for a cluster<br>2. Set Power Management for each ESX host in the cluster<br>3. Observe VMware DPM generating and executing recommendations | 20 minutes |
| Availability and Capacity | Fault Tolerance* | 2.5 VMware FT allows failover of a virtual machine with no data loss during server failures.<br><br>1. Turn on VMware Fault Tolerance for a virtual machine<br>2. Convert virtual disks to thick-provisioned virtual disk<br>3. Observe the following actions after turning on VMware FT<br>4. Simulate server failure to demonstrate FT failover<br>5. Observe vSphere alarms after host failure | 45 minutes |
| Availability and Capacity | Storage vMotion and Thin Provisioning* | 2.6 Storage VMotion and Thin Provisioning.<br><br>1. Move VM from one datastore to the iSCSI datastore.Change the virtual disk format as you move the VMhome to the new datastore | 20 minutes |

| CATEGORY | FEATURES | WHAT WILL BE COVERED | TIME ESTIMATES |
|---|---|---|---|
| Application Deployment and Management | VMware vApp* | 2.7 Use VMware vApp to deploy and manage a multi-tier application:<br><br>1. Create a vApp<br>2. Specify startup sequence for the multi-tier application and perform single-step power operation | 10 minutes |
| Maintenance | Update Manager* | 2.8 Using Update Manager to automate ESX host and virtual machine patching and remediation Patching a cluster of ESX hosts with critical host patches<br><br>1. Attaching a Critical Host Patches Baseline to the cluster<br>2. Scanning the cluster for critical patch vulnerabilities<br>3. (Optional) Staging patches<br>4. Remediating the cluster with critical patches | Varies depending on number of patches |
| | | Orchestrated upgrade of datacenter to ESX 4.0 Upgrading an ESX 3.5 host to ESX 4.0 Upgrading VMware Tools and VM hardware<br><br>1. Attaching Tools upgrade Baseline group to the VM<br>2. Scanning the VM for VMware Tools and VM hardware upgrade compliance<br>3. Remediating the VM with VMware Tools and VM hardware upgrades | 60 minutes per host |
| | | Configuring Update Manager to use a central shared Patch Repository<br><br>1. Modifying Update Manager settings using vSphere Client | 10 minutes to configure Update Manager. Time to setup patch repository varies depending on the number and size of patches |

*Section 3 Summary:*

| CATEGORY | FEATURES | WHAT WILL BE COVERED | TIME ESTIMATES |
|---|---|---|---|
| Infrastructure Setup | Linked Mode* | 3.1 Automatic Role Replication across vCenter instances and performing cross vCenter tasks<br><br>Automatic Role Replication across vCenter instances:<br>1. Create a custom role<br>2. Grant role to user or group<br>3. Verify replication<br><br>Perform cross vCenter tasks<br>1. Remediate VMs with out-of-date VMware Tools<br>2. Identify datastores with low free space | 20 minutes |
| Infrastructure Setup | vNetwork Distributed Switch* | 3.2 Migrate from Standard Switch to a vNetwork Distributed Switch Per Host Manual Migration to vDS:<br><br>1. Create vDS<br>2. Create DV Port Groups<br>3. Add host to vDS and migrate vmnics and virtual ports<br>4. Delete Standard Switch<br>5. Repeat Steps 3 & 4 for remaining hosts<br><br>Configuration and Deployment of vDS using Host Profiles<br><br>1 - 4 Migrate Reference Host to vDS using Step 1- 4 of Manual Migration<br>5. Create Host Profile of Reference Host<br>6. Attach and apply Host Profile to Candidate Hosts<br>7. Migrate VM Networking to vDS | 90 minutes |
| Infrastructure Setup | Private VLANs with vNetwork Distributed Switch* | 3.3 Create and use a Private VLAN on a vNetwork Distributed Switch:<br><br>1. Configure vDS for Private VLAN<br>2. Create new DV Port Groups for Private VLANs<br>3. Move VMs to new DV Port Groups | 30 minutes |
| Availability and Capacity | VMware Hot Add* | 3.4 Hot add capacity to powered-on virtual machines:<br><br>1. Enable memory/CPU hotplug support<br>2. Hot add CPU and memory to a powered-on virtual machine | 10 minutes |

| CATEGORY | FEATURES | WHAT WILL BE COVERED | TIME ESTIMATES |
|---|---|---|---|
| Availability and Capacity | Dynamic Storage Management* | 3.5 Migrate virtual machines to fill up a datastore, trigger an alarm, and then solve the issue by increasing the size of that datastore.<br><br>1. Use datastore views to confirm which virtual machines are in each datastore<br>2. Use Storage VMotion to fill up a datastore and trigger an alarm<br>3. Detect and investigate alarm that is triggered<br>4. Expand the datastore using VMFS Volume Grow<br>5. Notice alarm is now no longer raised | 60 minutes |
| Availability and Capacity | Custom Alarm Setup* | 3.6 Using a custom alarm for network access<br><br>1. Configure a vNetwork Distributed Switch<br>2. Set up a custom network alarm<br>3. Trigger the alarm | 20 minutes |
| Programmability | vSphere Management Assistant (vMA) | 3.7 Using vMA to interact remotely with ESX and ESXi Adding a vSwitch to an ESX host, creating a portgroup and adding an uplink:<br><br>1. Adding target hosts to vMA<br>2. List the vSwitches on the host<br>3. Add a vSwitch to the host, add a portgroup and an uplink | 10 minutes |
| | | Gathering logs from multiple ESX and ESXi hosts:<br><br>1. Adding target hosts to vMA<br>2. Setting Up Log Collection for ESX/ESXi Hosts | 10 minutes |
| Programmability | PowerCLI | 3.8 Using PowerCLI to perform vSphere management tasks:<br><br>1. Enabe VMotion on all VMs<br>2. Storage VMotion with PowerCLI<br>3. Simple Automated Reporting with PowerCLI | 60 minutes |

# VMware vSphere Review Worksheet

You can use the worksheet below to organize your competitive review process.

| HARDWARE CHECKLIST: | |
|---|---|
| All hardware has been validated against the VMware Hardware Compatibility List (HCL) | |

| SOFTWARE CHECKLIST: | |
|---|---|
| VMware vSphere VMware ESX | |
| VMware vCenter Server | |
| VMware vSphere Client | |

After you have successfully installed the VMware vSphere software components on your hardware, you can proceed to perform the review of VMware vSphere. For each scenario, you can use the corresponding checklist below to ensure that you are following the proper sequence.

| SECTION 1 | |
|---|---|
| Network Configuration | |
| Storage Configuration | |
| Cluster Setup | |
| High Availability | |
| vMotion | |

| SECTION 2 | |
|---|---|
| FC Storage Setup | |
| Host Profiles | |
| Distributed Resource Scheduling | |
| Distributed Power Management | |
| Fault Tolerance | |
| Storage vMotion and Thin Provisioning | |
| vApp | |
| Update Manager | |

| SECTION 3 | |
|---|---|
| Linked Mode | |
| vNetwork Distributed Switch | |
| Private VLAN | |
| Hot Add | |
| Dynamic Storage Management | |
| Custom Alarm Setup | |
| Management Assistant | |
| PowerCLI | |

**Help and Support During the Review**

This guide is intended to provide an overview of the steps required to ensure a successful review of VMware vSphere. It is not meant to substitute for product documentation. Please refer to the online product documentation for vSphere for more detailed information (see below for links). You may also consult the online Knowledge Base if you have any additional questions. Press and analyst reviewers that require further assistance may contact the VMware Public Relations team (mmarks@vmware.com) to be placed in contact with technical resources at VMware. Customers that require further assistance should contact a VMware sales representative or channel partner.

VMware vSphere and vCenter Resources:

- Product Documentation:
  http://www.vmware.com/support/pubs/
- Online Support:
  http://www.vmware.com/support/
- Support Offerings:
  http://www.vmware.com/support/services
- Education Services:
  http://mylearn1.vmware.com/mgrreg/index.cfm
- Support Knowledge Base:
  http://kb.vmware.com
- VMware vSphere Management Assistant—VMware Command-Line Interface Installation and Reference Guide
- PowerCLI Toolkit Community:
  http://communities.vmware.com/community/developer/windows_toolkit
  (or type Get-VIToolkitCommunity within PowerCLI)
- PowerCLI Blogs:
  http://blogs.vmware.com/vipowershell

### VMware Contact Information

For customers seeking additional information or to purchase VMware vSphere, VMware's global network of solutions providers is ready to assist. If you would like to contact VMware directly, you can reach a sales representative at 1-877-4VMWARE (650-475-5000 outside North America) or email sales@vmware.com. When emailing, please include the state, country and company name from which you are inquiring. You can also visit http://www.vmware.com/vmwarestore/.

Press and analyst reviewers conducting comparative reviews of VMware vSphere and competing virtualization products should contact the VMware Public Relations team (mmarks@vmware.com).The VMware PR team can arrange access to the vSphere Competitive Reviewer's Hands-On Lab and can arrange access to special technical support resources.

### Providing Feedback

We appreciate your feedback on the material included in this guide. In particular, we would be grateful for any guidance on the following topics:

- How useful was the information in this guide?
- What other specific topics would you like to see covered?
- Overall, how would you rate this guide?

Please send your feedback to the following address: tmdocfeedback@vmware.com, with "VMware vSphere Competitive Reviewer's Guide" in the subject line. Thank you for your help in making this guide a valuable resource.

# Introduction: Top 15 vSphere Advantages Over the Competition

1. **The Industry's Most Reliable Virtualization Platform Just Got Better—VMware ESX/ESXi 4.0**
   VMware ESX/ESXi 4.0 extends VMware's legacy of highly reliable, highly scalable virtualization by delivering even greater levels of robustness, security, and performance. Already, over 85% of ESX/ESXi deployments are in production environments—an example of how companies, both large and small, trust VMware for their business critical workloads. ESXi 4.0 is VMware's thin virtualization form factor with no dependence on a general-purpose server operating system in the virtualization layer. With a 70MB disk footprint, ESXi 4.0 dramatically shrinks the code base that needs to be maintained and secured, ultimately resulting in a more secure environment. In contrast, all versions of Microsoft Hyper-V R2 will still rely on Windows Server running inside the parent partition, the same architecture as Hyper-V R1. Therefore, the smallest version of Hyper-V R2 currently available (Windows Server 2008 R2 RC with Server Core installation) still has a disk footprint of~3.6GB, representing millions more lines of code to maintain and secure. Hyper-V R2's continued dependence on Windows means it still faces performance and scalability limitations, especially when running many concurrent virtual machines on the same host. With Hyper-V, the security and stability of your datacenter will always be dependent on the security and stability of Windows.

2. **Reliable, Cost-effective Solutions for Small Offices—New vSphere Essentials Editions**
   The robust, proven capabilities of VMware vSphere are now also available in two cost-effective packages designed for small offices, starting at just $166 per processor. vSphere Essentials Edition enables server consolidation and centralized provisioning, management, and patching for immediate savings on hardware and operational costs. It also includes integrated physical-to-virtual conversion capabilities and the VMware VMsafe security APIs for third-party security products, resulting in an even better level of security than what is available on physical servers. vSphere Essentials Plus Edition is an easy-to-deploy "Always on IT" package that includes everything from Essentials and adds capabilities to dramatically improve application uptime and quickly deploy data protection (with built-in data deduplication to save on storage costs). With vSphere Essentials and Essentials Plus, small offices get the industry's most proven, complete virtualization platform in an integrated package that solves a small office's most pressing needs—application uptime and data protection. The "free" Hyper-V R2 offering from Microsoft will still be just a hypervisor with point capabilities, instead of a complete solution, and small businesses still need to purchase Microsoft System Center to get management capabilities that are critical for controlling costs.

3. **Higher Consolidation Ratios Means Lower Cost than "Free"—vSphere Performance Improvements**
   Better performance and utilization lead to higher virtual machine consolidation ratios, which lead to lower capital expenditure costs. vSphere significantly improves the performance of all sub-systems, over the already high standards set by VMware Infrastructure 3, from CPU to memory to storage to networking to cluster-level utilization, to achieve the highest consolidation ratios in the industry. (Refer to the vSphere Key Features document for details on all of vSphere's performance improvements.) This VMware advantage results in a lower total cost compared to virtualizing with other vendors' so-called "free" offerings. Microsoft Hyper-V R2 will continue to trail considerably in consolidation ratios as it lacks fundamental capabilities like a high performance 'gang' scheduler, memory oversubscription, direct driver model, and logical resource pools with dynamic load balancing. As a result, Microsoft's "free" Hyper-V offering is usually more expensive than VMware's robust, proven vSphere solution.

4. **Zero Downtime, Zero Data Loss for Applications—New VMware Fault Tolerance (FT)**
   VMware FT ensures that protected applications are always available, even in the event of hardware failure—your applications may never have to go down again. FT creates a shadow copy of a protected virtual machine and automatically triggers a seamless stateful failover should the virtual machine stop responding due to hardware failure. After the failover, FT automatically creates a new shadow copy on another host to ensure continuous protection. FT works with all types of shared storage (Fibre Channel, NAS or iSCSI) and with all operating systems supported by VMware ESX. No complex set-up is required, and applications do not have to be cluster-aware. Microsoft has no equivalent functionality. Microsoft, in January 2009, did make a pre-announcement with Marathon Technologies on an FT-like capability for Hyper-V R2. But since then, there has been no update on delivery date or any public beta code. Microsoft will claim that active-active clustering can address the same need, but active-active clustering is complex to set-up and only works with a small set of cluster-aware applications.

5. **Virtual Networking for Internal Clouds—New VMware vNetwork Distributed Switch**
   With VMware vNetwork Distributed Switch, IT can manage one virtual switch that spans an entire cluster instead of managing a separate virtual switch for each host—a new, time-saving way to manage virtual networks. It creates a single distributed switch that spans a cluster of ESX/ESXi hosts and retains network runtime state when virtual machines move between hosts. This new capability is a critical enabler for building internal clouds as it allows cluster-level network settings to be managed and policies enforced centrally. Networking vendors have built third-party virtual switches, like the Cisco Nexus 1000V, based on the vNetwork Distributed Switch to make it easier to integrate virtualized environments and manage physical and virtual networks with a common set of tools. For customers this means that environments that were not previously virtualized, due to security reasons, DMZ or compliance requirements, can now be easily virtualized and centrally controlled. Microsoft Hyper-V R2 will have nothing comparable to vNetwork Distributed Switch. Those who deploy Hyper-V R2 will have to manually manage virtual networks on a host-by-host basis. Each time a Hyper-V virtual machine migrates from one host to another, the admin may need to manually reconfigure network settings for the virtual machine.

6. **A Better Way to Enforce Security in a Virtual Environment—New VMware vShield Zones**
   A key benefit of virtualization is the ability to break down silos within the datacenter. So why create silos of physical virtualization hosts to enforce security zones? VMware vShield Zones let's you manage your security zones in software. vShield Zones controls network access to sensitive areas of the virtual datacenter (ex. DMZ, applications subject to SOX compliance) on a virtual machine by virtual machine basis. Companies can enforce security zones using this integrated vSphere capability (manage it in software) instead of creating new physical silos of virtualization hosts (manage it by separating hardware). This capability is critical to the sharing of resource computing pools, a core element of cloud computing. Microsoft Hyper-V R2 will have nothing comparable to vShield Zones. Those who deploy Hyper-V R2 will have to enforce security zones by setting up silos of physical Hyper-V hosts.

7. **Easiest Way to Configure Virtualization Hosts—New VMware Host Profiles**
   VMware Host Profiles greatly simplify ESX host configuration management, thereby reducing operational costs since IT admins spend less time manually configuring and compliance checking each individual host. Host Profiles automatically apply a "gold" host configuration profile (includes networking, storage, and security settings) to multiple ESX hosts. It also monitors compliance to the "gold" host configuration profile and can remediate noncompliant hosts with the push of a button. Microsoft Hyper-V R2 RC has no automated, out-of-box host profiling capability. Host configuration and remediation requires a manual installation and not-so-easy configuration of System Center Configuration Manager.

8. **Add Virtual Machine Resources with No Downtime—New Hot-add CPU/memory, Hot-Extend Disks**
   Even with the best pre-planning, applications sometimes require more resources than originally expected. VMware vSphere delivers hot-add virtual CPU / memory and hot-add/extend virtual disks to dynamically add virtual machine resources. The ability to hot-add and hot-extend allows IT to increase the amount of resources available to an application by provisioning additional CPU, memory, and disk to the virtual machine without disrupting the application or the end-users. Hot-add/extend of virtual disk is supported on all virtual machines. Hot-add of virtual CPU/memory is supported on any guest operating system that natively supports hot-add CPU/memory on a physical server. Microsoft had originally said hot-add of virtual CPU/memory would be in Hyper-V R1, but had to de-commit. Microsoft has made no mention of this capability for Hyper-V R2.

9. **Virtualize 100% of Your Applications—New Support for Eight Virtual CPUs and 256 GB per VM**
   Higher CPU and memory maximums per virtual machine allow companies to virtualize the CPU and memory intensive applications in their datacenters. VMware vSphere enables a single virtual machine to simultaneously use up to eight logical processors (8-way virtual SMP) and 256GB of RAM. With 8-way virtual SMP even the most processor-intensive applications, like databases and messaging servers, can be virtualized with no impact to performance. With 256GB per virtual machine, companies can run the most memory-intensive workloads in virtual machines. Microsoft Hyper-V R2 will only support up to 4-way virtual SMP on Windows Server 2008 VMs—all other guest operating systems are limited to 1- or 2-way virtual SMP. Regarding memory, Hyper-V R2 will only support up to 64GB of RAM per virtual machine. These limitations of Hyper-V R2 mean that companies can only virtualize a small subset of their applications.

10. **Enabling the Internal Cloud in the Datacenter—Improved Logical Resource Pools and DRS**
    VMware vSphere's new cluster-level management capabilities (ex. vNetwork Distributed Switch, vShield Zones, and Distributed Power Management), its performance and utilization optimizations, and its VMware Distributed Resource Scheduler (DRS) all improve the effectiveness and flexibility of VMware Logical Resource Pools. These resource pools aggregate and share resources across many servers—the essence of cloud computing. Companies can create a logical, shared pool of resources for a specific business group and guarantee resource availability while maintaining isolation from other pools. VMware Distributed Resource Scheduler (DRS) enables intelligent, automated load balancing so applications get the right level of resources at the right time. DRS is the heart of enabling logical resource pools that deliver on SLAs. Microsoft Hyper-V R2 will have nothing comparable. Those who deploy Microsoft Hyper-V R2 will have to set up dedicated hosts or clusters of hosts for each business group, a rigid, siloed infrastructure that is time-consuming and costly to maintain.

11. **Lower OpEx Costs during Planned Maintenance—Improved VMware VMotion, Storage VMotion**
    The need to perform planned maintenance during non-peak hours is a significant contributor to higher operational costs. Overtime pay for nights and weekends is compounded with time spent coordinating with business owners to schedule a maintenance window. vSphere improves on the market-proven VMware VMotion and Storage VMotion capabilities that allow IT admins to perform planned maintenance during normal business hours without a maintenance window. Enhanced VMotion Compatibility (EVC) automatically configures servers whose CPUs feature Intel FlexMigration and AMD-V Extended Migration technologies to be VMotion-compatible with servers that use older CPUs. Storage VMotion now works across different types of storage (FC, iSCSI, NFS, DAS) and has a new graphical administrator interface in vCenter Server. Microsoft Hyper-V R2 will have a CPU compatibility mode but it downgrades the entire Hyper-V cluster to look like Pentium 4 CPUs to the VMs (Intel CPU generation from 2005). For storage migration, Hyper-V R2 will have an inferior capability called "Quick Storage Migration" which causes application downtime.

12. **Save on Storage Costs—New VMware vStorage Thin Provisioning with Comprehensive Alerts**
    VMware vStorage Thin Provisioning is a cost-saving technology that defers and avoids excess storage costs. The technology lowers capital and operating expenditures by reducing disk purchase and cutting the power and cooling cost of the excess disk. Thin provisioning works by enabling IT admins to create virtual machines without having to provision all the storage upfront. When a virtual machine is created, the thin-provisioned disk only consumes what's needed. Then, the virtual disk grows over time when more storage space is required. vStorage Thin Provisioning comes with comprehensive consumption-based monitoring and alerting. IT admins can set alerts to trigger when they need to procure more storage or rebalance virtual machines across the available storage with Storage VMotion. These monitoring and alerting capabilities prevent accidentally running out of storage space. Microsoft Hyper-V R2 has thin provisioning of disks, but lacks the built-in monitoring and alerting capabilities that make it safe to use.

13. **Save Even More Energy—VMware Distributed Power Management is now Fully Supported**
    VMware Distributed Power Management (DPM) reduces datacenter energy consumption during non-peak hours by consolidating workloads within a cluster and turning off unneeded servers—think of it as cluster-wide power management. While other offerings only focus on power savings for individual servers, DPM provides a holistic, cluster wide approach to power savings.. To conserve energy during periods of low utilization (ex. evenings, weekends), DPM consolidates workloads and powers off unused host servers. When utilization is expected to increase (ex. before a work day begins), DPM brings servers back online to ensure service levels are met. Microsoft Hyper-V R2 RC has nothing comparable. Microsoft talks about PRO Tips, but has not demonstrated a PRO Tips based solution that can intelligently consolidate, power-off, and power-on a cluster of Hyper-V hosts based on application resource requirements. Microsoft also touts Core Parking, but that only conserves energy at the core-level.

14. **Use the Operating System that's Right for You—Broadest Guest Operating System Support**
    VMware has always supported the broadest set of guest operating systems in the industry, including Windows, Linux, Solaris and Novell NetWare, so companies can virtualize their existing applications and maintain flexibility for future applications. vSphere adds new support for several additional operating systems such as Asianux, CentOS, Debian , FreeBSD, OS/2, and new versions of Windows Server, Solaris, SCO OpenServer, SCO Unixware, RHEL, SLES, MS-DOS, and NetWare. In all, vSphere supports over forty five different guest operating systems/versions—that's more versions of Windows than even Microsoft Hyper-V supports and more versions of Linux than Citrix XenServer supports. In contrast, Microsoft Hyper-V currently supports only one non-Windows operating system—Novell SUSE Linux. This lack of non-Windows support limits a customer's ability to virtualize existing non-Windows applications and restricts choice when making future application decisions.

**15. Built-in NIC Failover and Load Balancing—Improved Integrated NIC Teaming**

VMware vSphere provides built-in NIC failover and load balancing to each networked virtual machine, which results in greater hardware availability and fault tolerance in case of NIC failure. It works with any NIC supported by VMware ESX. NIC teaming policies allow users to configure multiple active and standby adapters, and teaming configurations can vary per port groups on the same virtual switch and uplinks. Microsoft Hyper-V R2 will still not have integrated NIC teaming, instead relying on third-party NIC drivers to provide the functionality. The issues with the third-party approach are: 1) the drivers only work with NICs from that same third-party, 2) it requires a separate installation, and 3) it is unclear whether Microsoft or the third-party provides support should an issue arise.

# Section 1: Features for Small-Scale Deployments

## 1.1. vNetwork Standard Switch

**What is it?**

Virtual switches (vNetwork Standard Switches) are just like physical switches that live inside ESX hosts. Just like a physical access switch provides connectivity and fan-out to hosts at the network edge, a virtual switch provides the same connectivity function within a host to each of the VMs and uses the server NICs as uplinks to the physical network.

**Use Case:** Configuring a Standard Switch

In this exercise you will configure a standard switch on an ESX host for a number of traffic types on separate VLANs. You will also configure NIC teaming for effective load balancing and maximum availability.

### 1.1.1. VMware Differentiators

VMware vSphere provides an integrated, easy-to-use, hardware-independent solution to set up and manage NIC failover, load balancing, networking traffic shaping and networking security.

- **Easiest-to use networking management:** With vSphere, users can perform fundamental networking management tasks directly from vCenter Server in just a few clicks. Users can set up NIC teaming and load balancing policies, shape outbound traffic from virtual switches and set up layer-2 (data link layer) networking security.

  Microsoft does not provide native support for NIC teaming and forces users to rely on NIC hardware capabilities which are typically managed through unfamiliar and complex Command Line Interfaces. VMware vSphere greatly reduces the complexity related to networking management by providing a hardware independent solution that gives users greater flexibility of choice and can be managed directly from vCenter in just a few easy clicks.

- **Hardware independence:** VMware vSphere allows users to benefit from NIC teaming, load balancing, traffic shaping and security even when not natively supported by hardware.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **VNETWORK STANDARD SWITCH MANAGEMENT** | | | |
| Integrated native support for active/active and active/passive NIC teaming | Yes | No | No |
| Integrated native support for NIC traffic load balancing policies (originating virtual port ID, IP hash, source MAC hash) | Yes | No | No |
| Integrated native support for network failover detection based on Link Status and Beacon Probing | Yes | No | No |
| Integrated native support for layer-2 (data link) networking security policies (Promiscuous Mode, MAC address change, Forged Transmit) | Yes | No | No |
| Integrated native support for switch outbound traffic shaping at the port level (average bandwidth, peak bandwidth, burst size) | Yes | No | No |
| Simplify port configuration by utilizing Port Groups across multiple virtual ports. The Port Group specifies all information needed to enable a port: NIC teaming policy, VLAN tagging, Layer 2 security, and traffic shaping. | Yes | No | No |
| Discover and advertise physical and virtual network configurations for better debugging and monitoring of Cisco-based environments from within vCenter Server. | Yes | No | No |

### 1.1.2. vNetwork Standard Switch Hands-on Review

This section assumes little or no virtual network knowledge. It will lead the reader through some basic configuration of virtual networking using vNetwork Standard switches (formerly called vSwitches or virtual switches).

| | | | |
|---|---|---|---|
| Infrastructure Setup Troubleshooting | vNetwork Standard Switch Configuration | 1.1 Configure an existing vNetwork Standard Switch according to typical enterprise configuration with VLANs and NIC teaming<br><br>1. Add Port Groups to Standard Switch<br>2. Configure NIC Teaming | 30 minutes |

*Getting Started*

Familiarize yourself with the vSphere Client, particularly the Configuration tab under the **Home** > **Inventory** > **Hosts and Clusters** view. Click on **Networking** in the Hardware box. See Figure 1.1 a The boxes highlight where you need to be to configure the Standard Switch.

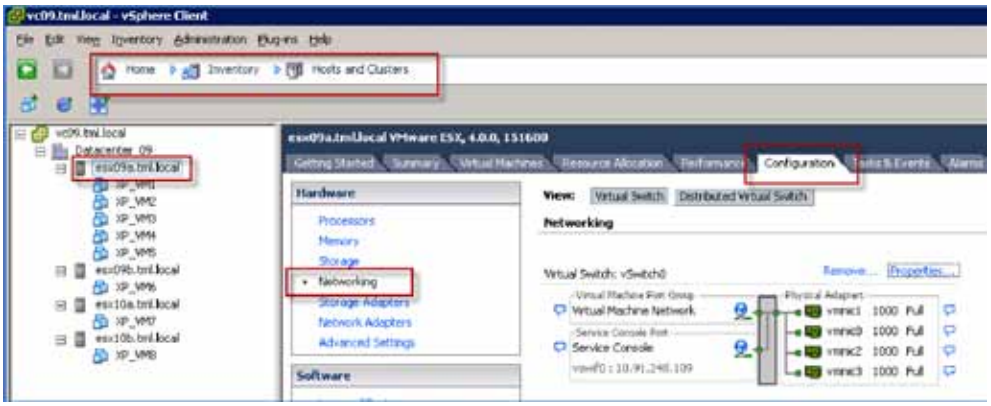



**Figure 1.1 a.** Configuration Panel in vSphere Client for Standard Switch

When an ESX host is initially created, it will have a Standard Switch (vSwitch0) already defined with a Service Console port labeled "vswif0". This is the management port used to communicate with the host. Note that an VMware ESXi host (also known as ESX Embedded) will use a vmkernel port instead of a Service Console port.

There are four physical adapters (NICs) in the example server (esx09a.tml.local). These are labeled vmnic0 through vmnic3. These are the uplinks from the virtual switch to the adjacent physical switch or switches.

*More about Virtual Switches*

Virtual Switches or Standard Switches operate very similarly to real physical switches. The physical NICs (vmnics or pnics) operate as uplinks to the physical network and virtual NICs (vnics) connect the virtual switch with the VMs and various virtual adapters in the host (e.g. Service Console, Software iSCSI port, VMotion port, etc.).

Virtual Switches also support VLAN segmentation and trunking using the IEEE 802.1Q specification. This enables you to separate and manage the various traffic types (management, VM, iSCSI, VMotion, NFS) without being restricted by the number of available vmnics. Best practice networking with ESX involves extending VLAN trunks to the VMware ESX host with individual VLANs allocated to each of the traffic types mentioned above.

Virtual Switches support NIC teaming. (Note: this is not related to any proprietary NIC teaming provided by the NIC manufacturers.) NIC teaming enables efficient use of the available NICs by balancing the traffic over the NICs. NIC teaming also contributes to high availability when teams are distributed over multiple adjacent physical switches.

*Desired Environment*

This target virtual network environment involves allocating one VLAN with corresponding IP subnet per traffic type. This is shown below in Table 1.

Note that in this example, you are using the Native VLAN for management. By default, this would correspond to VLAN 1 on the physical switch (but check!). In a real environment, best practice is to not use VLAN 1 and the Native VLAN and just use VLANs numbered 2 and above. Check the VLAN policies with your network administrator.

| TRAFFIC TYPE | PORT GROUP NAME | VLAN | IP NETWORK (255.255.255.0 MASKS |
|---|---|---|---|
| Virtual Machine traffic—application #1 | VM01 | 2936 | 10.91.101.0 (DHCP allocation) |
| Virtual Machine traffic—application #2 | VM02 | 2937 | 10.91.102.0 (DHCP allocation) |
| Virtual Machine traffic—application #3 | VM03 | 2999 | 10.91.103.0 (DHCP allocation) |
| Fault Tolerance | FT01 | 2935 | 10.91.251.0 |
| iSCSI | iSCSI01 | 2934 | 10.91.250.0 |
| VMotion | VMotion01 | 2933 | 10.91.249.0 |
| ESX host management | Management Network (VMware ESXi) Service Console (ESX)0 | Native (none) | 10.91.248.0 |

**Table 1** - Traffic types and VLAN allocation for example environment

In this environment example, the three VM subnets are using DHCP for IP address allocation. The other virtual adapters (FT01, iSCSI01, VMotion01) will typically use static IP address assignments. Have an IP address assignment plan available for each of these subnets.

### Step 1: Add Port Groups to a Standard Switch

Add a Port Group for each of the traffic types outlined above.

1. From the **Home** > **Inventory** > **Host and Clusters** panel, select the "Configuration" tab and "Networking" in the "Hardware" box.
2. Select "**Add Networking...**" from the top right of the panel

Be sure to select the "Virtual Machine" connection type for the VM port groups (e.g. VM01, VM02, and VM03) and the "VMkernel" connection type for the others (FT01, iSCSI01, and VMotion01). For Fault Tolerance and VMotion, select the correct checkbox in the Port Group Properties panel to ensure the appropriate services are available to those vmkernel ports. See Figure 1.1 b.

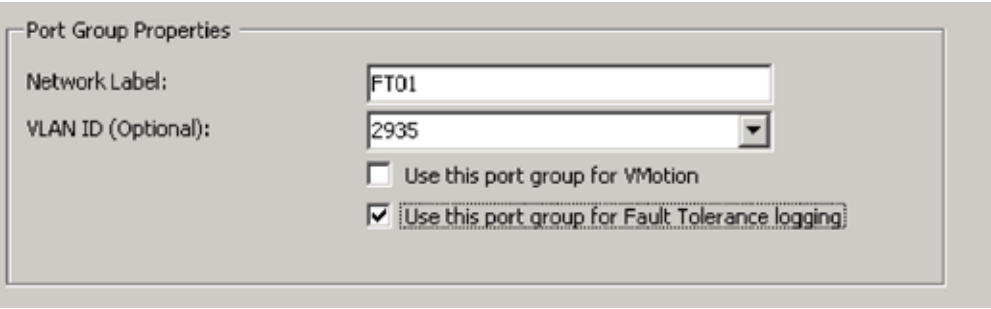



**Figure 1.1 b.** Fault Tolerance and VMotion require selection of appropriate checkbox during configuration

When all Port Groups are configured, the Standard Switch (vSwitch0) will look like Figure 1.1 c.


**Figure 1.1 c.** Standard Switch after configuration of port groups

### Step 2: Configure NIC Teaming

Proper NIC teaming policies protect the server against single points of failure in the network and distribute load over the available vmnics in a manageable way.

The NIC teaming policies for this evaluation environment are shown in Table 2. To protect against single points of failure in the network, the VMware ESX host is connected to two adjacent physical switches (Switch#1 and Switch#2) with the vmnic assignments shown.

Ensure that the adjacent physical switches have Layer 2 continuity (i.e. they share the same Layer 2 broadcast domain) on all trunked VLANs shown or failovers will not work.

NIC teaming policies can be set at the vSwitch level or Port Group level. Port Group policies will override vSwitch policies.

Edit each of the Port Groups according to the policies shown in Table 2. Refer to the ESX Configuration Guide for details on configuring NIC teaming.

| PORT GROUP | VLAN | LOAD BALANCING | VMNIC0 SWITCH#1 | VMNIC1 SWITCH#1 | VMNIC2 SWITCH#2 | VMNIC3 SWITCH#2 |
|---|---|---|---|---|---|---|
| VM01 | 2936 | Orig Virtual Port | — | Active | — | Active |
| VM02 | 2937 | Orig Virtual Port | — | Active | — | Active |
| VM03 | 2999 | Orig Virtual Port | — | Active | — | Active |

| PORT GROUP | VLAN | LOAD BALANCING | VMNIC0 SWITCH#1 | VMNIC1 SWITCH#1 | VMNIC2 SWITCH#2 | VMNIC3 SWITCH#2 |
|---|---|---|---|---|---|---|
| FT01 | 2935 | Explicit Failover | Active | — | Standby | — |
| iSCSI01 | 2934 | Explicit Failover | Standby | — | Active | — |
| VMkernel01 | 2933 | Explicit Failover | Standby | — | Active | — |
| management | native | Explicit Failover | Active | — | Standby | — |

**Table 2** - NIC teaming policies for Standard Switch in evaluation environment

Example configurations for the VM01 Port Group and the Service Console Port Group using these policies are shown in Figure 1.1 d. Note how the vmnics are assigned as active, standby or unused, and the load balancing policy is selected.

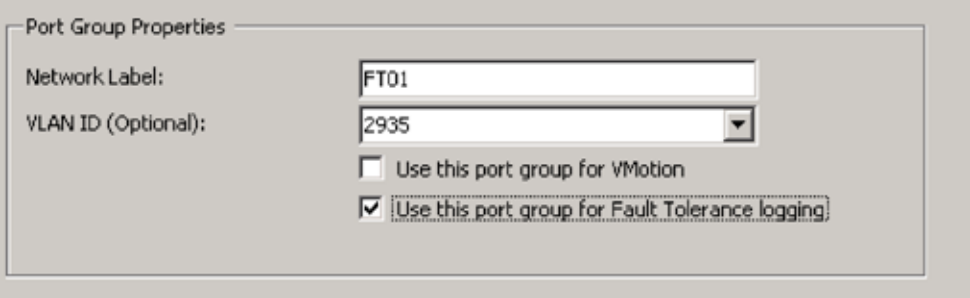



**Figure 1.1 d.** NIC Teaming Policy for VM01 Port Group and Service Console

This completes the basic configuration of a Standard Switch. Replicate these configuration changes on the remaining ESX hosts using the process above or Host Profiles. Host Profiles is are described later in this document.

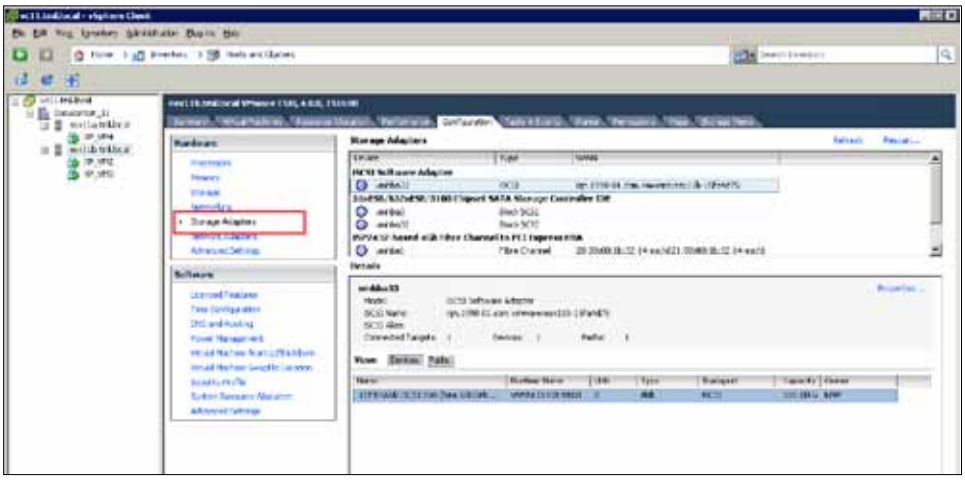
## 1.2. iSCSI Storage

| | | | |
|---|---|---|---|
| Infrastructure Setup | iSCSI Storage Configuration | 1.2 Configure iSCSI Storage to house virtual machines<br><br>1. Confirm iSCSI SW initiator has been configured on VMware ESX<br>2. Create a new iSCSI datastore | 10 minutes |

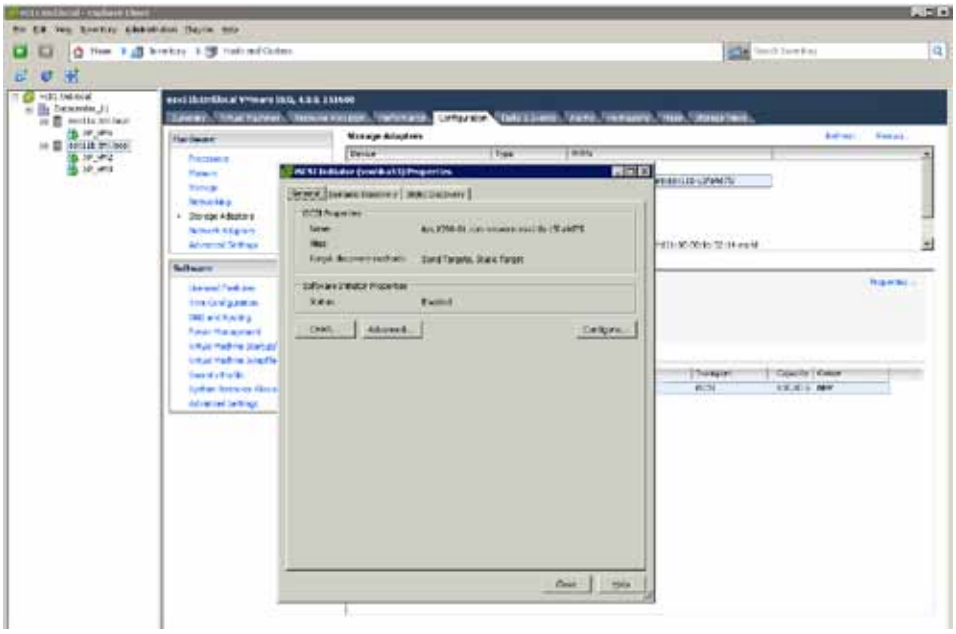
*Use Case-Configure iSCSI Storage to house virtual machines*
This next section will create a datastore on an iSCSI LUN to place virtual machines. For this to be done, first confirm that the ESX server has been configured to enable use of the iSCSI software initiator and the storage resources have been provisioned such that the VMware ESX host has access to it and is able to both read and write to the iSCSI LUN. The VMware ESX host needs to have the iSCSI software initiator enabled and the IP address for the storage target configured. This can be confirmed following the steps below:

**Step 1: Confirm iSCSI software initiator has been configured on the VMware ESX**

1. The best way to confirm if this has been done is to select the VMware ESX from the inventory list and under the configuration tab select the storage adaptors option.



2. The information about the existing iSCSI targets is shown in detail.
3. To view more details about the specific settings for these iSCSI connections select the properties option (top right) and the following screen will show those details.

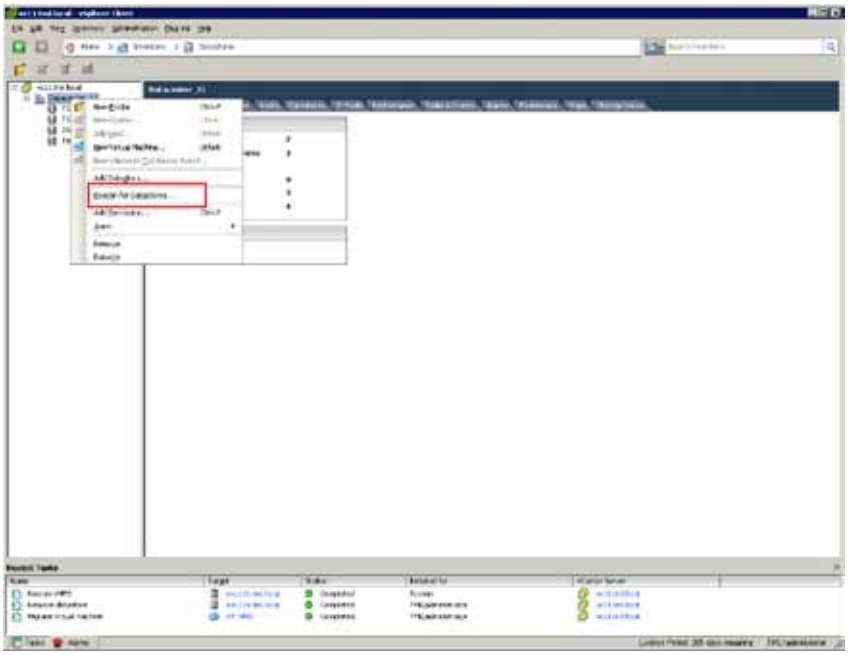


If this has not been enabled, please refer to the Basic System Administration Guide for the detailed steps to enable the iSCSI initiator in vSphere.

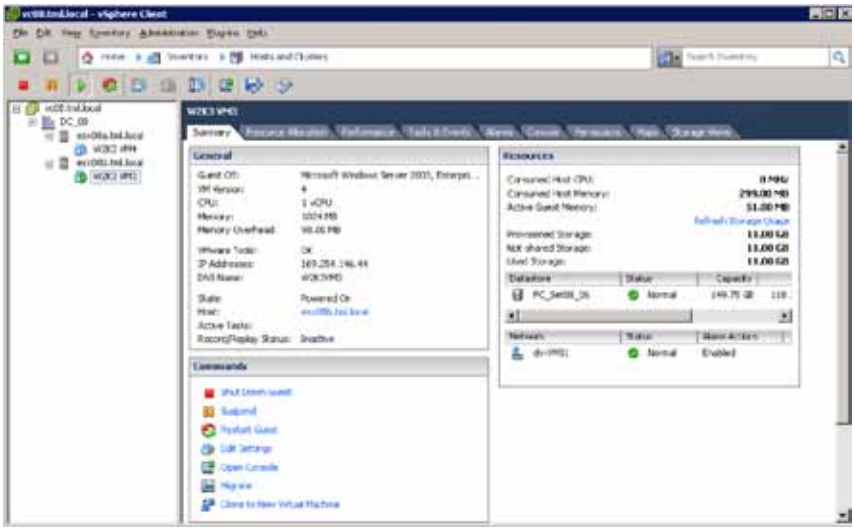
**Step 2: Create a new iSCSI Datastore**

In this section, you will use the new datastore view to create a datastore on an unused iSCSI LUN.

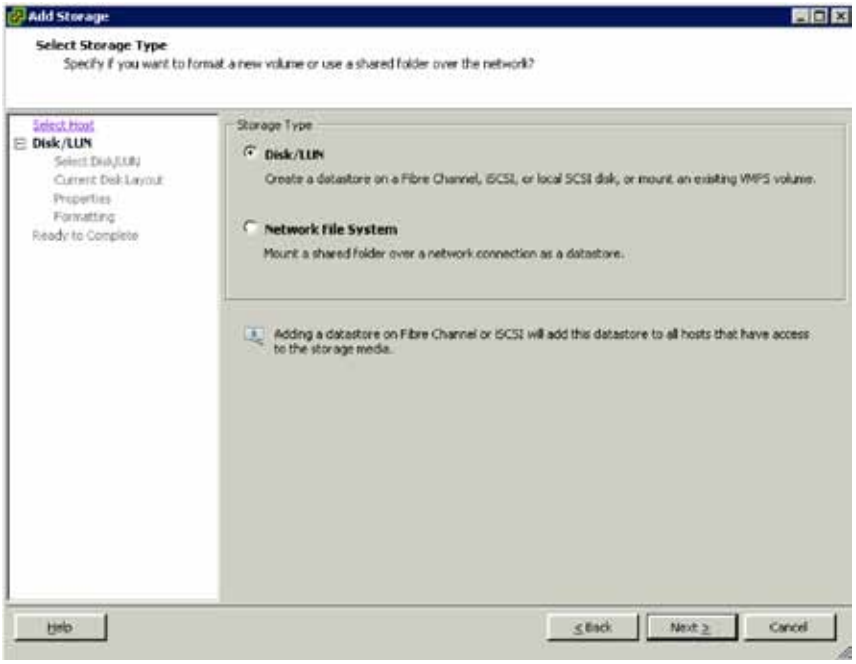
1. Log into vCenter, go to the datastore inventory, and highlight the datacenter.
2. Right-click mouse and select "Add Datastore".



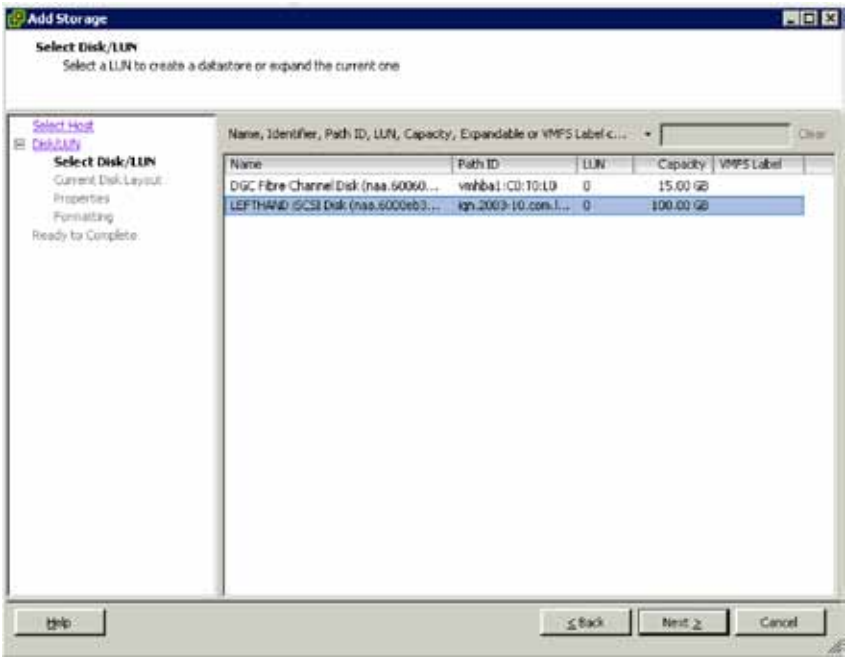
3. Select VMware ESX host to associate with this new datastore. Click **Next**.



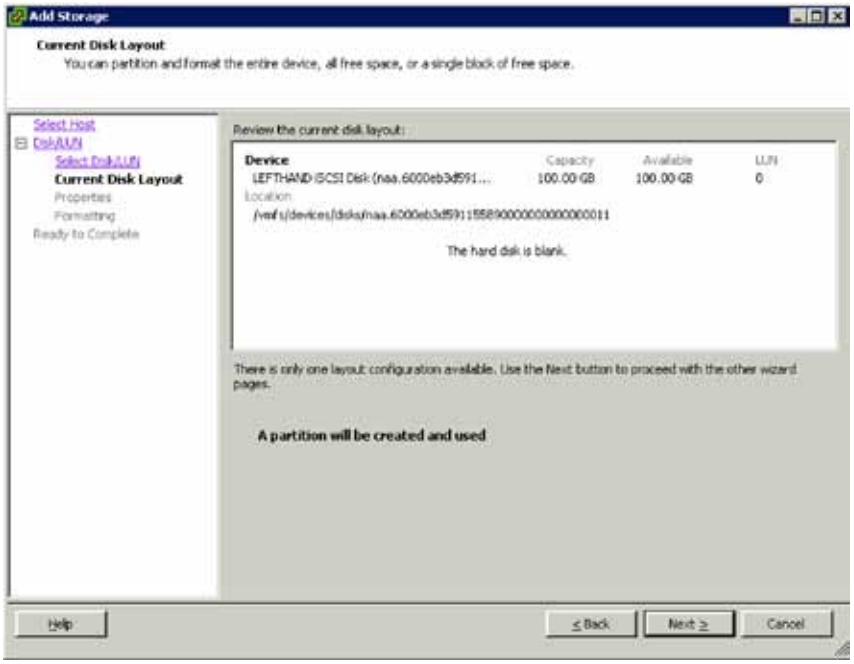
4. Select Disk/LUN. Click **Next**.



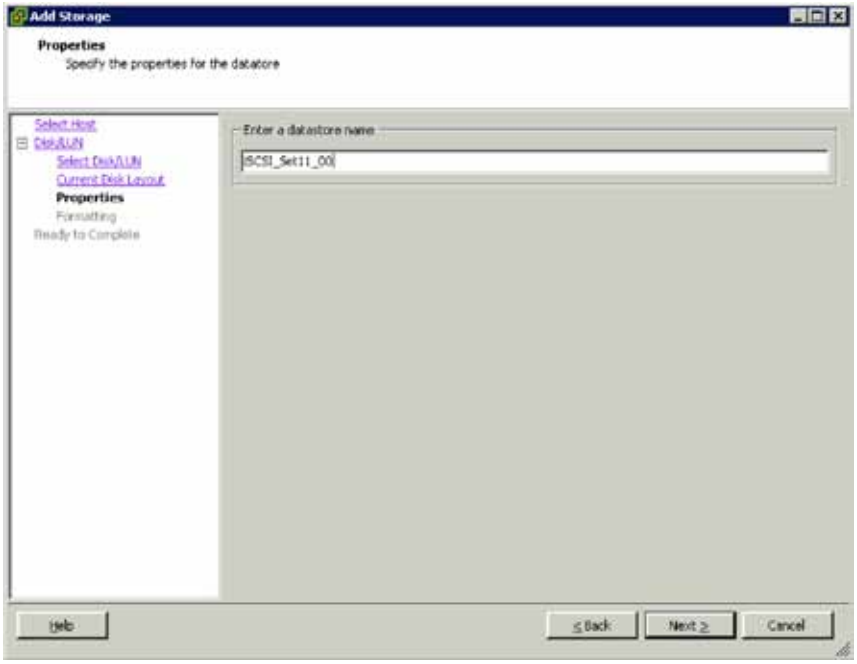

5. Select the iSCSI LUN from the dropdown list. Click **Next**.



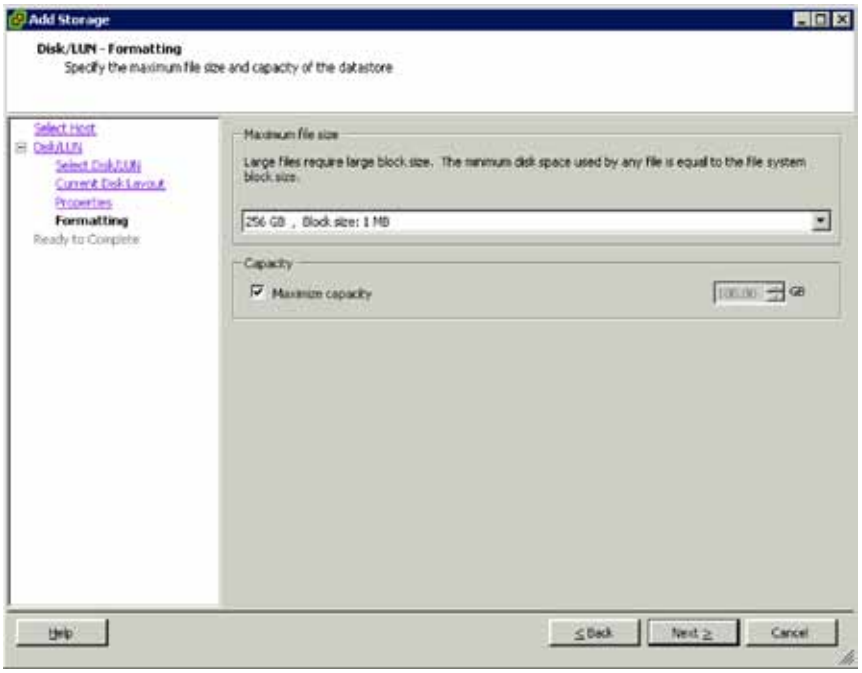
6. Review the information about this LUN and click **Next** once you have confirmed that the proper iSCSI LUN has been selected.



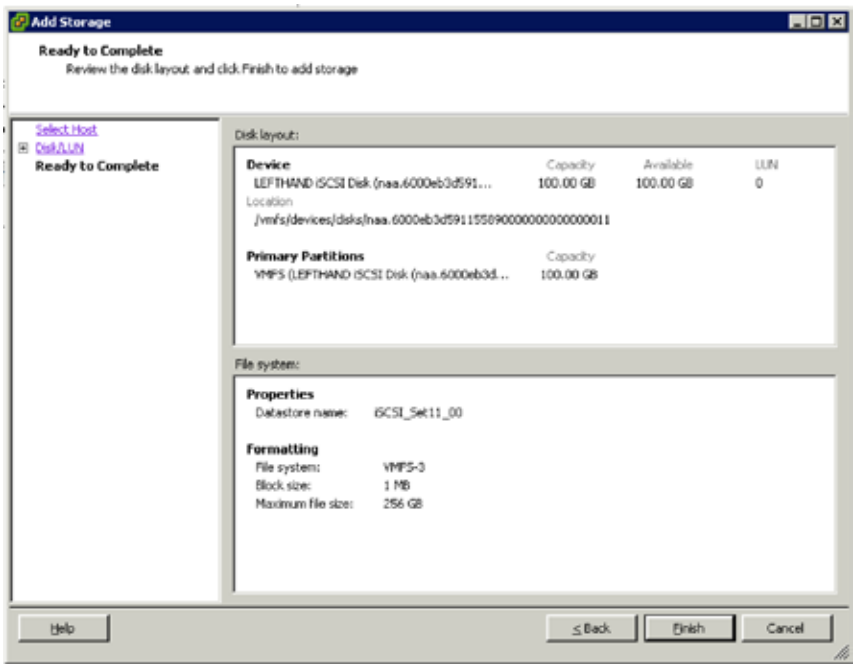

7. Enter a name for the new iSCSI datastore and click **Next**.



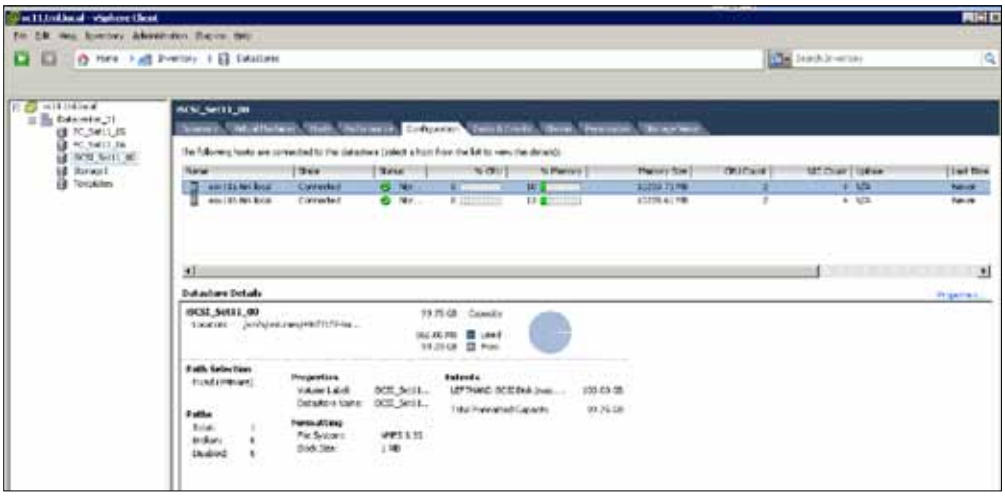
8. Select the default block size and click **Next**.




9. Review your choices and click **Finish** to complete the process.



10. Selecting the "Configuration" tab will show details about the new iSCSI datastore that you have just created.



## 1.3. ESX Host Cluster

**What It Is:** A cluster is a collection of VMware ESX hosts with shared resources and a shared management interface. When you add a host to a cluster, the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts.

**Use Case:** Enabling vSphere Clustering Features.

Create a cluster of ESX hosts to enable vSphere features such as VMware High Availability, VMware Fault Tolerance, VMware Distributed Resource Scheduler, and VMware Distributed Power Management. These features will provide high availability and better resource management for your virtual machines.

| | | | |
|---|---|---|---|
| Infrastructure Setup | ESX Host Cluster Setup | 1.3 Create a new cluster of ESX hosts<br><br>1. Create a new cluster<br>2. Add ESX hosts to the cluster | 10 minutes |

**Step 1: Create a New Cluster**

1. Right-click the datacenter called Datacenter_05 and select "New Cluster". You should see the window in Figure 1.3.a.
2. Type in a name for the cluster such as Cluster_01. Do not check any other boxes in this window, as you will do that later in the VMware High Availability and VMware Distributed Resource Scheduler sections.
3. Click **Next** until you arrive at the Ready to Complete window.
4. Click **Finish** to begin the creation of a new cluster.

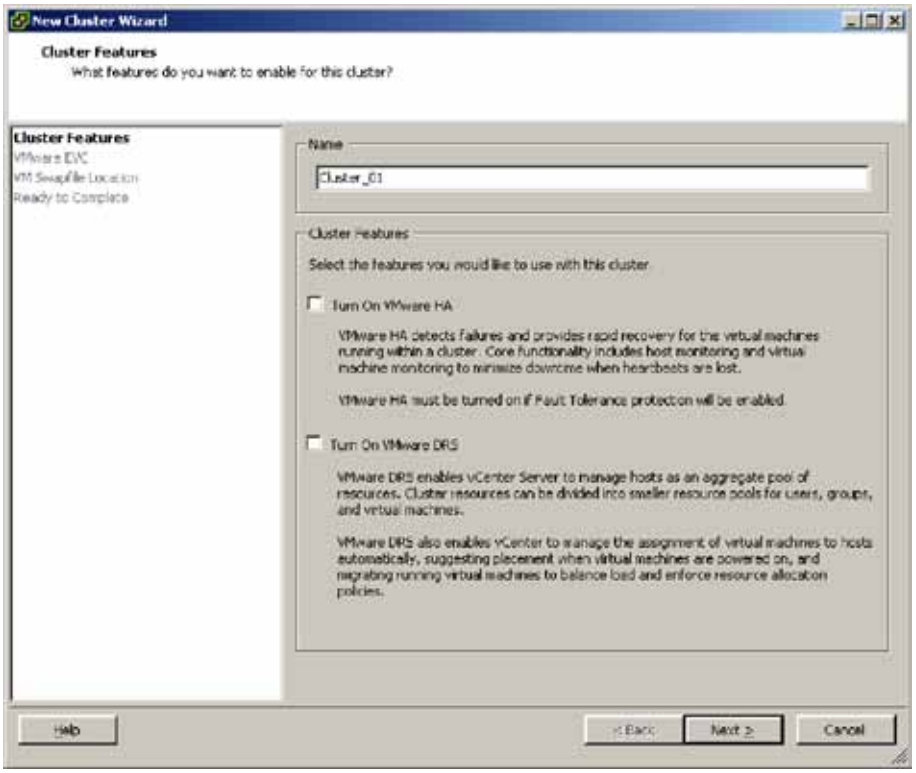



**Figure 1.3 a.** Create a cluster of ESX hosts

**Step 2: Add ESX Hosts to the Cluster**

After the cluster is created, you will need to add ESX hosts to it.

1. Drag and drop your ESX hosts into the cluster from the left pane. The resulting hierarchy will look like the window in Figure 1.3 b.

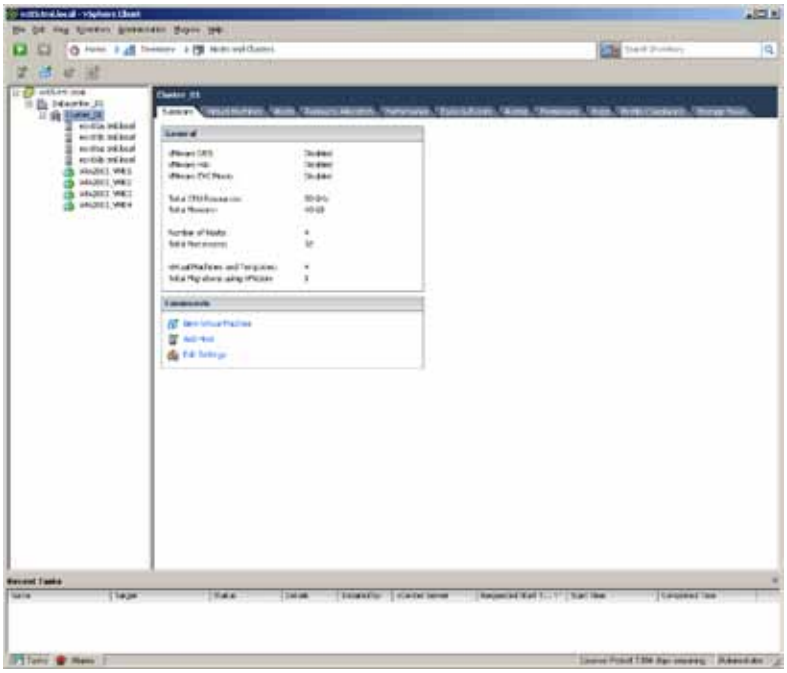


**Figure 1.3 b.** View of cluster after ESX hosts have been added

## 1.4. High Availability (HA)

**What It Is:** VMware High Availability (HA) utilizes heartbeats between ESX hosts and virtual machines in the cluster to check that they are functioning. When a host or virtual machine failure is detected, VMware HA automatically restarts affected virtual machines on other production servers, ensuring rapid recovery from failures. Once VMware HA is configured, it operates without dependencies on operating systems, applications, or physical hardware.

**Use Case:** Protect Virtual Machines from Server Failures and Guest OS Failures

When running Web servers or databases that are critical to your business, VMware HA ensures they will be restarted immediately upon failure of their servers. Interruption to your business will be minimized as the virtual machine is restarted on another available server in your HA cluster.

### 1.4.1. VMware Differentiators

VMware HA is the most scalable, flexible, cost-effective and simple to setup solution for high availability in virtual environments.

- **Most Scalable:** VMware HA is the most scalable high availability solution for virtual environments. A single VMware HA cluster can scale up to 32 nodes (vs. the 16 of Microsoft Windows Server 2008 Cluster Server 64-bit and Citrix XenServer).
- **Most Flexible:** VMware HA can be used to protect VMs running over 55 different Guest Operating Systems (vs. the 11 of Hyper-V R2 and the 21 of Citrix XenServer 5.5), giving users the greatest flexibility when it comes to operating systems.
- **Most Cost Effective:** VMware HA is fully integrated with Memory Overcommit and VMware DRS. Thanks to this tight integration, users can minimize the amount of spare hardware resources needed to guarantee that VMs will be restarted in the event of host failure. VMware HA is included even in low price packages such as VMware vSphere 4 Essentials Plus Edition.

  Microsoft and Citrix offerings lack such capabilities and integration requiring users to considerably overprovision hardware resources in order to guarantee the actual restart of VMs in case of host failure.
- **Easiest to Setup and Configure:** Configuring VMware HA clusters and enabling VMware HA protection on a VM is a very simple task that can be completed with a single tool (VMware vCenter) in just a few clicks. With vCenter HA, clusters can be created via Wizard, hosts added to a cluster by simple drag-and-drop and made VMware HA enabled with a single click

  Microsoft's offering requires separate tools to create highly available clusters (Microsoft Failover Cluster Manager) and to enable high availability on Hyper-V hosts (Microsoft Virtual Machine Manager). In addition, to allow highly available VMs share LUNs, users need to deploy Microsoft Cluster Shared Volumes, a hybrid cluster file system that greatly complicates storage administration.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **VMWARE HA** | | | |
| Max number of hosts per HA cluster | 32 | 16 | 16 |
| Automated continuous cluster resource checking for guaranteed restart | Yes | Yes | Yes |
| Restart a VM even when the total memory allocated to the VMs exceeds the physical memory of a destination host | Yes | No | No |
| Setup VM restart prioritization to minimize downtime of more critical VMs | Yes | Yes | Yes |
| Guest OS Failover Protection—Restart a VM in case of guest OS failure | Yes | Yes | No |
| Integration with Maintenance Mode—Automatically disable HA in case a server is placed in maintenance mode | Yes | Maintenance Mode requires SCVMM R2 | No |
| Smart failover—Restart VMs on the most appropriate host based on real time workload conditions | Yes | No | No |
| Single management console | Yes | Yes | Yes |
| Number of Guest OS supported | 55 | 11 | 21 |
| Enhanced host isolation response | Yes | No | No |

### 1.4.2. High Availability Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | High Availability | 1.4 VMware HA detects server failure and restarts virtual machines on another host<br><br>1. Turn on VMware HA on a cluster<br>2. Set Admission Control and Additional VMware HA options | 10 minutes |

**Step 1: Turn on VMware HA on a cluster**

VMware HA can only be turned on for a cluster of ESX hosts. Please ensure that you have followed the prior steps in creating a cluster of ESX hosts. Please also ensure that DNS is set up and working properly, including forward and reverse lookups, fully-qualified domain names (FQDN) and short names. Consult your network administrator for assistance in DNS configurations.

It is also recommended you set up an alternate isolation response address (best practice).

1. To enable VMware HA on your cluster, right-click the cluster and select **Edit Settings**. The cluster settings window should appear. Refer to Figure 1.4 a.
2. Under Cluster Features of the cluster settings window, select **Turn On VMware HA**. Each ESX host in the cluster will now be configured for VMware HA. Please note that you will need cluster administrator permissions to edit the cluster settings.

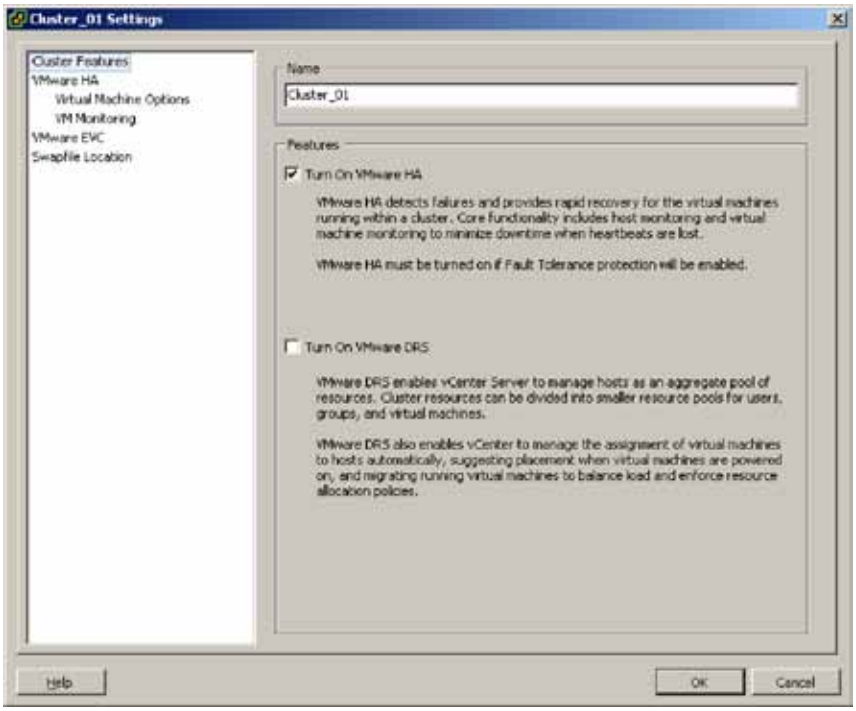



**Figure 1.4 a.** Turn on VMware HA for a cluster

### Step 2: Set Admission Control and Additional VMware HA options

You may want to set additional **VMware HA** options to allow for admission control, monitoring and setting policies for your hosts and virtual machines. These can be configured under **VMware HA** in the cluster settings window. The following is a listing of these addition features. Refer to Figure 1.4 b. as well.

- Disabling host monitoring will allow you to perform ESX host maintenance without triggering **VMware HA** into thinking the host has failed.
- Admission control allows you to control whether virtual machines should be restarted after host failures depending on if resources are available elsewhere in the cluster. **VMware HA** uses one of three admission control policies: 1) tolerate some number of host failures, 2) specify a percentage of cluster resources or, 3) specify a designated failover host.
- VM monitoring restarts virtual machines after their VMware Tools heartbeat is lost, even if their host has not failed. The monitoring sensitivity level can be set for each virtual machine.

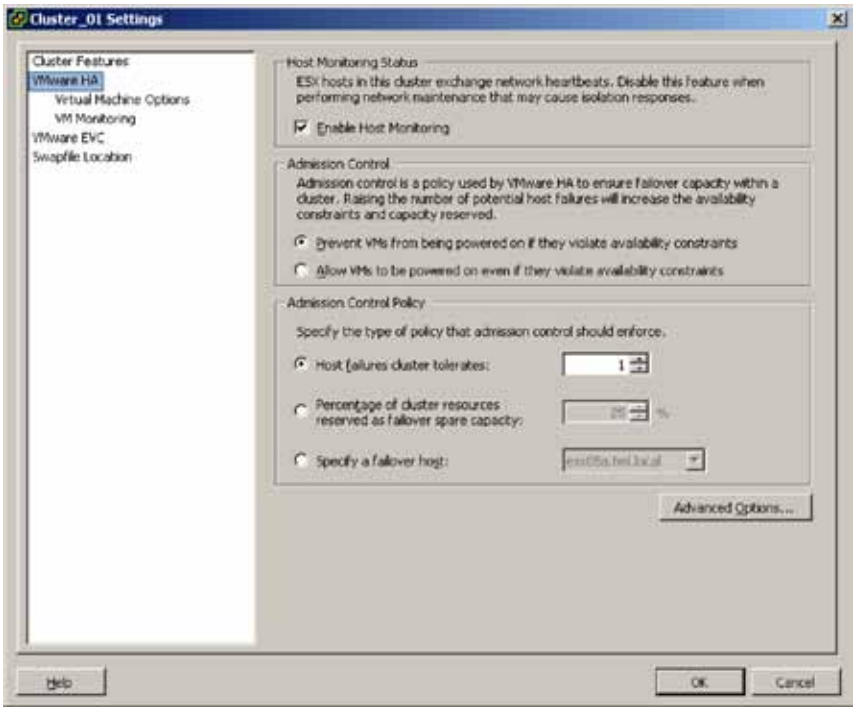



**Figure 1.4 b.** Additional VMware HA settings

## 1.5. VMotion

**What It Is:** VMware vCenter Server allows the migration of running virtual machines from one ESX host to another using VMware VMotion, assuming the source ESX host is VMotion compatible with the destination ESX host. Please see http://kb.vmware.com/kb/1991 for Intel-based ESX hosts or http://kb.vmware.com/kb/1992 for AMD-based ESX hosts. The workload in the virtual machine experiences no interruption of service and no data loss (including TCP/IP packets) during the migration using VMware VMotion.

**Use Case:** Maintain a Balanced Load across Hosts.

VMware VMotion gives users the flexibility to change the placement of their running virtual machines onto different ESX hosts. This may be for load balancing purposes or even for maintenance purposes. A user could migrate all running virtual machines off of an ESX host they wish to shutdown and perform maintenance on.

When the host comes back online the virtual machines could then be migrated using VMotion back onto the newly available host.

### 1.5.1. VMware Differentiators

VMware VMotion is the most trusted, proven and powerful live migration solution for virtual environments.

- **Most mature:** VMware VMotion was the first live migration solution introduced in the market in 2003. It is used in production environments by more than 70% of VMware customers which makes it the most proven and trusted solution.
- **Greatest value:** VMware VMotion is fully integrated with other unique VMware technologies such as Memory Overcommit, Maintenance Mode, Distributed Resource Scheduler, Distributed Power Management, Distributed Networking and vShield Zones, which allows users to benefit from live migration to solve the broadest set of use cases.

  Microsoft and Citrix offer less mature live migration solutions which can be used to respond only to the most basic use cases, such as manual migration of VMs between two hosts. Live migration is an enabler and as such it provides value when it works in conjunction with other platform capabilities, which both Microsoft and Citrix offerings lack

  In addition, Microsoft Hyper-V Live Migration requires Cluster Shared Volumes (CSV), Microsoft 's hybrid cluster file system. CSV adds substantial administration complexity and does not allow for simultaneous live migrations for clusters of less than 4 nodes.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **LIVE MIGRATION** | | | |
| Integration with Memory Over Commitment—Allow VM live migration to a host even when total virtual memory exceeds physical host memory | Yes | No | No |
| Customizable CPU Compatibility Settings—Allows live migration across different generation of CPUs from the same vendor | Yes | Yes | No |
| Supports FC SAN, NAS, iSCSI | Yes | Limited (no NAS support) | Yes |
| Migration Wizard—Identifies the best destination for a virtual machine using real-time information provided by the migration wizard. | Yes | No (requires SCVMM) | Yes |
| Priority Levels—Assign a priority to each live migration operation to ensure that the most important virtual machines always have access to the resources they need. | Yes | No | No |
| Scheduled Migration Tasks—Automate migrations to happen at pre-defined times and without an administrator's presence | Yes | Limited (requires scripting) | No |
| Migration Audit Trails—Maintain a detailed record of migration operations, including date/time and the administrators responsible for initiating them | Yes | Yes | No |
| Maintain secure network connections during migration events | vShield Zones | No | No |
| Enable networking statistics and policies to migrate with VMs | vNetwork Distributed Switch | No | No |

### 1.5.2. VMotion Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | VMotion | 1.5 Allows the migration of running virtual machines from one ESX host to another.<br><br>1. Migrate a running virtual machine from one host to another host | 10 minutes |

**Step 1: Migrate a Running Virtual Machine from One Host to Another Host**

In order to use VMotion to migrate a virtual machine from one ESX host to another, perform the following:

1. Right-click the virtual machine you wish to migrate such as Win2003_VM01. This opens the Migrate Virtual Machine window.
2. Select Change host under **Select Migration Type** and click **Next**. Please note that selecting **Change datastore** invokes Storage VMotion, which will be covered in subsequent sections.

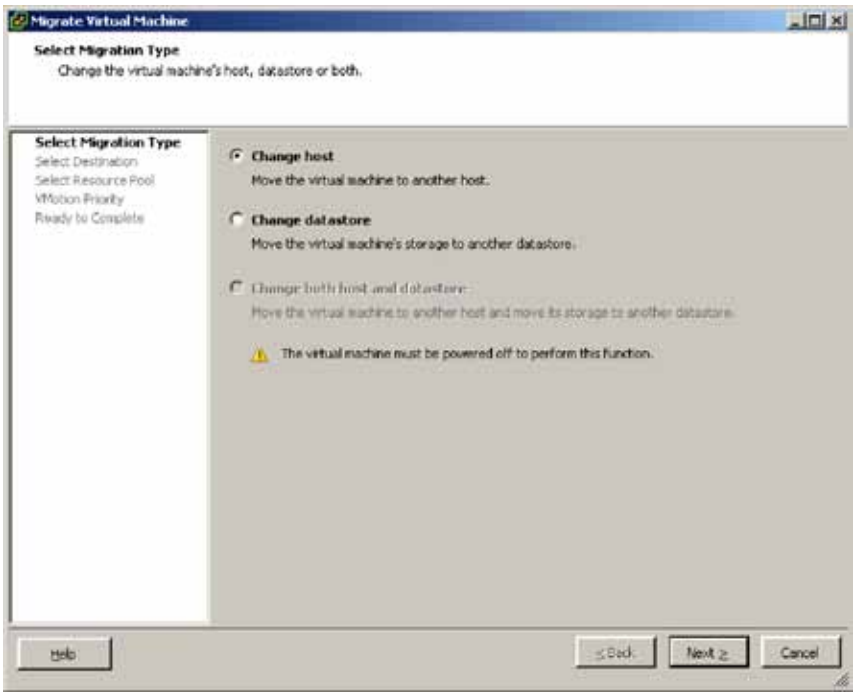



**Figure 1.5 a.** Select the Migration Type

3. Under **Selection Destination**, expand Cluster_01 and select a destination host such as "esx06a.tml.local." Click **Next**.

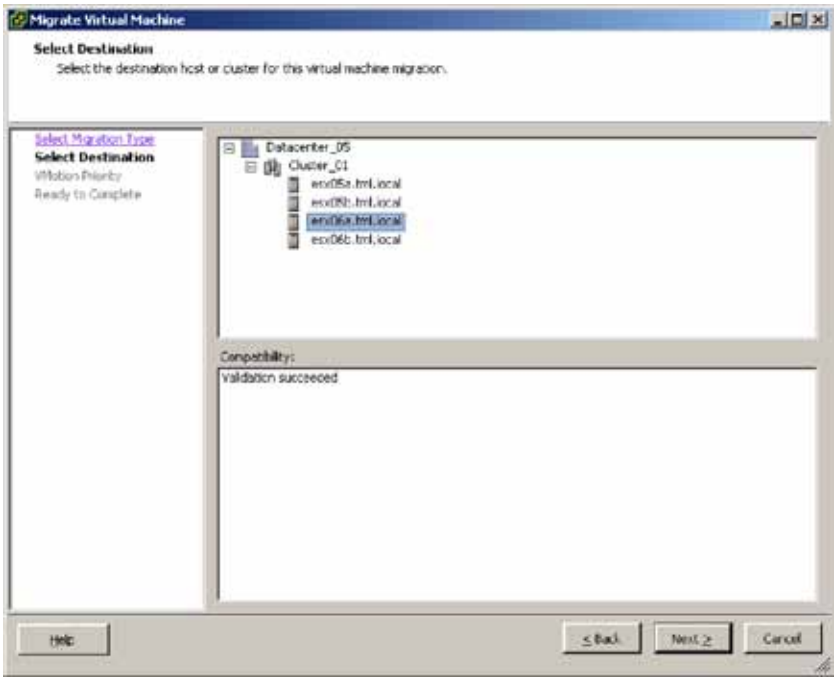



**Figure 1.5 b.** Select a Destination Host

4. Under **VMotion Priority**, select **Reserve CPU for optimal VMotion performance (Recommended)** to reserve resources on both source and destination to ensure that the VMotion migration process completes as fast as possible. If resources are not available, then VMotion migration will not proceed. Click **Next**. Selecting **Perform with available CPU resources** will always allow VMotion migration to proceed whether there are or are not resources available.

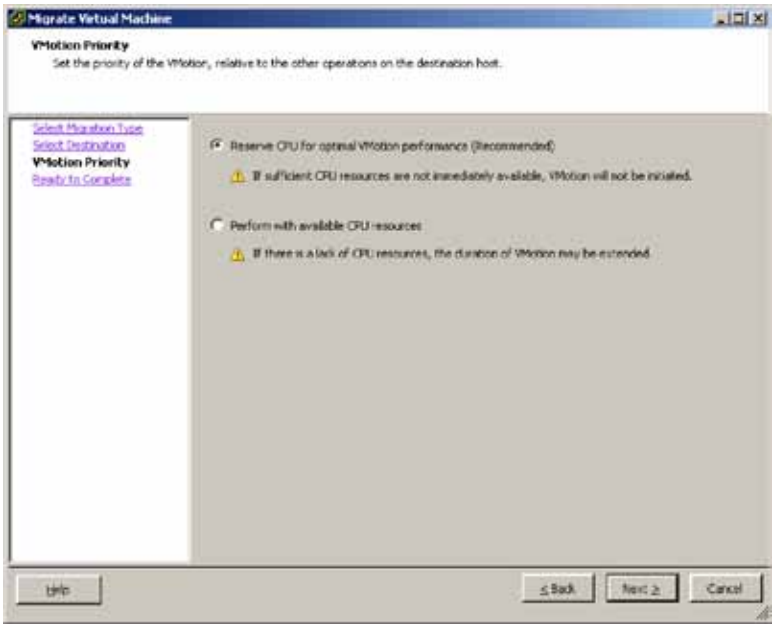



**Figure 1.5 c.** Select the VMotion Priority

5. Review the Summary under **Ready to Complete** and click **Finish** to initiate the VMotion migration.

After the VMotion operation, you will notice that Win2003_VM01 is now running on esx06a.tml.local. You can see this either under the Summary tab for the virtual machine or the **Maps** tab for the cluster.

# Section 2: Features for Small-to Medium-Scale Deployments

## 2.1. Fibre Channel Storage

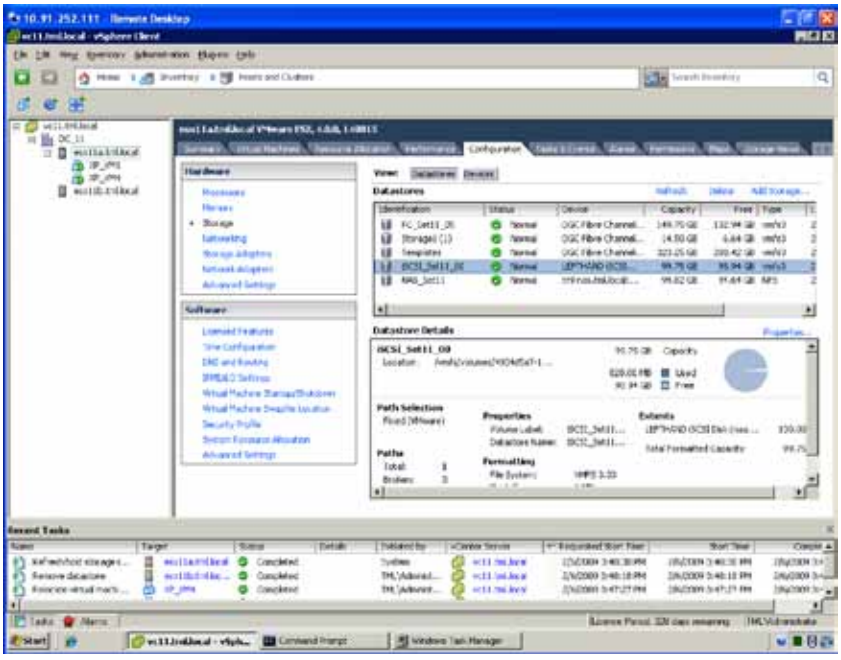
**Use Case:** Create a Fibre Channel datastore to house Virtual Machines

This next section will use an existing datastore, on a VMFS volume, to house the virtual machines. In addition, you will create a new datastore on an unused LUN. This new datastore will be used in a Storage VMotion exercise and will serve as the target datastore to which the VM will be migrated. As you will also be using this same datastore to exercise the VMFS Volume Grow feature in a later section, you will provision a datastore on the LUN that is smaller than the available storage of that LUN. You will build a VMFS volume that is only 10GB in size although the LUN upon which it resides is much larger. Follow the steps below:

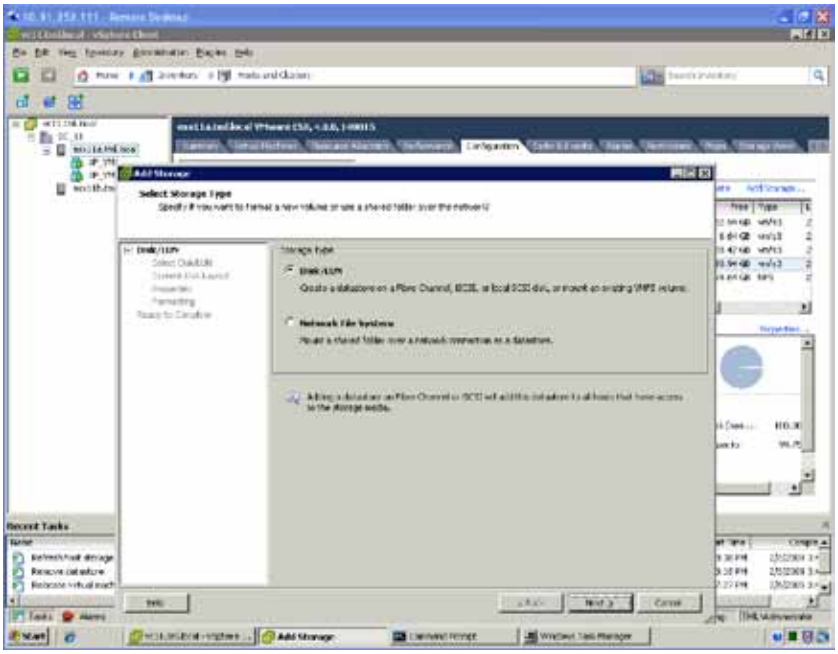
| | | | |
|---|---|---|---|
| Infrastructure Setup | Fibre Channel Storage Configuration | 2.1 Create a FC datastore<br><br>1. Creating a new VMFS volume/datastore | 10 minutes |

**Step 1: Creating a new VMFS Volume/Datastore**

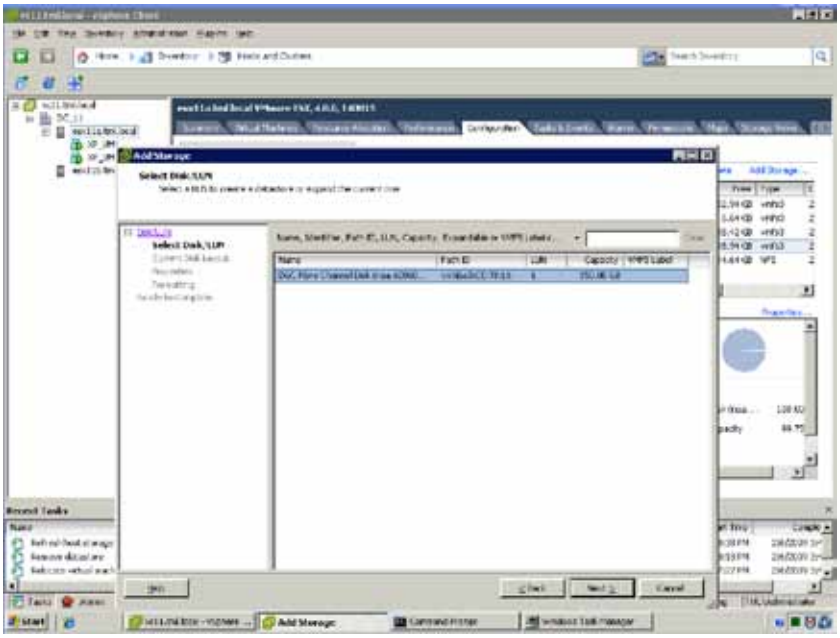
1. Log into vCenter. Highlight one VMware ESX host and then select the configuration tab for that host in the right section of the view.
2. Select "Storage" in the Hardware navigation panel to reveal the datastores known to this VMware ESX host.



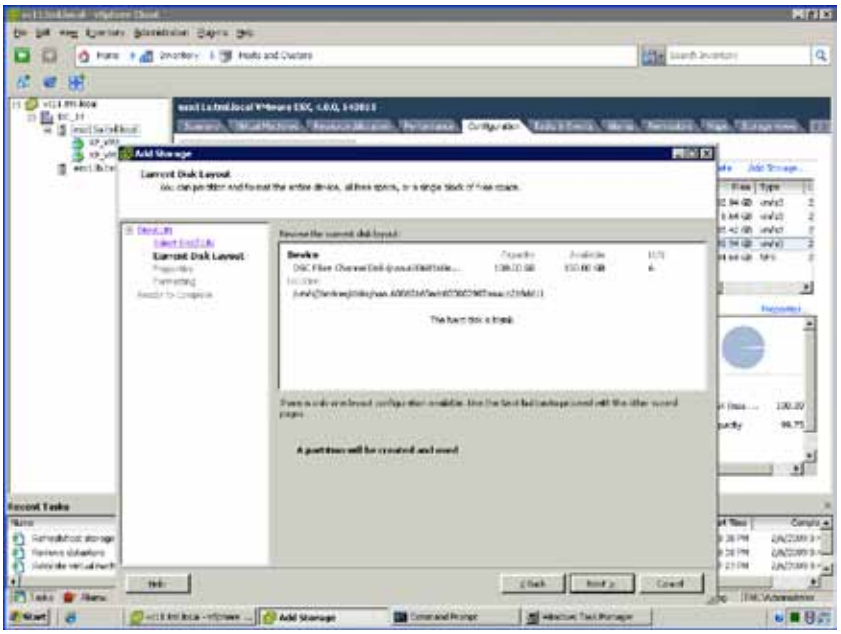
3. Create a new datastore by selecting the **Add Storage** option.
4. Select **Disk/LUN**. Click **Next**.



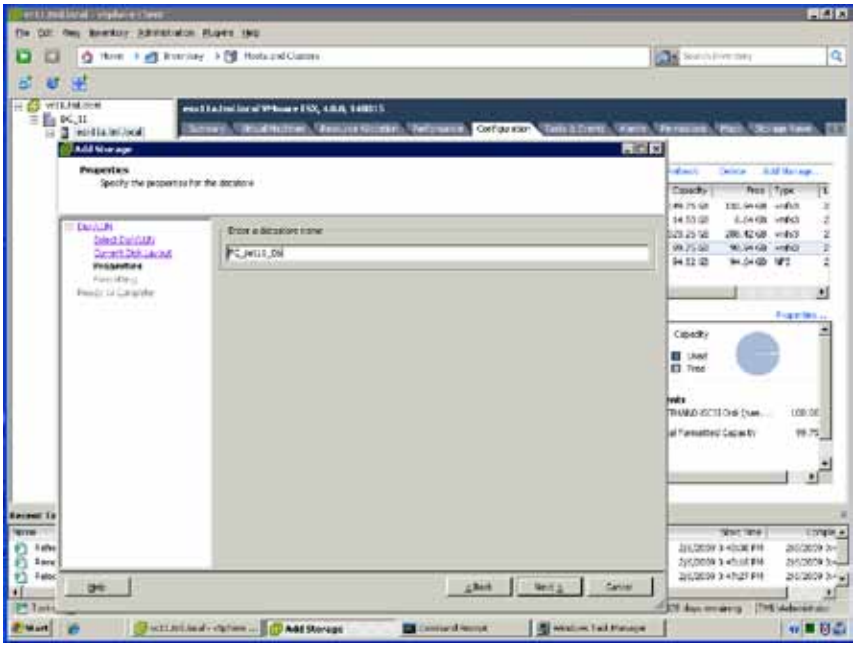
5. Select a free LUN from the dropdown list. Click **Next**.



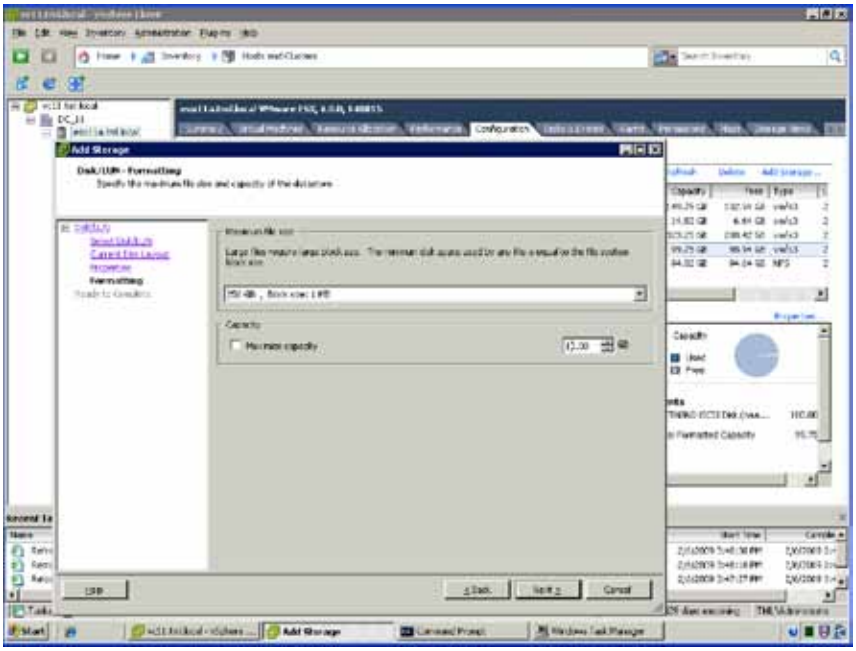
6. Review the information about this LUN you have selected and click **Next** once you have confirmed that the proper LUN has been selected.



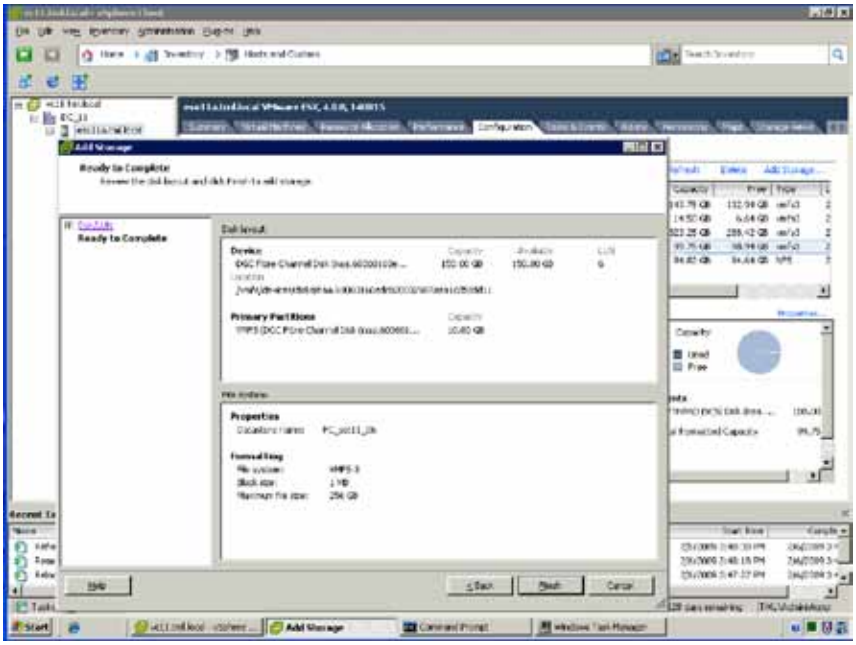
7. Enter a name for the new datastore and click **Next**.



8. Select the default block size and uncheck the box for use Maximum Capacity and enter 10GB. This is done so that you can grow the size of this VMFS Volume later. Click **Next**.



9. Review your choices and click **Finish** to complete the process.



You have now created a new datastore that is 10GB in size but resides on an FC LUN that is much larger (150GB). Although this is not generally considered best practice to have a datastore that is smaller than the LUN on which it resides, you are doing this to prepare for a Volume Grow in the later section. As many arrays enable a dynamic expansion of the LUNs presented to a server, the creation of a small datastore on a large LUN sets up the ability to grow the datastore without having to first dynamically expand the LUN first.

## 2.2. Host Profiles

**What It Is:** Host Profiles creates a profile that encapsulates the host configuration and helps to manage the host configuration, especially in environments where an administrator manages more than one host in vCenter Server. Host profiles eliminates per-host, manual, or UI-based host configuration and maintains configuration consistency and correctness across the datacenter. Host profile policies capture the blueprint of a known, validated reference host configuration and use this to configure networking, storage, security, and other settings on multiple hosts or clusters. You can then check a host against a profile's configuration for any deviations.

**Use Case:** Use Host Profiles to Automate Host Provisioning and Configuration

### 2.2.1. VMware Differentiators

VMware Host Profiles is a unique VMware capability. It is the simplest and most automated solution to manage and host setup and maintain configuration compliance.

- **Easiest to use:** VMware Host Profiles is a new built-in feature of VMware vCenter that does not require the installation of any additional products. Users can access Host Profiles directly from the vCenter Console and create a baseline "gold image" configuration profile by either simply importing settings from a file or exporting them from existing hosts. By enabling automated configuration compliance checking and remediation, VMware Host Profiles makes it very efficient to perform configuration management of large numbers of hosts. Users can monitor configuration compliance and remediate out of compliance host setups with just a few clicks.

  Neither Microsoft Virtual Machine Manager (SCVMM) nor Citrix XenCenter provides host configuration capabilities out of the box. Microsoft users must deploy System Center Configuration Manager (SCCM), a separate non-integrated product, to obtain configuration management capabilities for physical servers. SCCM—a very complex product to install and setup—requires extensive configuration, scripting and customization to provide the same functions as Host Profiles.

  With Resource Pools, Citrix XenCenter only provides the ability to share cluster level settings (such as VLANs) among groups of hosts. Citrix Resource Pools (not be confused with vSphere Resource Pools that enable true abstraction and aggregation of CPU and memory resources) do not provide host level configuration monitoring and remediation.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **HOST CONFIGURATION MANAGEMENT** | | | |
| Profile Creation—Wizard-based creation of "gold image" profile by exporting settings of existing hosts or by importing from a file | Yes | No | No |
| Profile Editing—Enables users to define profile settings both by pre-set value and by policy/rule | Yes | No | No |
| Profile Settings—Controls at least the following settings: Memory Reservation, Storage, Networking, Date and Time, Firewall, Security, Services, Users and User Groups Security | Yes | No | No |
| Compliance Checking—Enables automated scanning to determine configuration compliance of a host to the associated profile | Yes | No | No |
| Out-of-compliance Remediation—Enables automated remediation of out of compliance host configurations | Yes | No | No |

### 2.2.2. Host Profiles Hands-on Review

| | | | |
|---|---|---|---|
| Infrastructure Setup | Host Profiles | 2.2 Use host profiles to automate host provisioning and configuration:<br><br>1. Add two new hosts and reconfigure their DNS and NTP settings<br>2. Create a host profile from a reference host<br>3. Attach host profile and check for host compliance<br>4. Apply host profile and re-check for host compliance | 30 minutes |

In this exercise, you will be adding two new hosts to the vCenter inventory and applying a host profile to bring the newly added hosts to the desired host configuration. You will then run a compliance check to ensure that the hosts are correctly configured.

**Step 1: Add two new hosts and reconfigure their DNS and NTP settings**

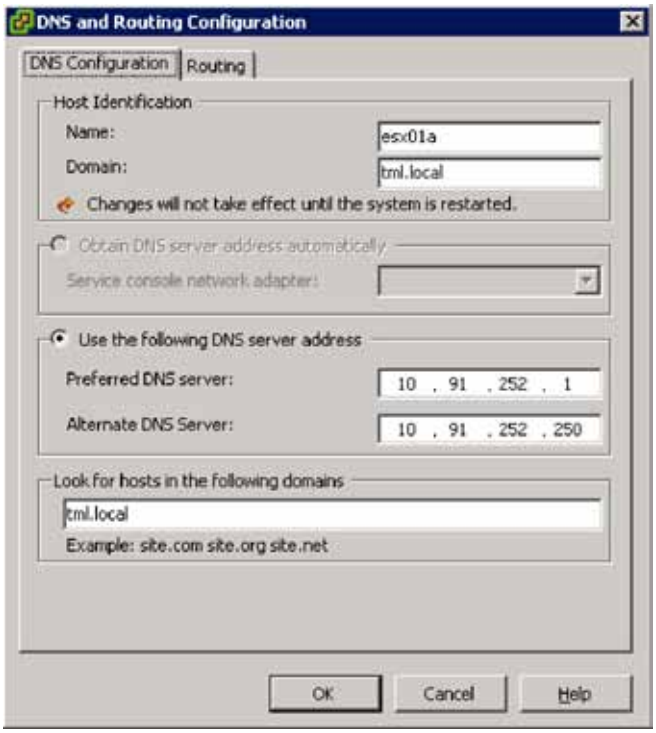
In this step, you will add two VMware ESX hosts, and simulate a misconfiguration by modifying a few configuration settings, specifically the Network Time Protocol (NTP) and the Domain Name System (DNS) server names.

1. Add two new hosts, "esx01a.tml.local" (VMware ESX) and "esx01b.tml.local" (VMware VMware ESXi), to the vCenter Server inventory.
2. Using the vSphere client, reconfigure DNS and NTP settings on "esx01a.tml.local" and "esx01b.tml.local" using invalid IP addresses.

a. Select the host from the inventory panel. Click the **Configuration** tab.

b. Select Time **Configuration** > **Properties** > **Options** > **NTP Settings**. Add an invalid IP address under NTP Servers, or remove all NTP Servers that may currently be associated with this host. Click **OK**.

c. Click **DNS and Routing**, and click **Properties**. Under the DNS Configuration tab, modify the DNS server address for the Alternate DNS Server (e.g., change from "10.91.252.2" to "10.91.252.250"). Click **OK**.

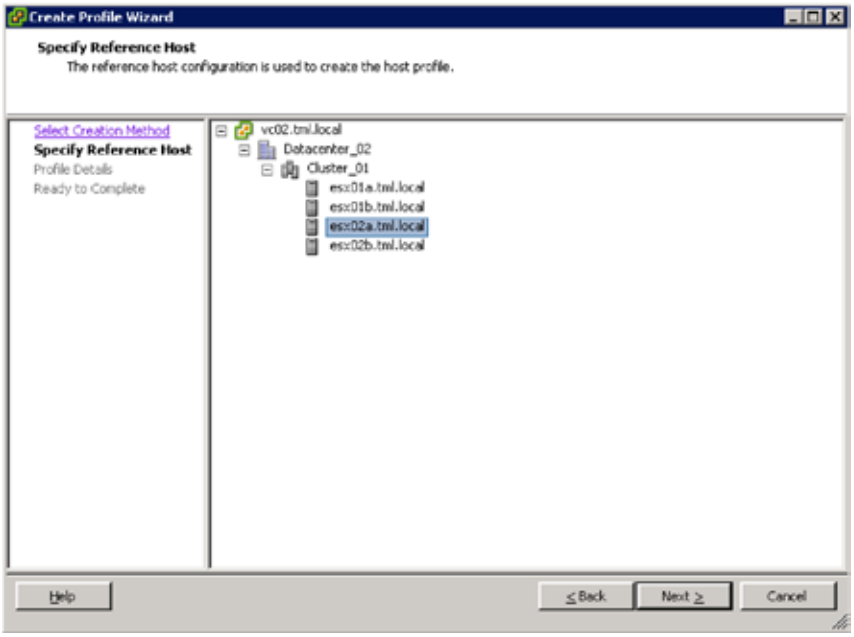



**Step 2: Create a host profile from a reference host**

There are two ways to create a host profile. Using the Create Profile Wizard, you can create a new profile from an existing host, or you can import an existing profile. In this step, you will create a new host profile based upon an existing host configuration.

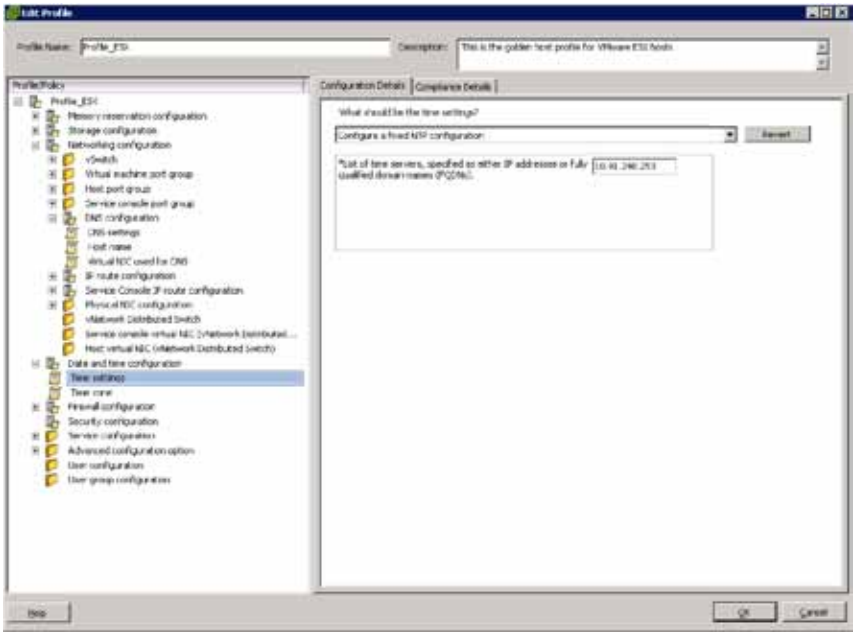
1. Access the Host Profiles main page by selecting **View** > **Management** > **Host Profiles**.
2. On the Host Profiles main page, click the Create Profile icon to start the **Create Profile** Wizard.

3. Select **Create profile** from existing host to create a new profile. Click **Next**.
4. Select "esx02a.tml.local" (VMware ESX) as the reference host. This host's configuration is used to create the profile. Click **Next**.




5. Type the name and enter a description for the new profile. Click **Next**. The name "Profile_ESX" with description "This is the golden host profile for VMware ESX hosts" will be used.
6. Review the summary information for the new profile and click **Finish** to complete creating the profile. The new profile appears in the profile list.

7. To view the host configuration parameters and host profile policies that are captured by a host profile, click **Edit Profile**. Each host profile is composed of several sub-profiles that are designated by functional group to represent configuration instances, such as vSwitch and Virtual Machine Port Group. Each sub-profile contains many policies that describe the configuration that is relevant to the profile. On the left side of the Profile Editor, expand a sub-profile until you reach the policy you want to view. In particular, take note of the DNS and NTP settings that were captured from the reference host. Click **Cancel** when you are finished viewing the settings.



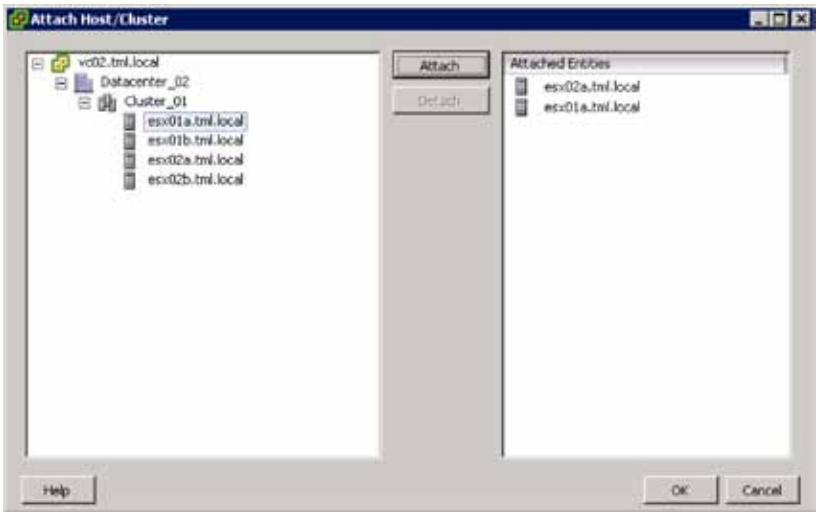
8. Repeat the above steps to create a VMware VMware ESXi host profile called "Profile_ESXi", using "esx02b.tml.local" as the reference host. You should end up with two host profiles, one for VMware ESX and one for VMware VMware ESXi.

**Step 3: Attach host profile and check for host compliance**

In this step, you will attach the hosts to their respective host profiles. Attaching the host profile allows you to monitor for configuration compliance.

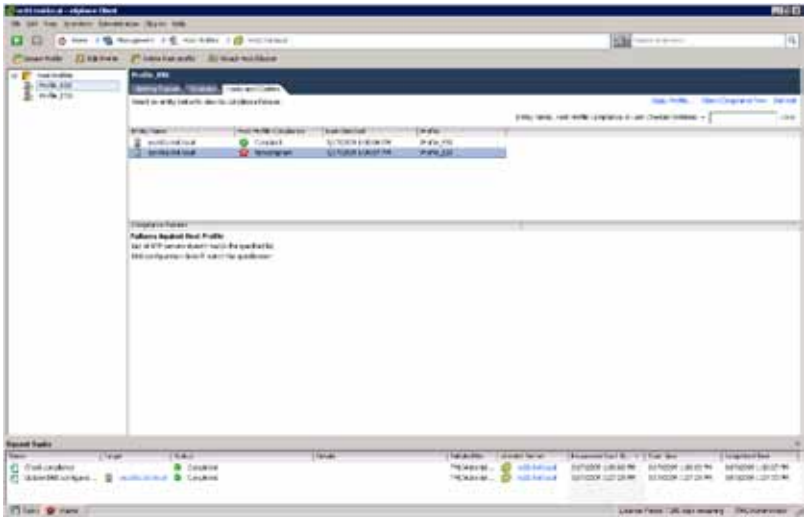
1. Attach "esx01a.tml.local" and "esx02a.tml.local" to Profile_ESX and check compliance.
   a. In the Host Profiles main view, select the Profile_ESX profile.
   b. Select **Attach Host/Cluster**

c. Select "esx01a.tml.local" on the left pane, click **Attach**. Repeat with "esx02a.tml.local". Click **OK**.




d. Click the **Hosts and Clusters** tab within the Host Profiles main page. This tab lists the entities that are attached to this profile.

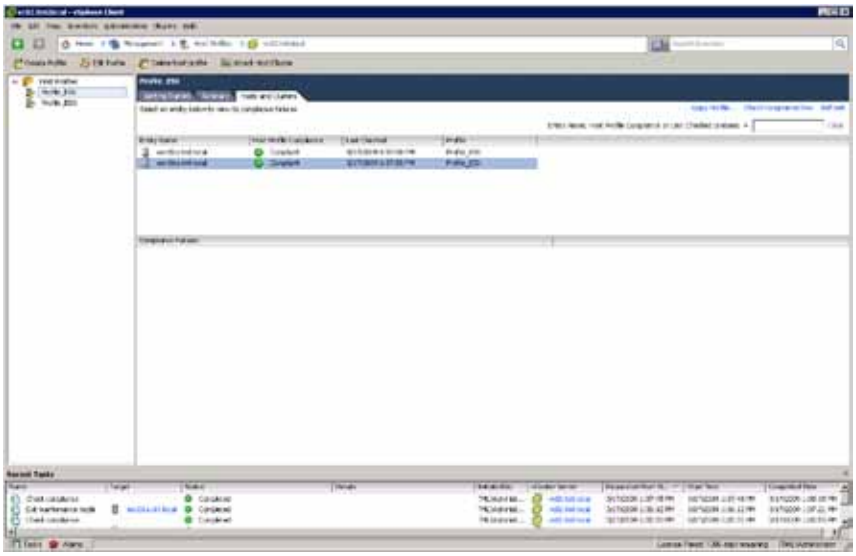
2. Repeat the previous step to attach "esx01b.tml.local" and "esx02b.tml.local" to Profile_ESXi.
3. Click **Profile_ESX** and click on **Check Compliance Now**. The reference host "esx02a.tml.local" should show up as Compliant, while the newly added host "esx01a.tml.local" should show up as Noncompliant. Under Compliance Failures, it's been reported that the list of NTP servers and the DNS configuration on "esx01a.tml.local" does not match those specified in the host profile.
4. Repeat the previous step to check compliance on Profile_ESXi.



**Step 4: Apply host profile and re-check for host compliance**

In this step, you will apply the host profile to the newly added hosts. This will configure the hosts based on the configuration policies specified by the host profile. Once you've applied the profile, the newly added host will have the same host configuration settings as the reference host. Note that the host must be in maintenance mode before the profile can be applied.

1. Right-click the noncompliant host "esx01a.tml.local" and click **Enter Maintenance Mode**.
2. Once in maintenance mode, right-click the noncompliant host "esx01a.tml.local" and click **Apply Profile**. The wizard will show you the specific configuration changes that will be applied on the host. Click **Finish**.
3. Bring host "esx01a.tml.local" out of maintenance mode.
4. Click **Check Compliance Now**. All hosts should now show up as Compliant.
5. (Optional) Use the vSphere Client user interface to verify that Host Profiles has reconfigured the DNS and NTP settings to match the settings of the reference host.



## 2.3. Distributed Resource Scheduler

**What It Is:** VMware Distributed Resource Scheduler (DRS) automatically load balances resource utilization across a cluster of ESX hosts by using VMotion to migrate virtual machines from a heavily utilized ESX host to a more lightly used ESX host. VMware DRS analyzes the CPU and memory consumption of a virtual machine over time to determine whether to migrate it.

**Use Case:** Redistribute Virtual Machines off of an ESX Host during Maintenance

VMware DRS migrates virtual machines off of an ESX host when a user enters that host into maintenance mode. DRS will intelligently migrate virtual machines to other available hosts in the DRS cluster in a load-balanced manner. After the maintenance on that host is completed and the user takes it out of maintenance mode, DRS will then migrate virtual machines back onto the host.

### 2.3.1. VMware Differentiators

DRS is a unique feature of VMware vSphere. Only DRS enables true dynamic resource allocation of abstracted and aggregated compute resources. DRS clusters are effectively giant computers, also called "software mainframes", whose resources are dynamically shifted among applications by the intelligent DRS engine based on real time workload conditions.

- **VMware DRS can aggregate discrete physical resources (CPU, memory) in logical pools, maximizing infrastructure utilization.**

  VMware DRS clusters are more than simple groups of physical hosts; they are actual abstract aggregations of physical resources in logical pools. When changes to the infrastructure happen, for example a new host is added to a DRS cluster, its physical components (memory, CPU power, etc.) become part of the existing pool transparently to the end-user.

  Neither Microsoft Hyper-V nor Citrix XenServer have anything similar to VMware DRS because they lack the concept of true resource pools. To enable workload balancing with Microsoft Hyper-V, users must leverage Microsoft PRO Tips, which in turn require System Center Operations Manager, an additional product loosely-integrated with System Center Virtual Machine Manager. With Microsoft PRO Tips, resources are monitored at the host level without coordination among nodes in the cluster, because PRO Tips lacks abstraction and aggregation capabilities.

- **With VMware DRS, users can align IT resources to business logic and SLAs.**

  VMware DRS makes it easy for IT managers to define policies that align IT resources with business logic. Users can configure how VMware DRS must prioritize applications that are competing for the same resource pool to deliver the appropriate service level agreements. When an application experiences increased load, VMware DRS first evaluates its priority against the established resource allocation rules and policies and, if justified, allocates additional resources. Neither Microsoft nor Citrix support a similar feature.

- **Only VMware DRS can automatically adjust resource allocations to running applications without affecting availability or causing downtime.**

  VMware DRS fully leverages the live migration capabilities of VMware VMotion technology, which allows DRS to redistribute virtual machines while applications are running—even in production—transparently to the end-user. In addition, administrators can configure VMware DRS to operate in fully automatic mode, which enables real-time dynamic resource optimization while dramatically increasing system administrator productivity.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **DYNAMIC RESOURCE ALLOCATION** | | | |
| Resource Pools—Aggregate resources across many servers into shared pools. Manage resources independently of the physical servers that contribute them. | Yes | No | No |
| Resource Pools Hierarchy—Organize resource pools hierarchically to match available IT resources to the business organization. Ensure that resource utilization is maximized while business units retain control and autonomy of their infrastructure. Resource pools can be flexibly added, removed, or reorganized as business needs or organization change. | Yes | No | No |
| Resource Pools Isolation—Maintain isolation between resource pools. Make allocation changes within a resource pool without impacting other unrelated resource pools. | Yes | No | No |
| Resource Allocation Policies—Allows users to define how resources are allocated among different pools in a cluster and among multiple virtual machines using a "Shares" system | Yes | No | No |
| Rules—Create rules that govern the allocation of virtual machines to physical servers. For example, certain virtual machines can always run on the same server for performance reasons. Alternatively, specified virtual machines can always run on different servers for increased availability. | Yes | No | No |
| Dynamic Resource Allocation—Continuously monitor workload conditions and dynamically responds to changing virtual machine requirements using live migration to move virtual machines non-disruptively between servers, automating operational management of virtual machine environments | Yes | Yes, with PRO Tips and SCOM 2007 | Limited, WLB in XenServer 5.5 cannot automate dynamic VM balancing |

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **DYNAMIC RESOURCE ALLOCATION** | | | |
| Integration with Memory Overcommitment—Allow VM live migration to a host even when total VM memory allocation exceeds the physical host memory. Performs what-if analyses on possible resource reallocations prior to execution to guarantee that final reallocation represents improvement over initial conditions | Yes | No | No |
| Operate in Manual or Automated Mode—Implement resource redistribution recommendations with various level of automation: Fully automated with ability to set migration from conservative to aggressive (virtual machines are automatically placed, recommendations are automatically implemented if above migration threshold), manual (recommendations are implemented only if user approves), semi-automated (virtual machines are automatically placed, recommendations are implemented only if user approves) | Yes | Manual and Automatic modes; Automatic limited to "Warning" and "Critical" choices | Manual only. Optimization recommendation can be accepted or rejected |
| Integration with Access Control and Delegation—Allow access control and delegation at the resource pool level. Virtual machine creation and maintenance for a business unit can be delegated to a business unit system administrator thus eliminating reliance on central IT for every routine operation. | Yes | Host group level only; all users are administrators | Integration with LDAP; All users are administrators |
| Management of Sets of Virtual Machines running distributed applications—Optimize the service level of distributed applications by controlling the aggregate allocation of resources for the entire set of virtual machines running the distributed application | Yes | No | No |

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **DYNAMIC RESOURCE ALLOCATION** | | | |
| Integration with Maintenance Mode and Update Management—When a physical server is placed in maintenance mode, automatically migrate all virtual machines to other physical servers, allowing server maintenance with zero downtime and optimizing reallocation of remaining resources | Yes | Yes, in R2 | Yes |
| Easily Add and Deploy New Capacity—Add new physical servers to a resource pool and automatically take advantage of the additional capacity by redistributing virtual machines among the servers | Yes | Yes, at cluster level only | Yes, at pool level only |
| Initial Placement—When a virtual machine is first powered on, automatically place the virtual machine on the most appropriate physical server or make a recommendation | Yes | No | Yes |
| Usage Statistics—Display detailed CPU and memory usage statistics at both the virtual machine and resource pool aggregation levels in a cluster | Yes | No | Yes, at VM and Host level only |
| History View of Implemented Actions—Provide an historical view of implemented actions as well as view of faults that have occurred in applying recommendations | Yes | Yes, in Jobs view and via PowerShell | Yes, WLB report |

### 2.3.2 Distributed Resource Scheduler Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Distributed Resource Scheduler | 2.3 Load balances resource utilization across a cluster using VMotion.<br><br>1. Turn on VMware DRS for a cluster<br>2. Set automation level for DRS cluster<br>3. Set automation level for each virtual machine | 10 minutes |

**Step 1: Turn On VMware DRS for a cluster.**

In this step, you will turn on VMware DRS for a cluster of ESX hosts that you created earlier. To turn on VMware DRS on your cluster see Figure 2.3 a. below.

1. Right-click the cluster and select **Edit Settings**. Under Cluster Features select **Turn On VMware DRS**. Each host in the cluster will now be configured for VMware DRS. Please note that you will need cluster administrator permissions to edit the cluster settings.

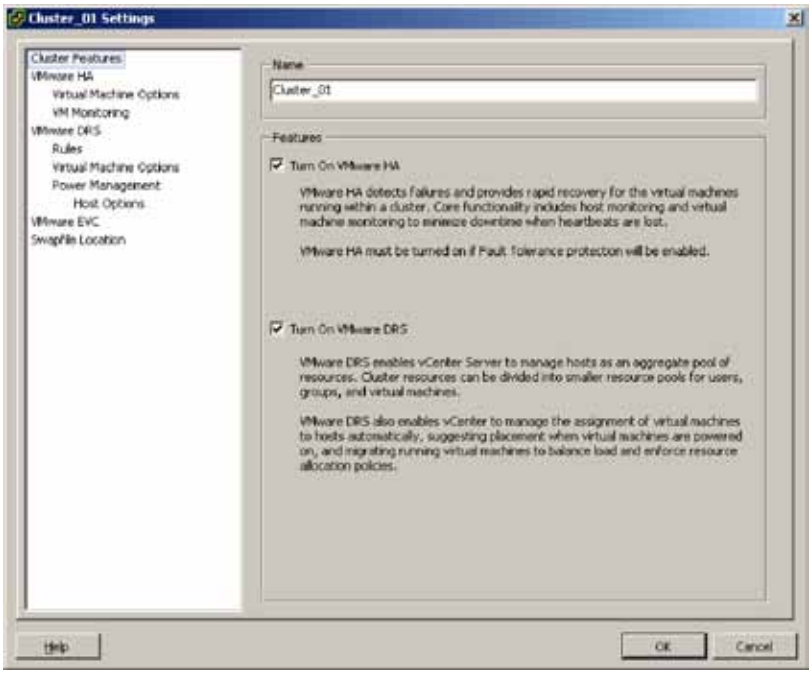



**Figure 2.3 a.** Turn On VMware DRS

**Step 2: Set automation level for DRS cluster.**

In this step you will be able to configure your DRS cluster to automatically balance your virtual machines across the cluster or simply provide recommendations to the user on where to migrate the virtual machines to achieve a load balanced cluster. Configuring the automation level of VMware DRS for the cluster is shown in Figure 2.3 b. You can also configure the automation level for each virtual machines within the cluster—explained in Step 3 below.

1. Click **VMware DRS** in the cluster settings window and you will notice that the automation level is set to Fully automated by default. The fully automated level optimally places virtual machines within the cluster upon powering them on, as well as migrates virtual machines after power on to optimize resource usage. You can adjust the sensitivity of the automated level by moving the slider bar to more conservative or more aggressive.
2. The partially automated level only places virtual machines within the cluster upon power on and then gives recommendations on where to migrate them to optimize resource usage.
3. The manual level gives placement recommendations at power on as well as where to migrate them later.

For this evaluation leave your VMware DRS settings at the default of Fully automated with the Migration threshold set in the center level.

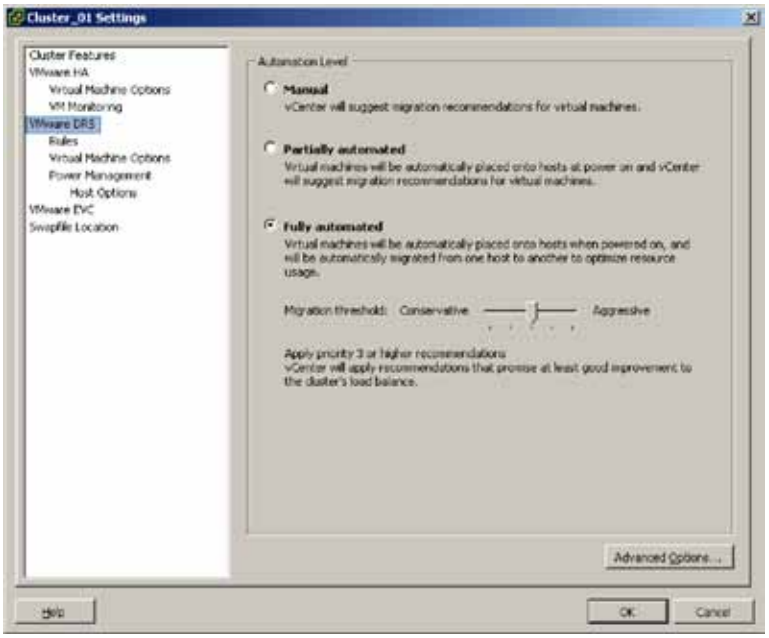



**Figure 2.3 b.** Enable fully automated mode for VMware DRS

**Step 3: Set automation level for each virtual machine.**

In this step, you will be able to configure each virtual machine, to be automatically balanced across the cluster or simply provide recommendations to the user on where to migrate the virtual machine to achieve a load balanced cluster.

1. To adjust the automation level for each virtual machine, click **Virtual Machine Options** under "VMware DRS" in the cluster settings window. For this evaluation keep your Virtual Machine Options set at their default values.

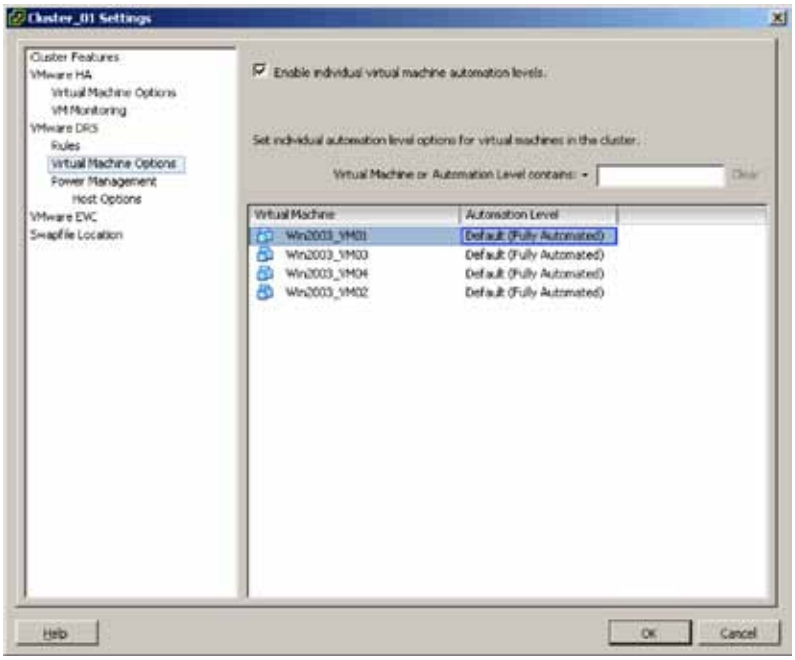



**Figure 2.3 c.** Set virtual automation levels for VMware DRS

## 2.4. Distributed Power Management

**What It Is:** VMware Distributed Power Management (DPM) monitors the CPU and memory resource utilization of a cluster and determines whether one or more ESX hosts should be powered off or powered on in order to maintain a pre-defined resource utilization threshold. When cluster resource utilization is low DPM will power one or more ESX hosts off to save power. Then when cluster resource utilization becomes high DPM will power one or more ESX hosts back on, assuming there are any available to be powered on.

**Use Case:** Power Savings During a Typical Workweek

VMware DPM can be used to power on and shut down ESX hosts based on utilization patterns during a typical workday or workweek. For example, services such as email, fax, intranet, and database queries are used more during typical business hours from 9 a.m. to 5 p.m. At other times, utilization levels for these services can dip considerably, leaving most of the hosts underutilized. Consolidating virtual machines onto fewer hosts and shutting down unneeded hosts during off hours reduces power consumption.

### 2.4.1. VMware Differentiators

VMware VDPM is a unique feature of VMware vSphere. DPM is the most effective way to extend power savings from virtualization. Tests have demonstrated potential savings of 50% in power consumption when turning on DPM.

- **VMware DPM extends power consumption cost savings beyond what users can obtain from simple server consolidation.**
  - VMware DPM is fully supported with vSphere and works in coordination with DRS. Based on user-defined policies, DPM monitors a DRS cluster and verifies whether SLAs could be met at a lower power consumption rate. When an application workload increases, DPM re-activates the suspended hosts. DPM and DRS thresholds are independent from each other and each intelligent engine can be set at different levels of aggressiveness.
  - VMware DPM supports three different wake protocols: Intelligent Platform Management Interface (IPMI), Integrated Lights-out (iLO) and Wake-On-Lan (WOL). DPM can selectively exclude hosts from power management and optionally implements recommendations in manual mode (Admin needs to approve) or fully automated mode.
- **No other virtualization offering provides DPM-like capabilities.** VMware DPM is another great example of how VMware vSphere is the most advanced virtualization platform and once again provides unique benefits that neither Microsoft nor Citrix can deliver.

### 2.4.2 Distributed Power Management Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Distributed Power Management | 2.4 Monitor the CPU and memory resource utilization of a cluster and decide whether to power off ESX hosts to reduce power consumption<br><br>1. Turn on VMware DPM for a cluster<br>2. Set Power Management for each ESX host in the cluster<br>3. Observe VMware DPM generating and executing recommendations | 20 minutes |

**Step 1: Turn on VMware DPM for a cluster**

Once you turn on VMware DRS for your cluster you can enable the cluster for VMware DPM, which allows the power management of ESX hosts within the cluster. You must also ensure that Wake-on-LAN, IPMI, or iLO are functioning properly on your hosts. Only then can VMware DPM automate the power on and power off of ESX hosts using one of those methods. Refer to Figure 2.4 a. to turn on VMware DPM.

1. Click **Power Management** under VMware DRS in the cluster settings window and you will see that VMware DPM is turned off by default.

2. For this evaluation select **Automatic** to enable VMware DPM on the cluster, and keep the DPM Threshold set at the default center level. In automatic mode, VMware DPM recommendations are executed without user confirmation. (In manual mode, execution of VMware DPM recommendations requires confirmation by the user).

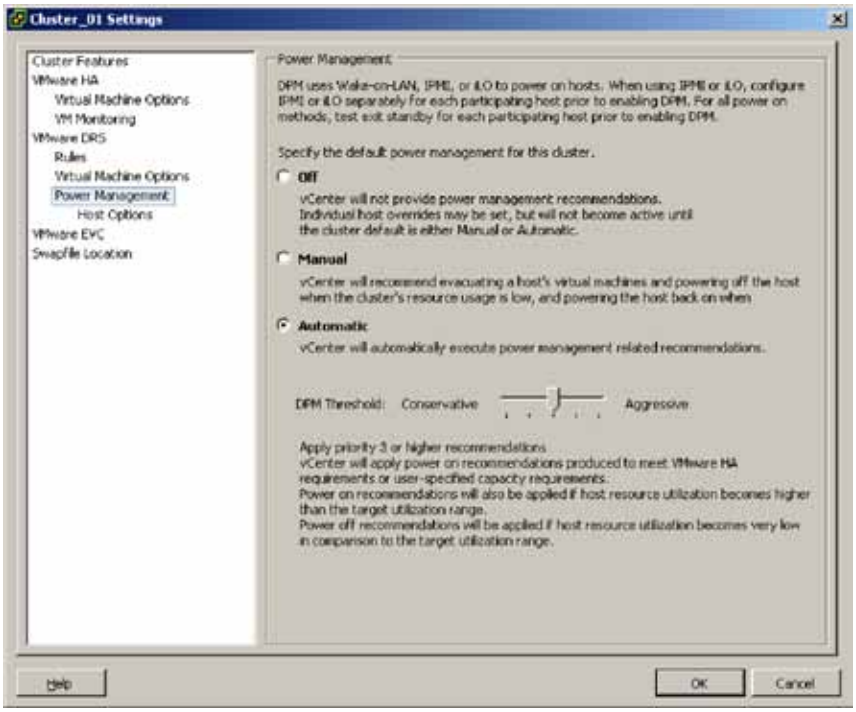



**Figure 2.4 a.** Enable VMware DPM

### Step 2: Set power management for each ESX host in the cluster

By default the VMware DPM automation setting applies to all hosts in the cluster, but you can override the setting on a per-host basis. For example, you should set any hosts in the cluster that cannot be powered on via Wake-on-LAN to Disabled. You should also set to Disabled any other hosts that you never want VMware DPM to power off.

1. To set power management options for individual ESX hosts in the cluster, click **Host Options** under Power Management in the cluster settings window.

2. Select **Disabled** under Power Management for "esx05a" if you wish to turn off VMware DPM for that host. For this evaluation leave your Host Options set at their default values.

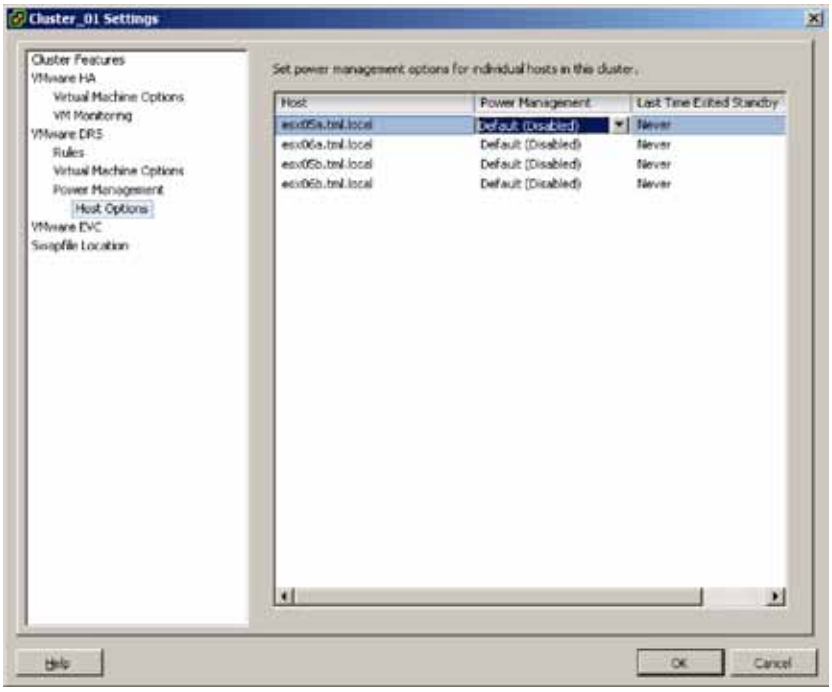



**Figure 2.4 b.** Set VMware DPM Host Options

### Step 3: Observe VMware DPM generating and executing recommendations

Once enabled, VMware DPM will begin generating recommendations and will execute them assuming VMware DPM was set to automatic mode. In this evaluation environment—with four ESX hosts and four virtual machines running at low CPU utilization—VMware DPM will begin to immediately take action. In this case, two of the four ESX hosts will be powered down.

VMware DPM performs the following actions when powering down an ESX host:

1. First VMware DPM will use VMotion to migrate virtual machines "Win2003_VM02" and "Win2003_VM03" to "esx05b" and "esx06a", respectively.

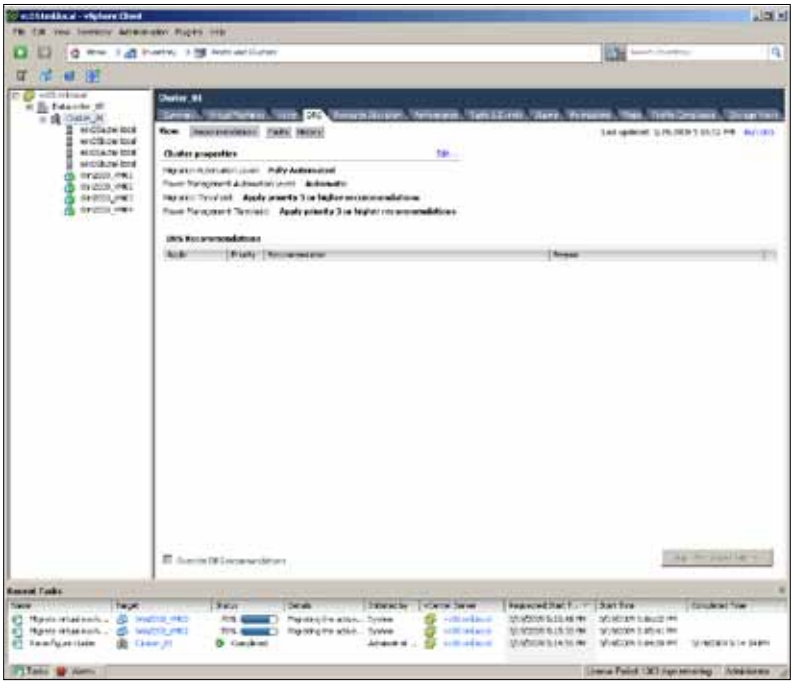


**Figure 2.4 c.** VMware DPM Uses VMotion

2. Then VMware DPM will disable VMware HA on hosts "esx05b" and "esx06a", which will then be powered down.

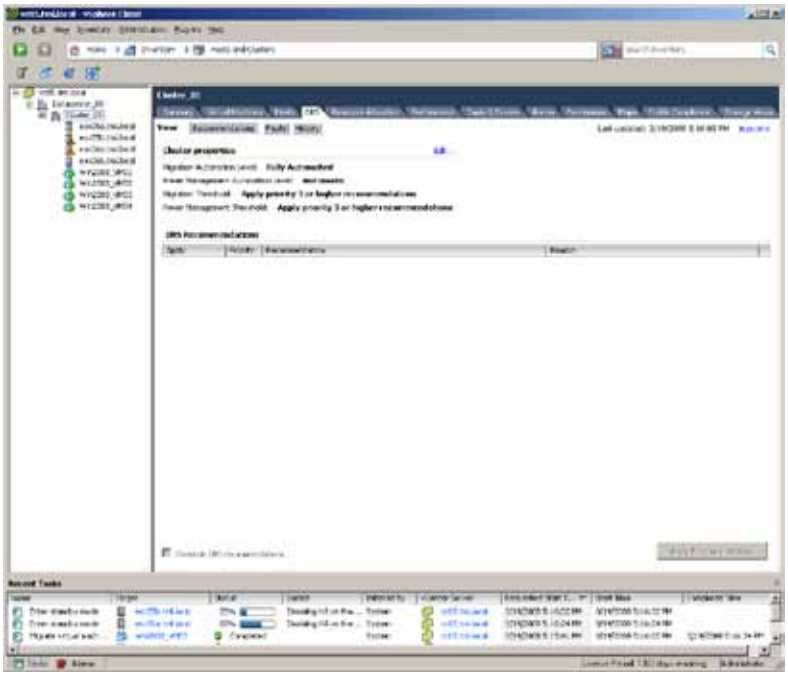


**Figure 2.4 d.** VMware DPM Disabling VMware HA for Hosts to Be Powered Down

3. Finally VMware DPM powers down hosts "esx05b" and "esx06a". Notice the special icons next to the powered down hosts in the left pane.

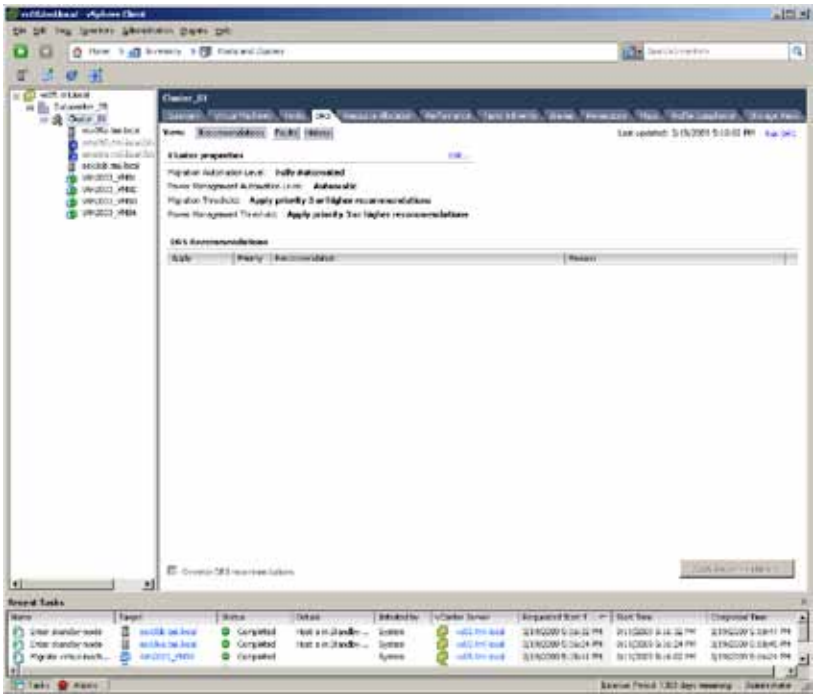


**Figure 2.4 e.** VMware DPM Powers Down Hosts

## 2.5. Fault Tolerance

**What It Is:** VMware Fault Tolerance (FT) protects a virtual machine in a VMware HA cluster. VMware FT creates a secondary copy of a virtual machine and migrates that copy onto another host in the cluster. VMware vLockstep technology ensures that the secondary virtual machine is always running in lockstep synchronization to the primary virtual machine. When the host of a primary virtual machine fails, the secondary virtual machine immediately resumes the workload with zero downtime and zero loss of data.

**Use Case:** On Demand Fault Tolerance for Mission-Critical Applications.

VMware FT can be turned on or off on a per-virtual machine basis to protect your mission-critical applications. During critical times in your datacenter, such as the last three days of the quarter when any outage can be disastrous, VMware FT on-demand can protect virtual machines for the critical 72 or 96 hours when protection is vital. When the critical periods end FT is turned off again for those virtual machines. Turning on and off FT can be automated by scheduling the task for certain times. Refer to Figure 2.5 a. below showing a server failure while running two virtual machines protected by VMware HA and a third virtual machine protected by FT. The HA-protected virtual machines are restarted on the other host while the FT-protected virtual machine immediately fails over to its secondary and experiences no downtime and no interruption.

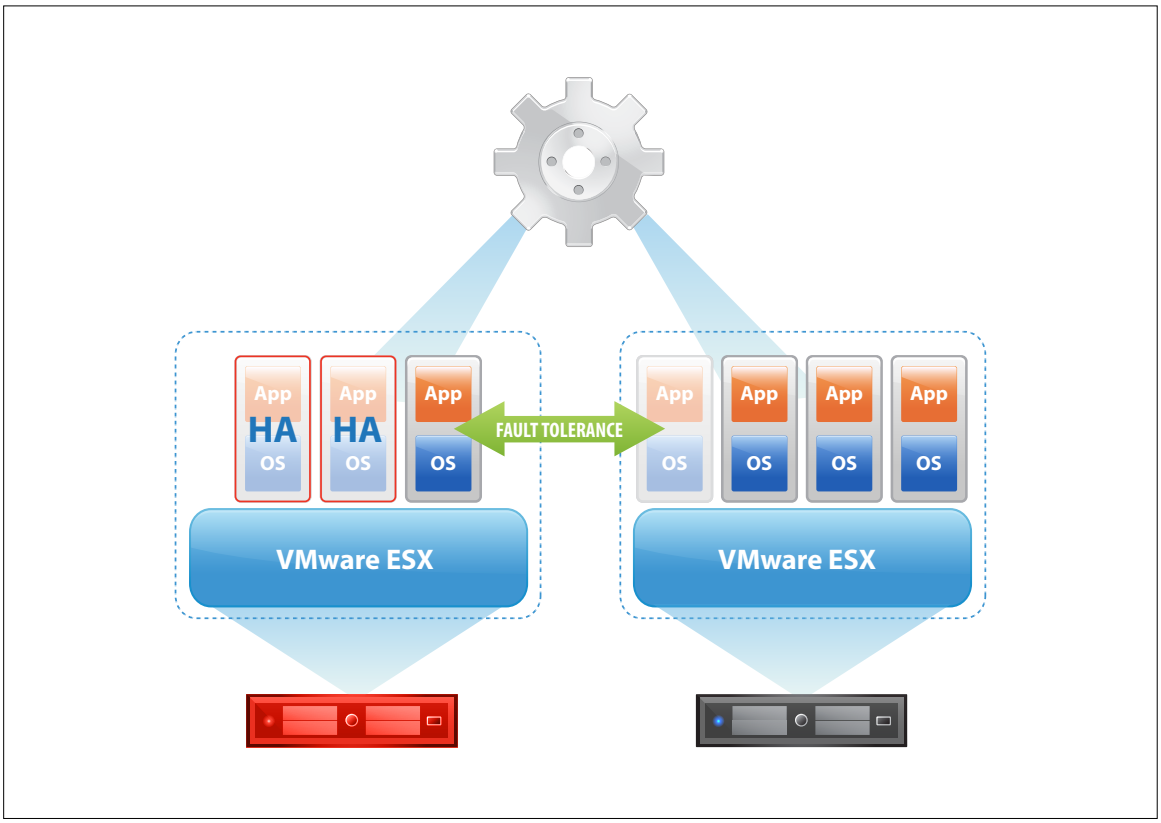



**Figure 2.5 a.** FT protects one virtual machine while HA protects the others

### 2.5.1. VMware Differentiators

Fault Tolerance is a unique VMware feature. It is the simplest and most cost effective solution to enable zero down time and zero data loss protection against hardware failures

- **Easiest to use:** VMware Fault Tolerance (FT) enables continuous availability for VMs and applications in a matter of few clicks with the same simple process as VMware HA. Once a virtual machine is made Fault Tolerant with VMware FT, vSphere will automatically place the "shadow VM" on the most appropriate secondary host and maintain the two VMs in perfect lock-step down to the CPU instruction level.
- **Most cost effective:** VMware FT does not require specialized hardware or additional third-party software. It is an integral part of vSphere and takes advantage of other key features such as VMware VMotion and DRS Intelligent Placement.
- **Neither Citrix nor Microsoft offer a solution for continuous application availability:** Both companies have repeatedly talked about future availability of third-party solutions, such as Marathon everRun VM Lockstep, which is still not shipping at the time of this writing. Even when such third-party solutions become available, they will come at a high additional cost, provide limited capabilities, and add substantial complexity because of their lack of integration with virtualization management, cumbersome installation, configuration, and set-up.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **CONTINUOUS AVAILABILITY** | | | |
| Zero Downtime, Zero-data-loss Protection—Automatically detect server failures and trigger instantaneous, seamless stateful failover resulting in continuous availability | Yes | No | No |
| Maintain Protection Levels After Failover—Ensure that an application's fault tolerance property is automatically reinstated even after a failover | Yes | No | No |
| Support continuous availability with all types of shared storage, including Fibre Channel, NAS or iSCSI | Yes | No | No |
| Integration with Live Migration—Fault tolerant virtual machines can still be live migrated | Yes | No | No |
| Intelligent Initial Placement—When a virtual machine is first made fault tolerant, its shadow copy is automatically placed on the most appropriate physical server | Yes | No | No |
| Single management console | Yes | No | No |
| Does not require specialized hardware | Yes | N/A | N/A |
| Number of Guest OSs supported | 55 | N/A | N/A |

### 2.5.2. Fault Tolerance Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Fault Tolerance | 2.5 VMware Fault Tolerance allows failover of a virtual machine with no data loss during server failures.<br><br>1. Turn on VMware Fault Tolerance for a virtual machine<br>2. Convert virtual disks to thick-provisioned virtual disk<br>3. Observe the following actions after turning on VMware FT<br>4. Simulate server failure to demonstrate FT failover<br>5. Observe vSphere alarms after host failure | 45 minutes |

**Step 1: Turn on VMware Fault Tolerance for a virtual machine**

1. Once your cluster is enabled with VMware HA, you can protect any virtual machine with VMware FT, given that the following prerequisites are met:
    1. The ESX host must have an FT-enabled CPU. For details please refer to http://kb.vmware.com/kb/10080 27.
    2. Hosts must be running the same build of ESX.
    3. Hosts must be connected via a dedicated FT logging NIC of at least 1GBps.
    4. Virtual machine being protected must have a single vCPU.
    5. Virtual machine's virtual disk must be thick provisioned.
2. To enable a virtual machine with VMware FT, right-click the virtual machine called Win2003_VM01 on esx05a, select **Fault Tolerance**, and click **Turn On Fault Tolerance**. Please note that you will need cluster administrator permissions to enable VMware FT.

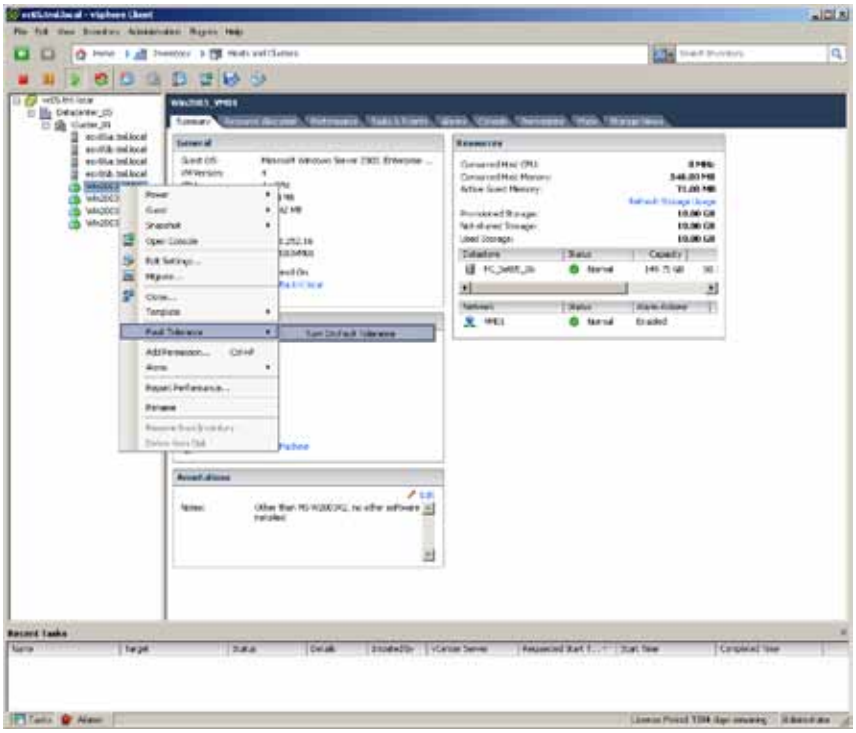


**Figure 2.5 b.** Enable VMware FT

### Step 2: Convert virtual disks to thick-provisioned virtual disk

VMware FT requires the virtual machine's virtual disk to be thick provisioned. Thin-provisioned virtual disks can be converted to thick-provisioned during this step.

1. A dialog box will appear indicating that virtual machines must use thick-provisioned virtual disks. Click **Yes** to convert to thick-provisioned virtual disks and continue with turning on VMware FT.


**Figure 2.5 c.** Thick-provisioned virtual disk dialog box

### Step 3: Observe the following actions after turning on VMware FT

The process of turning on FT for the virtual machine has begun and the following steps will be executed:

1. The virtual machine, Win2003_VM01, is designated as the primary virtual machine.
2. A copy of Win2003_VM01 is created and designated as the secondary machine.

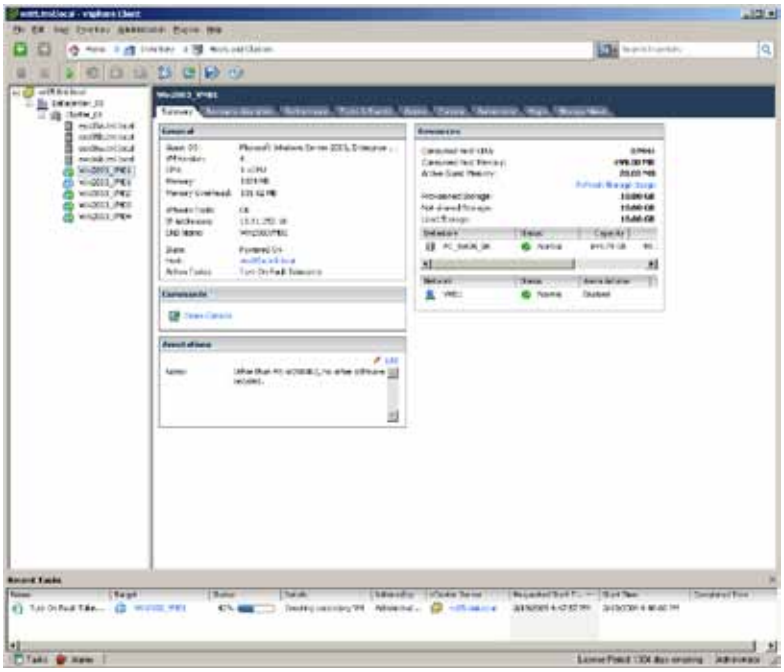


**Figure 2.5 d.** FT Creating Secondary Virtual Machine

3. The secondary virtual machine is migrated to another ESX host in the cluster, esx05b in this case. VMware DRS is used to determine what host the secondary virtual machine is migrated to when FT is turned on. For subsequent failovers, a host for the new secondary virtual machine is chosen by VMware HA. Win2003_VM01 is now labeled as **Protected** under **Fault Tolerance Status**.

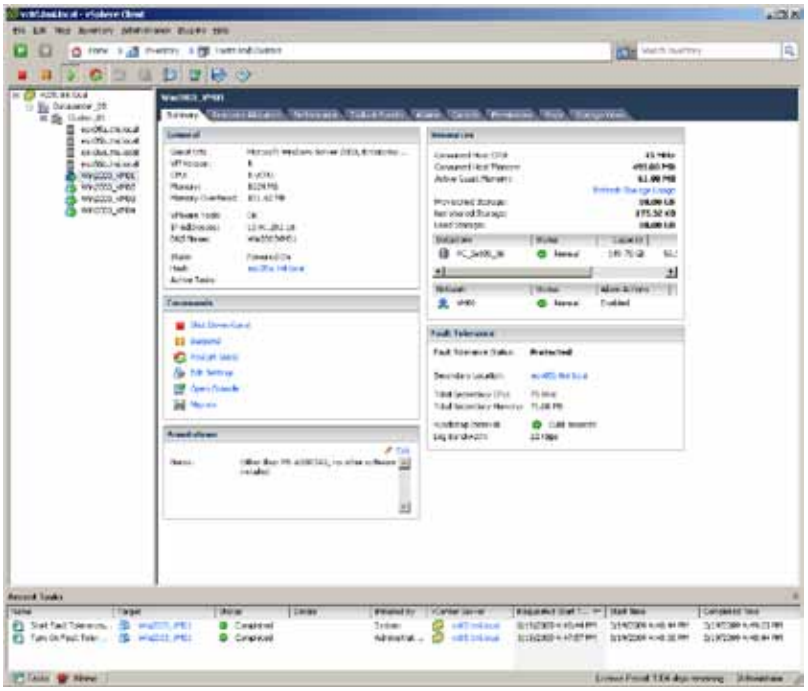


**Figure 2.5 e.** FT Now Protecting Virtual Machine

### Step 4: Simulate server failure to demonstrate FT failover

Now host esx05a will be rebooted to simulate a host failure and show the virtual machine, Win2003_VM01, is protected without any downtime, while Win2003_VM02 is restarted on another host by VMware HA. You may wish to run a workload of your choice in the FT-protected virtual machine to demonstrate zero downtime during the host failure. The new secondary virtual machine for the FT-protected workload will be spawned to a host chosen by VMware HA.

1. SSH into the esx05a host.
2. Issue a sync command to flush all the host's file system buffers to disk.
3. Issue a reboot—f command to reboot the host, simulating a host failure.

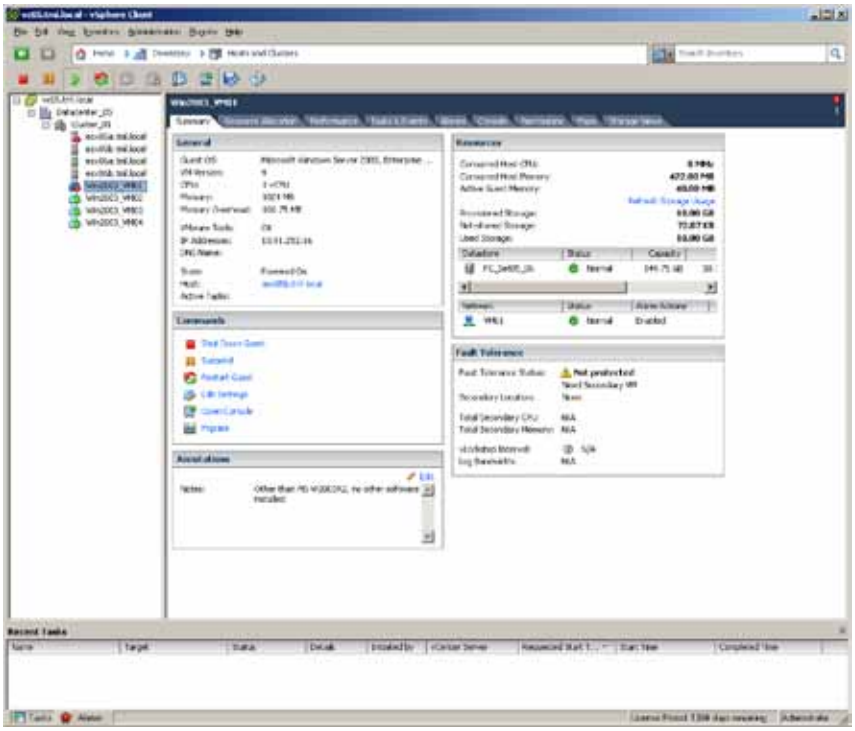


**Figure 2.5 f.** Host is Rebooted to Simulate Failure

### Step 5: Observe vSphere Alarms after Host Failure

Certain alarms are built into VMware vSphere to signal failures in ESX hosts as well as virtual machines. During the host failure invoked above, you can see an alarm for the FT-protected virtual machine.

1. Click the **Alarms** tab for Win2003_VM01. Here an alarm is generated even though the virtual machine's workload continues to run uninterrupted because of VMware FT.

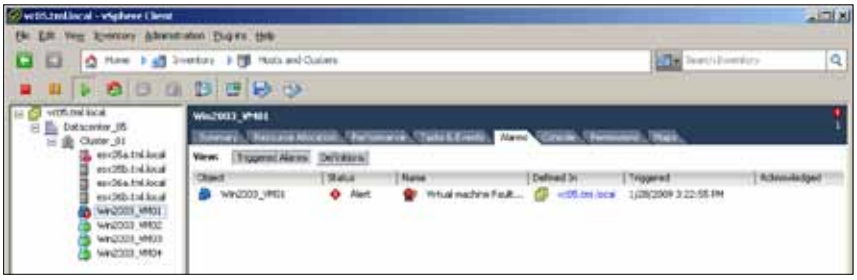


**Figure 2.5 g.** Virtual Machine Alert After Failure

2. Click the **Alarms** tab for the rebooted ESX host, esx05a, to see the change in the host connection and power state.

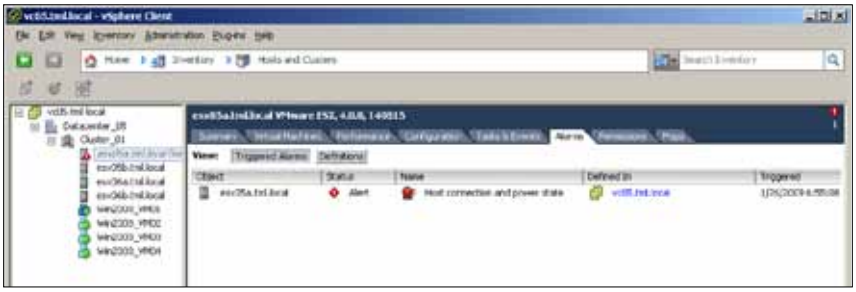


**Figure 2.5 h.** Host Alert After Failure

## 2.6. Storage VMotion and Thin Provisioning

**What It Is:** Storage VMotion enables relocation of the Virtual Machine home (files on disk) while the VM is up and running. Although released in version 3.5, Storage VMotion has been enhanced in the vSphere release to include several new capabilities:

1. Integration with the vCenter graphical interface
2. Support for changing the format of the virtual disks as they are moved
3. Use of change block tracking so that it no longer needs 2x CPU and memory to migrate the virtual machine files on disk
4. Full support for migration to and from FC, iSCSI, and NFS datastores

Virtual Thin Provisioning provides efficient storage utilization by using only what the actual virtual disk needs for storage capacity and growing the used space as the disk fills up. The feature has also been integrated in vCenter, so disk format can be easily defined at creation time as well as when VMs are cloned, migrated or deployed from templates.

**Use Case:** The following steps will show how Storage VMotion can be used in conjunction with thin provisioning to change the format from thick to thin as the running VM files on disk (also referred to as the VMhome*) are migrated from one datastore to another. The VMhome is the subdirectory in the VMFS structure that contains the components that comprise the virtual machine.

---

* The VMhome is the subdirectory within the Virtual Machine File System (VMFS) that contains all the components that make up a virtual machine. Each time a new virtual machine is created, there is a new subdirectory created in the VMFS. When Storage vMotion is done, the entire contents of that subdirectory is moved from one datastore to another. That process is moving the entire VMhome from one location to another while the VM remains up and running. If the VMhome is on a NFS storage device, the creation of a new subdirectory will be done on the NFS datastore.

### 2.6.1. VMware Differentiators

Storage VMotion and Thin Provisioning with a consumption-based monitoring and alerting system is a unique VMware feature. With VMware Storage VMotion and Thin Provisioning, users can eliminate downtime associated with storage management operations, reduce storage cost and make storage management more efficient.

- **Zero-downtime for storage management:** Only VMware with Storage VMotion allows users to perform virtual machine disk migrations without application downtime. Such capability is not unavailable for Hyper-V and XenServer users who will still have to schedule traditional downtime windows when virtual machines are migrated to different storage locations.
- **Lowest storage cost:** With VMware Thin Provisioning, users can defer disk storage purchases to when they are actually needed. In addition to the capability of creating thin provisioned disks, VMware vSphere also provides a built-in consumption-based monitoring system with which administrators can control disk space availability levels. Consumption-based monitoring is essential to the use of thin provisioning without the risk of unexpectedly running of out of space. Microsoft Hyper-V supports thin provisioned disks, but does not provide any consumption-based monitoring system making thin provisioning extremely risky—and therefore unlikely to be adopted in production.
- **Simpler and more efficient storage management:** VMware Storage VMotion simplifies storagemanagement tasks by supporting virtual disk migrations between and among Fibre Channel, iSCSI, and NAS systems. Users can very easily move data stores to the most appropriate storage tier without downtime. Storage VMotion provides additional management flexibility by also supporting virtual disk live migrations from thick to thin format.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SC | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **STORAGE VMOTION AND THIN PROVISIONING** | | | |
| Thin Provision Virtual Machines—Create virtual machines without provisioning all the storage required upfront | Yes | Yes | No?? |
| Consumption-based Monitoring and Alerting—Set alerts to notify administrators when they need to procure more storage or rebalance virtual machines across the available storage with Storage VMotion | Yes | (Dynamic Disk) | No |
| Disk Format Conversion—Supports thick-to-thin and thin-to-thick disk format conversion | Yes | No | No |

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SC | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **STORAGE VMOTION AND THIN PROVISIONING** | | | |
| Storage VMotion—Live migrate running virtual machines from one storage location to another with no disruption or downtime | Yes<br>Thin-thick powered off VM Thick-thin with Storage VMotion (VM can be on) | Yes (VMs must be powered off) | No |
| Heterogeneous Storage Support—Support for live-migration between different types of storage (FC, iSCSI, NFS and even local storage) and between RDMs to RDMs and RDMs to VMDKs (non-passthrough) | Yes | No | N/A |
| Administrator Interface—Perform storage management and storage live-migration directly from virtualization management console | Yes | N/A | N/A |

### 2.6.2 Storage VMotion and This Provisioning Hands-on Review

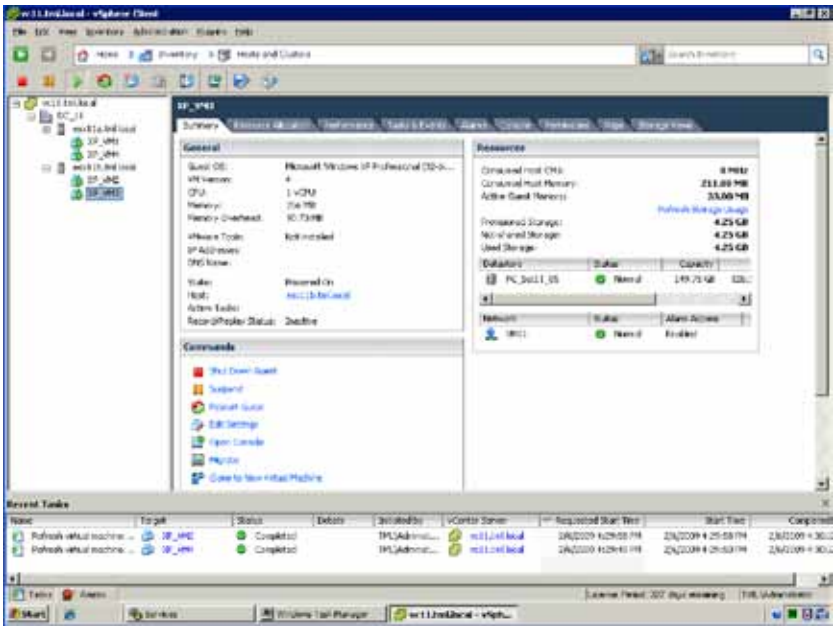
| | | | |
|---|---|---|---|
| Availability and Capacity | Storage vMotion and Thin Provisioning | 2.6 Storage VMotion and Thin Provisioning<br><br>1. Initiation of a Storage VMotion<br>Change the virtual disk format as you move the VMhome to the new datastore | 20 minutes |

**Step 1: Initiation of a Storage VMotion**

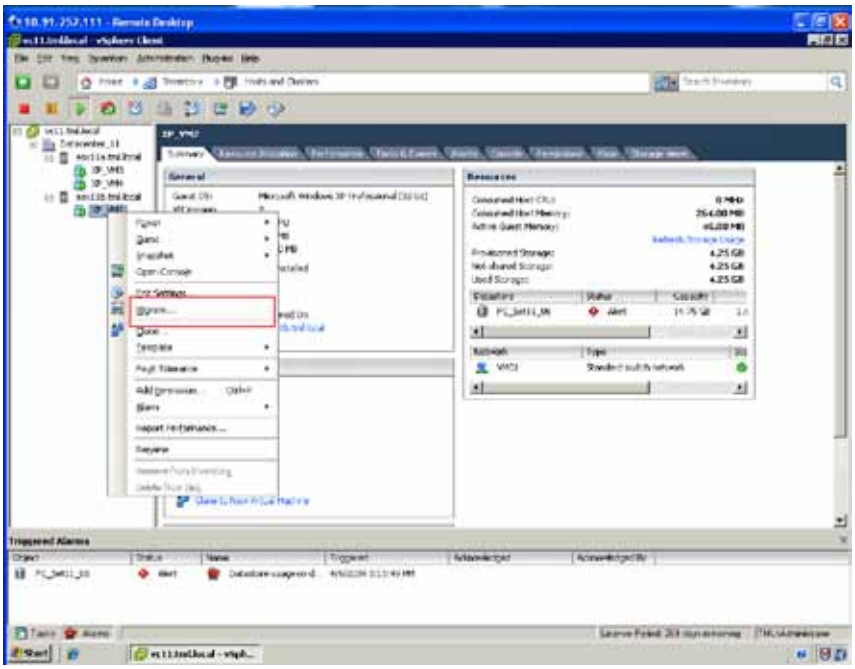
Use vCenter to step through the process of migrating a VMhome from one FC datastore to the iSCSI datastore. Select a running VM from the inventory and then move it to the iSCSI datastore while it's up and running—investigating the options available and monitoring the steps as this process completes. You will also move a VM with a virtual disk that was thick format to a new location where it will be thin provisioned to highlight the ease of this conversion as well as the space savings the thin virtual disk enables.

1. Login to vCenter and select a VM to be migrated with Storage VMotion.

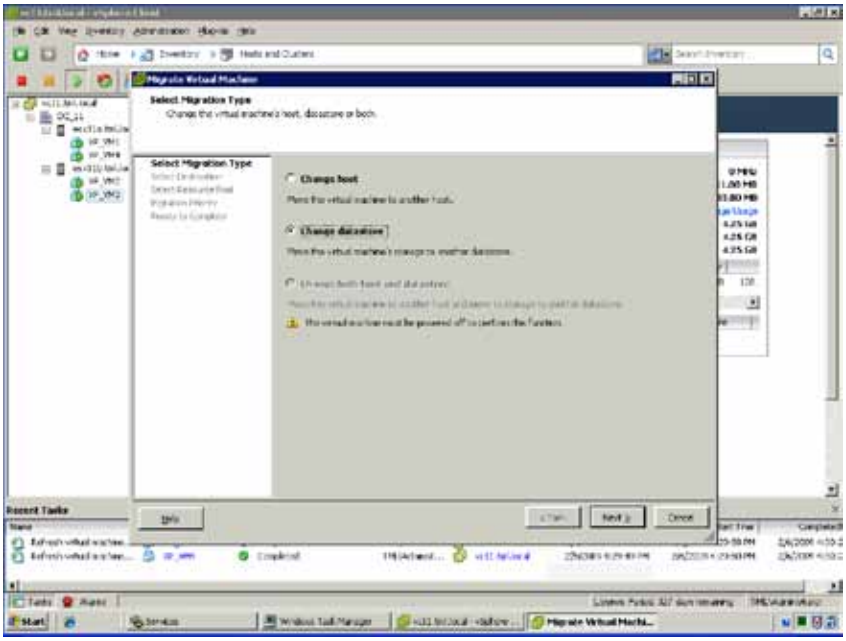
2. Highlight the **VM** in the left pane and click the **Summary** tab on the right side of the view. Note the information about the datastore on which it is located. The size of the VMhome in that datastore is 4.25GB.



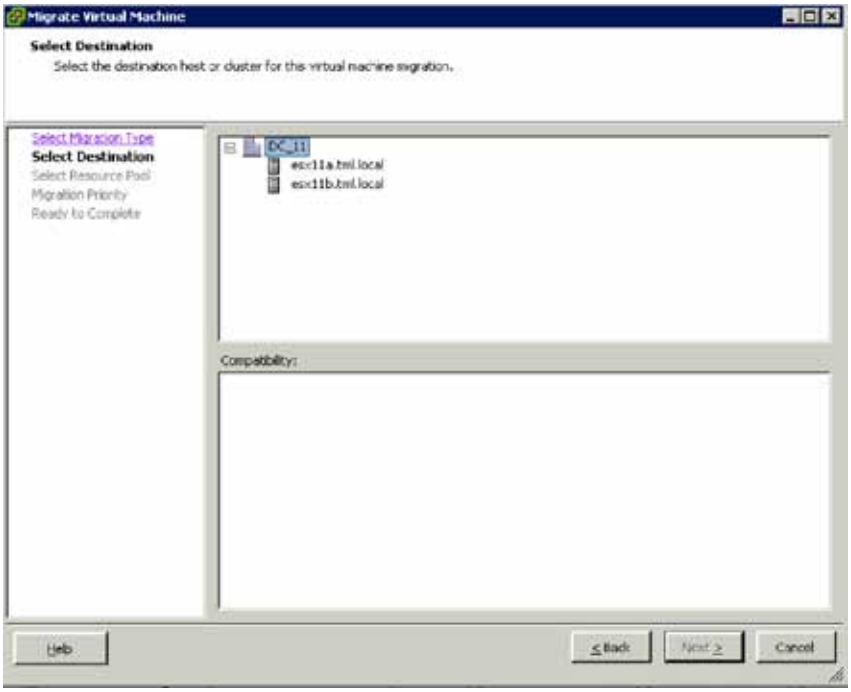
3. Select the **VM** in the inventory view and right-click to reveal options. Scroll down and select the **Migrate** option.



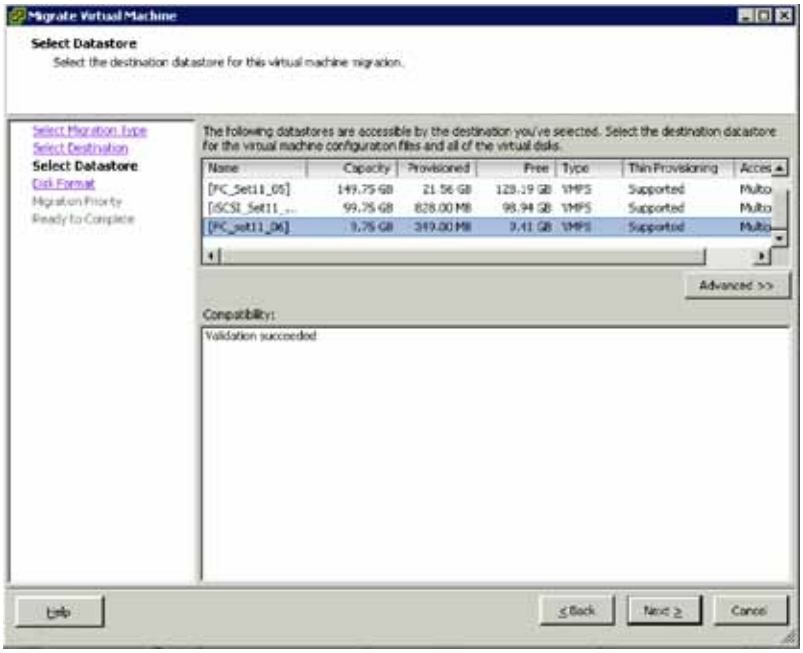
4. Select the **Change Datastore** option and click **Next**.



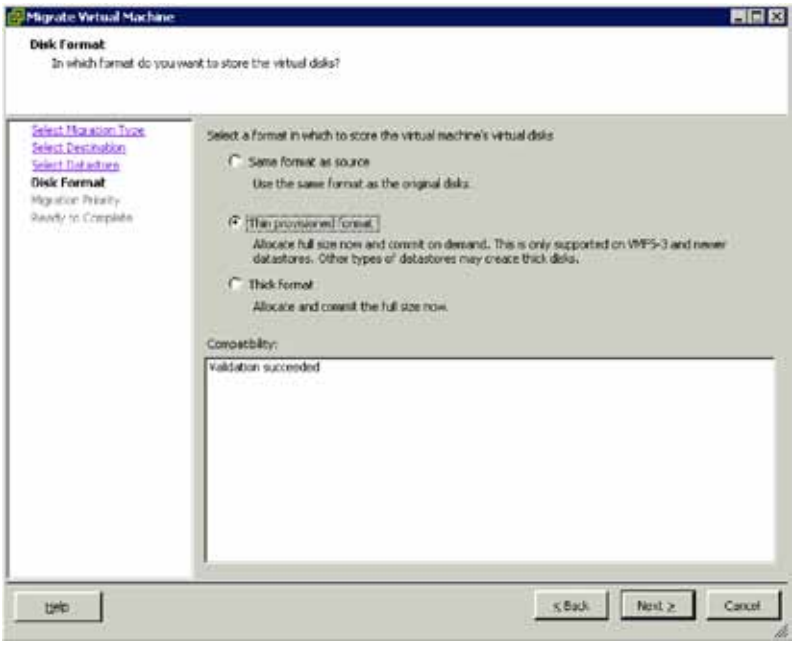
5. Select the **datacenter and VMware ESX** and click **Next**.



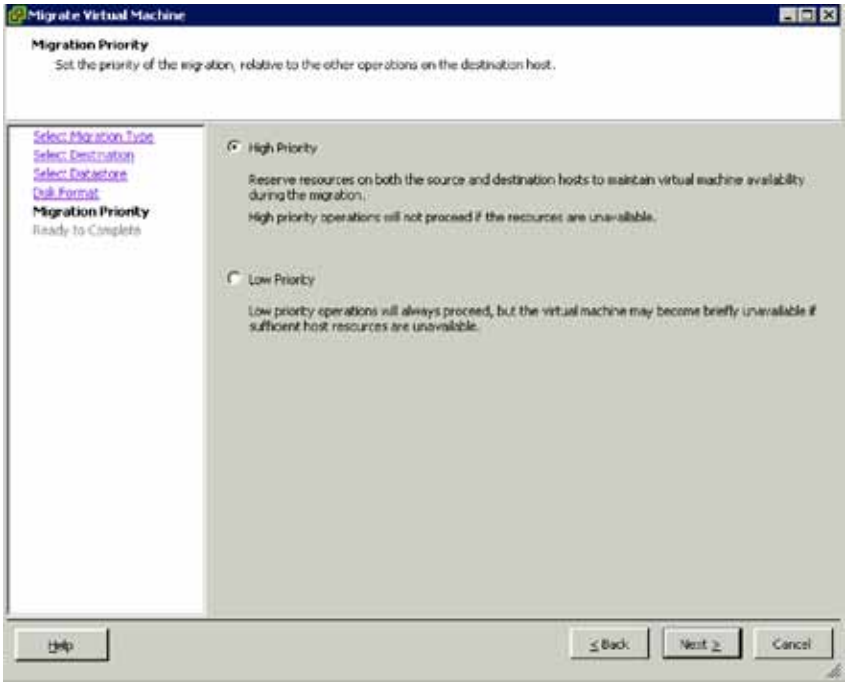
6. Select the datastore into which you would like to migrate the VM. Click **Next**.



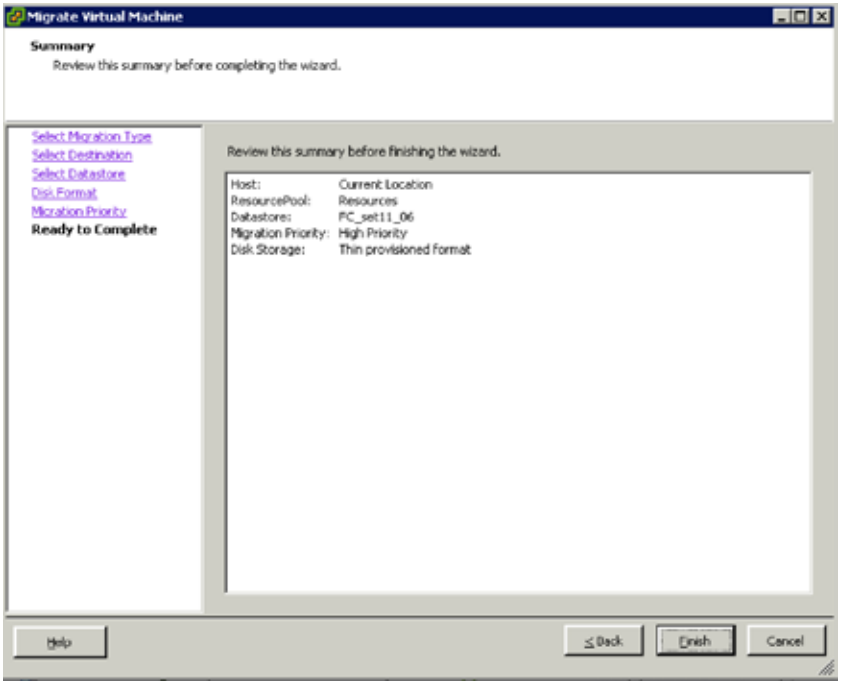

7. Chose the disk format you want the virtual machines virtual disks to utilize in the target datastore to which you are migrating the VM. In this case, select the **Thin provisioned** format to allow you to highlight storage space savings that can be achieved using the thin provisioned virtual disk format. Click **Next**.



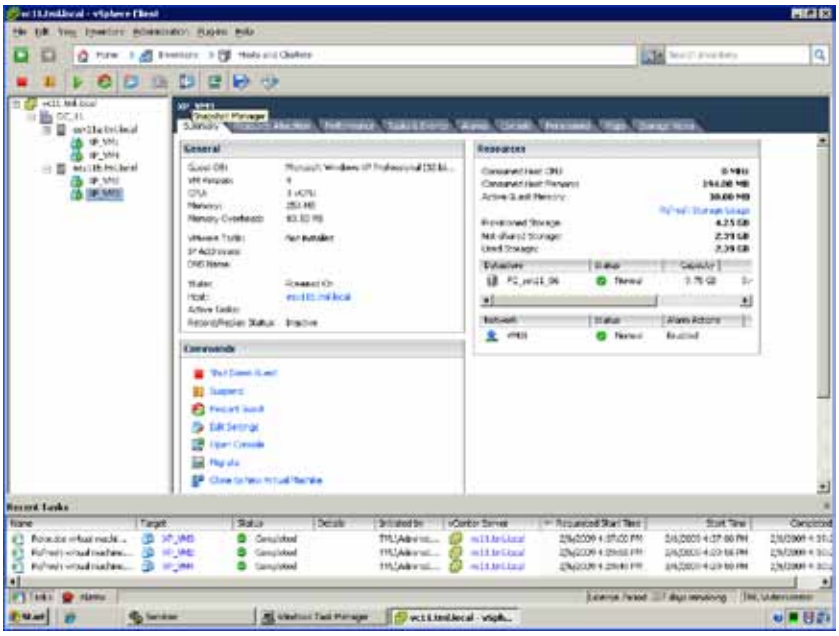
8. Select the priority for this migration to be completed. Default priority is high so leave as is. Click **Next**.




9. Review selections and click **Finish** to confirm.



10. The Storage VMotion task will show up in the recent tasks section of the vSphere window and percent progress will be reported.



Once the Storage VMotion process has completed, notice the amount of storage capacity in takes up in the target datastore. It is provisioned as 4.25GB, but is only using 2.39GB of space. The change in virtual disk format from thick to thin has saved 1.86GB (4.25—2.39) of capacity.

## 2.7. VMware vApp

**What It Is:** VMware vApp simplifies the deployment and ongoing management of an n-tier application in multiple virtual machines by encapsulating it into a single virtual service entity. vApps encapsulate not only virtual machines but also their interdependencies and resource allocations allowing for single-step power operations, cloning, deployment, and monitoring of the entire application. vCenter Server includes support for creating and running vApps, as well as importing and exporting them in compliance with Open Virtualization Format (OVF) 1.0 standard.

**Use Case:** Use VMware vApp to deploy and manage a multi-tier application.

### 2.7.1. VMware Differentiators

vApp is a unique VMware capability which allows users to greatly simplify the deployment and ongoing management of single and multi-tiered applications.

- With vApp, users can manage single and multi-tiered applications as a single service entity. vApp significantly improves the efficiency of application deployment and ongoing management tasks by enabling single-step power operations, cloning, deployment and monitoring.
- Neither Microsoft nor Citrix provide a comparable capability. This means that each virtual machine component of a multi-tiered application will have to be managed independently from the other components, making application deployment and management cumbersome and inefficient.
- vApp is based on the Open Virtualization Format (OVF) which makes it an interoperable and extensible framework. Users can easily import vApp constructs created by third-party vendors, create custom ones, and export them to files. vApp guarantees that regardless of where an application is deployed (internal or external cloud) the specified level of resources and setup will be applied without the need of inefficient re-configurations.

### 2.7.2 VMware vApp Hands-on Review

In this exercise, you will be creating a VMware vApp and specifying the startup sequence of the VMs encapsulated within the vApp. You will then perform a single-step power operation on the vApp, to demonstrate that the applications are following the designated startup sequence.

Before beginning this section, verify that you have the following:

1. At least two VMs, both registered against the same VMware ESX host
2. A host that is running ESX 3.0 or greater is selected in the inventory
3. A DRS-enabled cluster is chosen in the inventory
4. A folder is chosen in the Virtual Machines and Templates view

| | | | |
|---|---|---|---|
| Application Deployment and Management | VMware vApp | 2.7 Use VMware vApp to deploy and manage a multi-tier application:<br><br>1. Create a vApp<br>2. Specify startup sequence for the multi-tier application and perform single-step power operation | 10 minutes |

**Step 1: Create a vApp**

In this step, you will create a new VMware vApp that encapsulates two virtual machines (Win2003_VM01 and Win2003_VM02) into a single virtual service entity.

1. Right-click **Cluster_01**, and select **New vApp**.
2. On the Name and Folder page, specify "vApp_01" as the name for the vApp. Select **Datacenter_02** as the location in the inventory for the vApp. Click **Next**.
3. On the Resource Allocation page, you can allocate CPU and memory resources for this vApp. For this exercise, you can proceed with the defaults, and click **Next**.
4. On the Ready to Complete page, review and click **Finish** to complete the vApp creation.

5. Once the vApp has been created, select "Win2003_VM01" and "Win2003_VM02" and add them to vApp_01 by drag-and-drop.

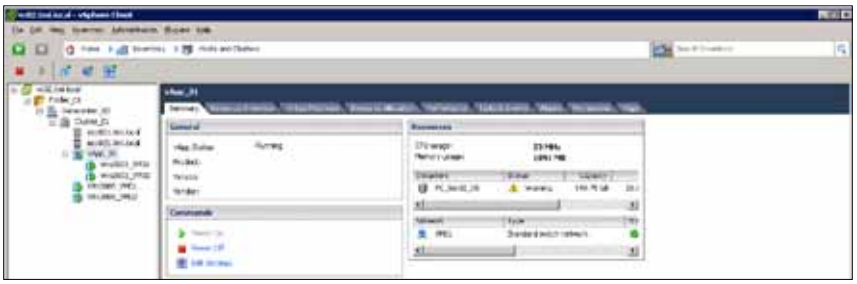
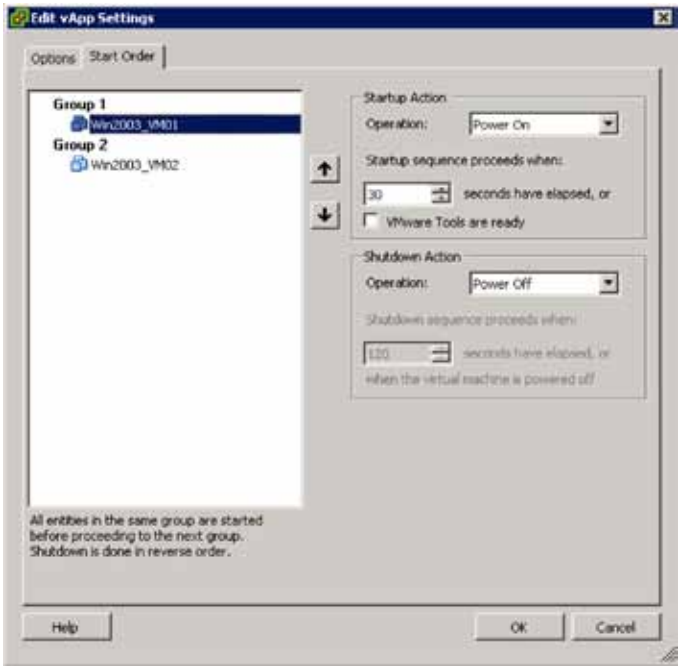


**Figure 2.7 a.** vApp_01 created and Win2003_VM01 and Win2003_VM02 added

**Step 2: Specify startup sequence for the multi-tier application and perform single-step power operation**

In this step, you will specify the order in which the virtual machines within the vApp start up and shut down. You will also specify delays and actions performed at startup and shutdown. You will then perform a single-step power operation on the vApp, to demonstrate that the applications are following the designated startup sequence.

1. On the Summary page of the vApp, click **Edit Settings**. Select the "Start Order" tab to edit startup and shutdown options.
2. Note the sequence that the Virtual Machines will start up. For the purposes of this exercise, specify "Win2003_VM01" in Group 1 and "Win2003_VM02" in Group 2. Use the arrow keys to change the startup order if necessary.
3. Note the delay and action for startup and shutdown for each virtual machine. The default settings specify that the first VM should start 120 seconds before the second VM. This is ideal for tiered applications where certain services need to be up and running (such as a database) before additional services start, and these additional services may reside in different virtual machines. For the purpose of this exercise, you can reduce this to 30 seconds. Click **OK** when finished.



4. In the Summary page for the vApp, click **Power On/Power Off**.
5. On the Task and Events tab, select the task for vApp_01. Note the 30-second delay between the startup times of Win2003_VM01 and Win2003_VM02, as well as the startup order. Each application within the vApp is powered on according to how the startup order is set.

## 2.8. Update Manager

**What It Is:** VMware vCenter Update Manager is a vCenter plug-in patch management solution for VMware vSphere. Update Manager provides a single patch management interface for ESX hosts, virtual machines and guests, allowing administrators to ensure their virtual infrastructure is compliant with baselines they define.

In this guide, you will walk through the following use cases:

1. Patching a cluster with critical host patches
2. Orchestrated upgrade of datacenter to ESX 4.0 by
   a. Upgrading ESX 3.5 to ESX 4.0 using an upgrade baseline
   b. Upgrading VMware Tools and VM hardware using a baseline group
3. Configuring Update Manager to use a central shared Patch Repository

To install VMware vCenter Update Manager, download and enable the plug-in for VMware vSphere Client. Please see the Update Manager Installation and Administrator guides.

**Use Case:** Patching a cluster of ESX hosts with critical host patches

VMware vCenter Update Manager provides a simple way of ensuring cluster-wide patch compliance. Update Manager patches one host at a time in the cluster using VMotion to migrate virtual machines away from the host that it is patching to other hosts in the cluster.

### 2.8.1. VMware Differentiators

VMware Update Manager is a unique VMware solution. Update Manager is fully integrated with vCenter, it is very easy to set up, and provides a high degree of automation that dramatically reduces application downtime and time spent on software patching.

- **Update Manager is a fully integrated module of VMware vCenter Server. It does not require a complex installation or additional infrastructure.**

  Microsoft's System Center Virtualization Machine Manager (SCVMM) does not have integrated patching capabilities for virtual environments. To obtain any patching capability, users must purchase and install System Center Configuration Manager (SCCM), which requires dedicated infrastructure, is complex to install, and uses a separate UI. In contrast, VMware Update Manager is a simple plug-in module for vCenter that can be rapidly installed, does not require additional infrastructure (beyond what already in use for vCenter), and can be accessed directly from the vSphere Client. VMware Update Manager is included even in the most basic bundle of VMware vSphere. Citrix XenServer only provides a patch tracking system that reports on the latest patch applied to a virtual machine. Users must manually keep track of patch availability, manually download patches and install them.

- **Only VMware supports automated patching of offline virtual machines directly out-of-the-box.**

  Neither Microsoft SCCM nor Citrix XenCenter support patching of offline or suspended virtual machines. On March 18th 2008, Microsoft released a 76-page technical note that describes a work-around methodology to perform automated patching of offline virtual machines using SCCM. Aside from considerable limitations (i.e., it can be used only on virtual machines in the SCVMM library and does not support suspended virtual machines), the technical paper clearly shows the complexity that users will have to face with Microsoft's solution. The proposed work-around makes extensive use of custom scripts and will probably require months of testing. On the other hand, VMware Update Manager offline patching capabilities are fully integrated and require no additional setup.

- **VMware Updated Manager is fully integrated with Maintenance Mode and VMware DRS to perform non-disruptive zero-downtime hypervisor patching directly out-of-the-box.**

  In contrast, Microsoft System Center Configuration Manager is a separate non-integrated tool with System Center Operations Manager and Virtual Machine Manager. Configuration Manager cannot take advantage of features like Maintenance Mode or PRO Tips out of the box, making Hyper-V updates a more cumbersome and manual process.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **UPDATE MANAGER** | | | |
| Installed as a plug-in to the management interface | Yes | No (requires Configuration Manager) | No |
| Automated Remediation—Patches hosts, Microsoft and Linux virtual machines, virtual appliances, virtual machine hardware and select applications | Yes (can also patch VMware Tools) | No | No |
| Offline Virtual Machine Patching—Scans and patches offline virtual machines for increased security | Yes | No (separate custom solution) | No |
| Non-disruptive Automated Patching of Virtualization Hosts—Integrated with maintenance mode and dynamic resource allocation for zero downtime host patching and dynamic re-allocation of resources | Yes (integrated with DRS and maintenance mode) | No (not integrated with PRO Tips) | No (not integrated with dynamic load balancing) |
| Orchestrated Upgrades—Use a host upgrade baseline to perform remediation at a cluster, folder, or datacenter level. A virtual machine upgrade baseline can also be used to upgrade virtual machine hardware and VMware Tools at once. | Yes | No | No |

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| UPDATE MANAGER | | | |
| Patch Staging and Scheduling Remote Sites—Download patches from a remote server to a local server without applying the patches immediately | Yes | No | No |
| Support for Multiple Baselines—Scans and remediates an inventory object against multiple baseline groups (set of upgrades and patches) | Yes | No | No |
| Patch Rollback—Allows reverting back to the state prior to a patch/upgrade to reduce the risk of virtual machine patching failures, by automatically taking a snapshot of the virtual machine state prior to applying a patch | Yes | No | No |
| Compliance Dashboard—Provides visibility into the patch status of hosts and virtual machines and automated scanning of servers in the data center for compliance to static or dynamic baselines. | Yes | No | No |
| Virtual Appliance Upgrades—Allows administrators to create pre-defined baselines to scan and upgrade a virtual appliance to the latest released or latest critical virtual appliance version | Yes | No | No |
| Integration with Power CLI—Allows administrators to use PowerShell commands to automate patch management directly from a command line | Yes | Yes (in Configuration Manager) | No |

### 2.8.2 Update Manager Hands-on Review

| | | | |
|---|---|---|---|
| Maintenance | Update Manager | 2.8 Using Update Manager to automate ESX host and virtual machine patching and remediation<br><br>Patching a cluster of ESX hosts with critical host patches<br><br>1. Attaching a Critical Host Patches Baseline to the cluster<br>2. Scanning the cluster for critical patch vulnerabilities<br>3. (Optional) Staging patches<br>4. Remediating the cluster with critical patches | Varies depending on number of patches |
| | | Orchestrated upgrade of datacenter to ESX 4.0<br>Upgrading an ESX 3.5 host to ESX 4.0<br><br>Upgrading VMware Tools and VM hardware<br><br>1. Attaching Tools upgrade Baseline group to the VM<br>2. Scanning the VM for VMware Tools and VM hardware upgrade compliance<br>3. Remediating the VM with VMware Tools and VM hardware upgrades | 60 minutes per host |
| | | Configuring Update Manager to use a central shared Patch Repository<br><br>1. Modifying Update Manager settings using vSphere Client | 10 minutes to configure Update Manager. Time to setup patch repository varies depending on the number and size of patches |

**Step 1: Attaching a Critical Host Patches Baseline to the cluster**

1. In your vSphere client, click the **Inventory** navigation button and select **Hosts and Clusters**.
2. Select a cluster from your inventory. In this guide, a cluster containing one ESX 4.0 host and one VMware ESXi 4.0 host has been selected. Click the **Update Manager** tab.
3. Click **Attach** to launch the Attach Baseline or Group window.
4. Select **Critical Host Patches** under Patch Baselines. Click **Attach**. Update Manager attaches the baseline and the compliance status is now Unknown.

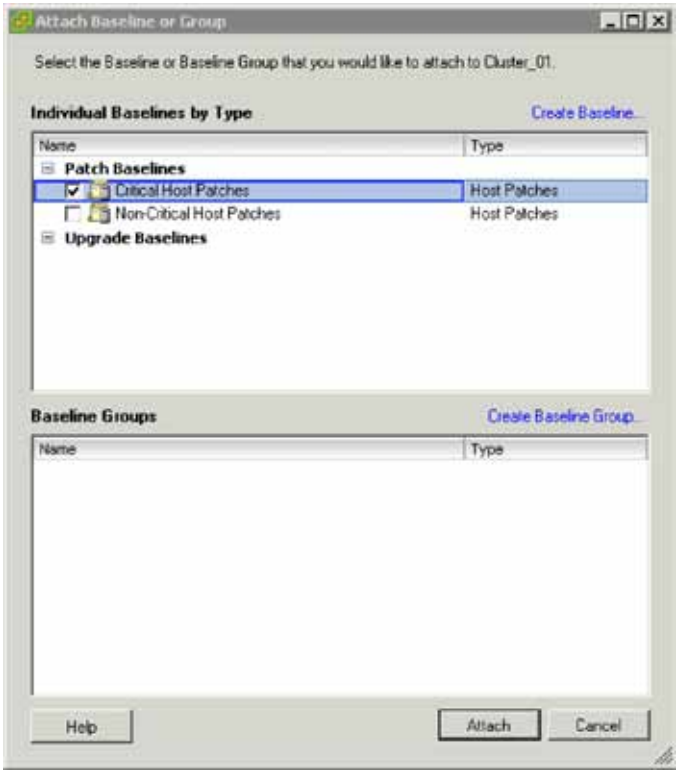



**Figure 2.8 a.** Attaching Critical Patches Baseline to Cluster

### Step 2: Scanning the cluster for critical patch vulnerabilities.

1. In your vSphere client, click the **Inventory** navigation button and select **Hosts and Clusters**.
2. Select the cluster that you previously selected and click the **Update Manager** tab.
3. Click **Scan** to launch the Confirm Scan window. Select **Patches**. Click **Scan**.
4. Update Manager runs a scan on the VMware ESXi 4.0 host and displays the compliance report. This task shows up in the Recent Tasks pane of the vSphere Client.

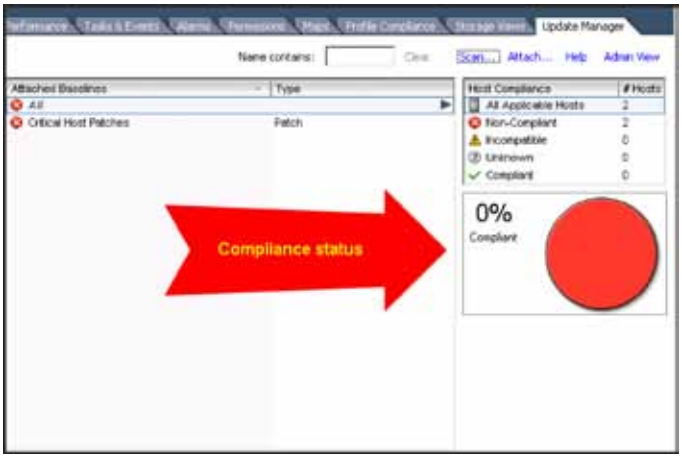



**Figure 2.8 b.** Compliance report after scan on a cluster. The report shows that the hosts are missing critical host patches and that the cluster is 0% compliant.

**Step 3: (Optional) Staging patches**

VMware vCenter Update Manager can optionally stage patches to the ESX hosts before applying them. This saves time downloading patches during the remediation phase.

1. In your vSphere client, click the **Inventory** navigation button and select **Hosts and Clusters**.
2. Select the VMware ESXi 4.0 host that you previously selected and click the **Update Manager** tab.
3. Click **Stage**. Select the patches that you wish to stage. Click **Next**.
4. Review your selections and click **Finish**. VMware vCenter Update Manager stages the patches you selected. This task shows up in the Recent Tasks pane of the vSphere Client.

**Step 4: Remediating the cluster with critical patches**

VMware vCenter Update Manager remediates hosts by migrating virtual machines off hosts using VMotion and placing the hosts in maintenance mode.

- In your vSphere client, click the **Inventory** navigation button and select **Hosts and Clusters**.
- Select the cluster that you previously selected and click the **Update Manager** tab.
- Click **Remediate**. Ensure **Critical Host Patches** is selected in Baselines. Select the hosts that you wish to remediate. In this guide, one host has been selected to remediate. Click **Next**.
- De-select the patches you wish to exclude. For the purpose of this guide, apply all applicable patches. Click **Next**.
- Enter a **Task Name**. Enter a **Task Description** (Optional). Click **Next**.
- Review your selections. Click **Finish**. VMware vCenter Update Manager remediates the host with the patches you selected. This task shows up in the Recent Tasks pane of the vSphere Client.

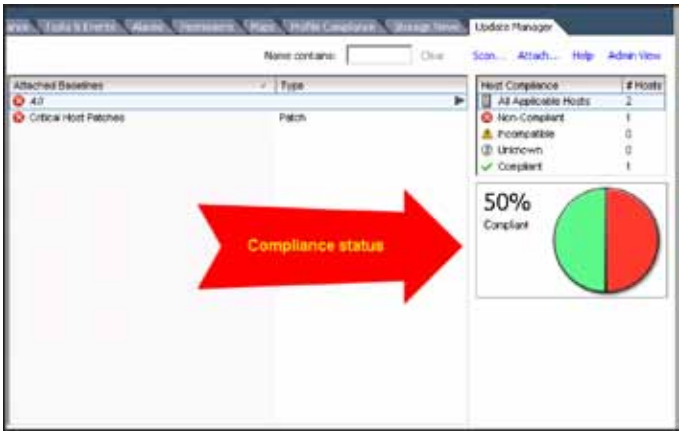



**Figure 2.8 c.** Compliance dashboard showing that the cluster is 50% compliant. One host in the cluster has been patched.

**Use Case:** Orchestrated upgrade of datacenter to ESX 4.0

VMware vCenter Update Manager provides a 2-step Orchestrated upgrade of your datacenter to ESX 4.0. The two steps are:

1. Upgrade ESX 3.5 hosts to ESX 4.0
2. Upgrade virtual machine VMware Tools and VM hardware to ESX 4.0

In this guide, you will walk through upgrading the virtual machines VMware Tools and VM hardware upgrade only.

*Upgrading an ESX 3.5 host to ESX 4.0*
VMware vCenter Update Manager provides pre-defined baselines to upgrade ESX 3.5 hosts to ESX 4.0. VMware vCenter Update Manager will put the hosts into maintenance mode and perform the upgrade. You will need the ESX 4.0 DVD ISO and the VMware ESXi 4.0 zip file as a prerequisite for this use case.

Please use the instructions in the VMware vSphere Migration Guide to upgrade ESX 3.5 hosts to ESX 4.0 using Update Manager.

*Upgrading VMware Tools and VM hardware*
VMware vCenter Update Manager provides pre-defined baselines to scan virtual machines for the latest VMware Tools and virtual machine hardware versions. You can view the compliance status of the virtual machines against these baselines and perform VMware Tools and virtual machine hardware upgrades on a folder, cluster, datacenter, or individual virtual machines.

Updates for virtual machines can be managed from the Virtual Machines and Templates inventory view.

**Step 1: Attaching Tools upgrade Baseline group to the VM**

1. In your vSphere client, click the **Inventory** navigation button and select **VMs and Templates**.
2. Select a virtual machine from the inventory and click the **Update Manager** tab.
3. Click **Attach** to launch the Attach Baseline or Group window.
4. Check the **VMware Tools Upgrade to Match Host** and **VM Hardware Upgrade to Match Host** boxes under Upgrade Baselines in the **Individual Baselines by Type** section. Click **Attach**. Update Manager attaches the baselines and the compliance status is now Unknown.

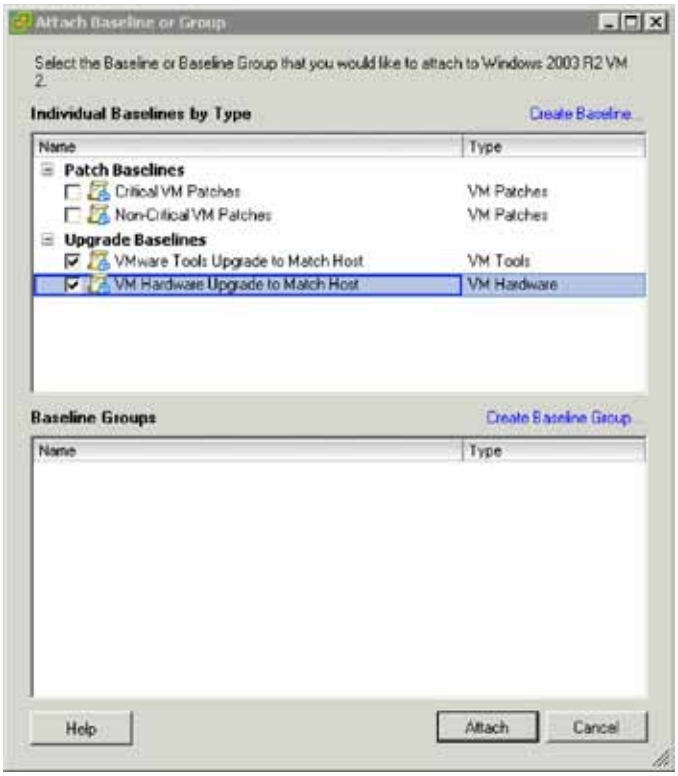



**Figure 2.8 d.** Attaching Tools Upgrade Baseline to a Virtual Machine

**Step 2: Scanning the VM for VMware Tools and VM hardware upgrade compliance**

1. In your vSphere client, click the **Inventory** navigation button and select **VMs and Templates**.
2. Select the virtual machine from the inventory and click the **Update Manager** tab.
3. Click **Scan**. Ensure that **VM Hardware upgrades** and **VMware Tools upgrades** are checked. Click **Scan**.
4. VMware vCenter Update Manager scans the virtual machine you selected. This task shows up in the Recent Tasks pane of the vSphere client.

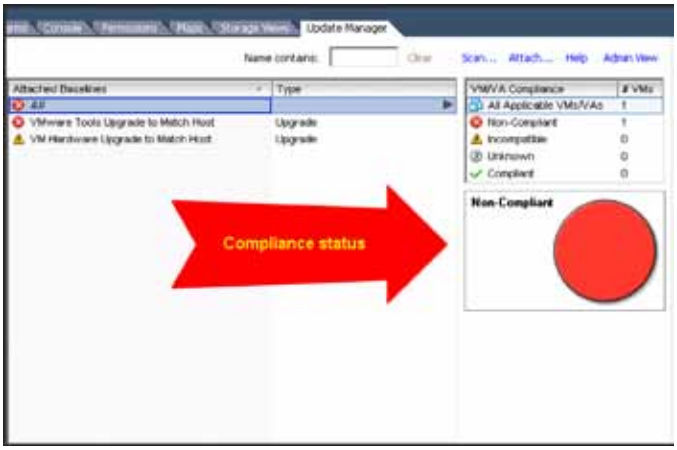



**Figure 2.8 e.** Compliance report scanning a virtual machine for VMware Tools and VM Hardware upgrades

**Step 3: Remediating the VM with VMware Tools and VM hardware upgrades.**

VM Hardware upgrades require up-to-date VMware Tools. First, you will upgrade the VMware Tools to match the host and then proceed to upgrade the VM Hardware.

*Upgrading VMware Tools to Match the Host*

1. In your vSphere client, click the **Inventory** navigation button and select **VMs and Templates**.
2. Select the virtual machine from the inventory and click the **Update Manager** tab.
3. Click **Remediate**. Select **VMware Tools Upgrade to Match Host**. Click **Next**.
4. Enter a **Task Name**.
5. (Optional) Enter a **Task Description**. Click **Next**.
6. (Optional) Enter **Snapshot Details**. Click **Next**.
7. Review the remediation options and click **Finish**.

*Upgrading VM Hardware to Match the Host*

1. In your vSphere client, click the **Inventory** navigation button and select **VMs and Templates**.
2. Select the virtual machine from the inventory and click the **Update Manager** tab.
3. Click **Remediate**. Select **VM Hardware Upgrade to Match Host**. Click **Next**.
4. Enter a **Task Name**.
5. (Optional) Enter a **Task Description**. Click **Next**.
6. (Optional) Enter **Snapshot Details**. Click **Next**. It is recommended that you keep snapshots around for as long as it takes to perform User Acceptance Tests on the upgraded VM. This will allow you to revert back to the older VM hardware version if necessary.

7. Review the remediation options and click **Finish**.

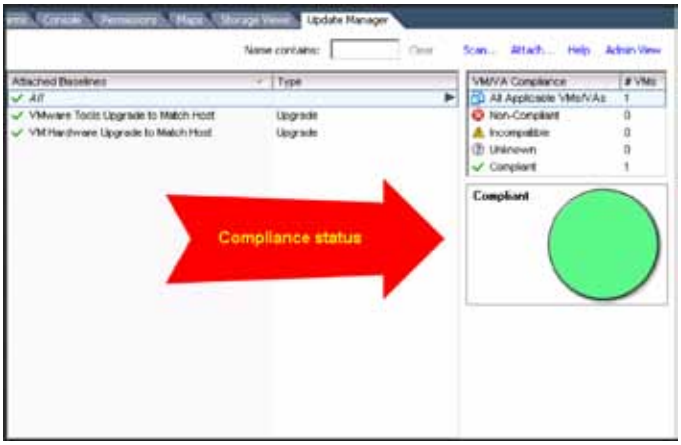



**Figure 2.8 f.** Compliance report after upgrading VMware Tools and VM Hardware for the virtual machine.

**Use Case:** Configuring Update Manager to use a central shared Patch Repository

Update Manager Download Service (UMDS) is an optional module that provides administrators the ability to download patch metadata and patch binaries in case the Update Manager server is not connected to the Internet for security or deployment restrictions. The UMDS can also be used as a central patch repository that can be shared by multiple instances of Update Manager servers.

Update Manager Download Service needs to be installed on a computer that has Internet access. It can be set up as a Web server that's URL can be specified in the Update Manager configuration interface as the shared repository URL.

Please access the Update Manager Administration Guide for instructions on how to set up Update Manager Download Server and export the patch metadata and patch binaries to a server.

In this guide, you will walk through how to configure your Update Manager instance to connect to a shared patch repository that has already been set up.

*Modifying Update Manager Settings Using vSphere Client*

1. In your vSphere client, click **View, Solutions and Applications**, and **Update Manager**. This opens the Admin View for Update Manager.
2. Click the **Configuration** tab.
3. Click **Patch Download Settings** in Settings.

4. Click **Use a Shared Repository** and type in the address of the share. Click **Apply**.

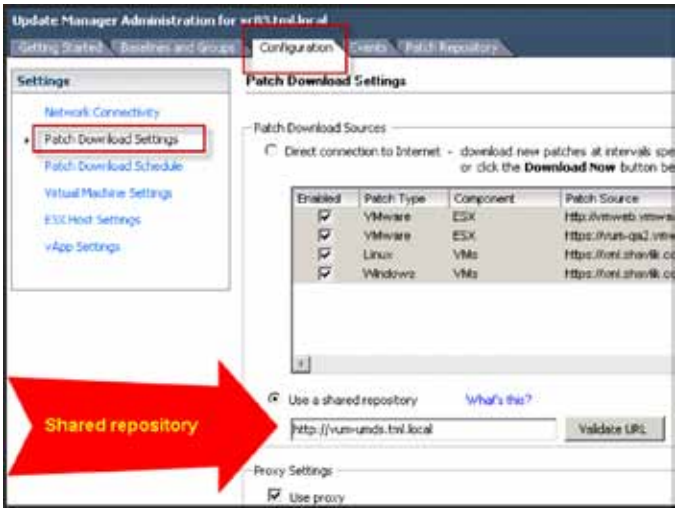



**Figure 2.8 g.** Configuring Update Manager to Use a Shared Repository of Patches

# Section 3: Medium- to Large-Scale, Multi-Site Deployments

## 3.1. Linked Mode

What is it: The Linked Mode feature provides a way to greatly improve the efficiency of managing multiple vCenter instances. After you form a Linked Mode group, you can log in with the vSphere Client to any single instance of vCenter and view and manage the inventories of all the vCenter Servers in the group. Figure 3.1 a. gives an example of what this looks like in the vSphere Client. The left-side inventory tree shows each vCenter instance at the top level, and for each lower level it shows the datastores, folders, clusters, hosts, etc. From this single inventory tree, an administrator can see the inventory of all vCenter instances at once. Using the +/- indicator, the inventory for any vCenter instance can be collapsed, making it easier to focus on a smaller set of items.

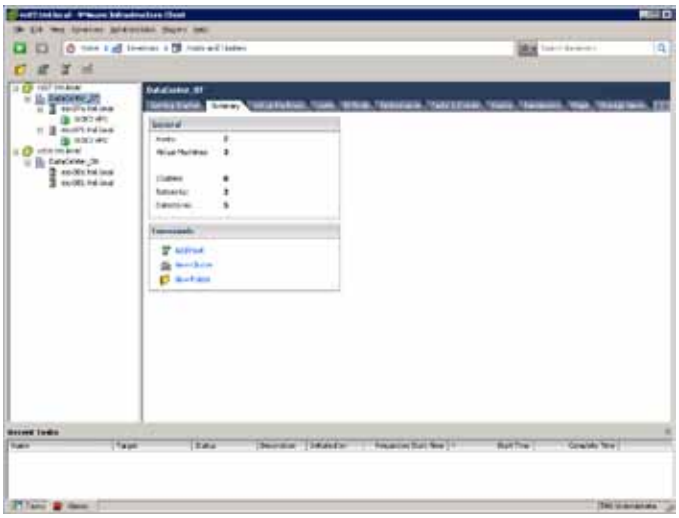


**Figure 3.1 a.** View of 2 linked vCenters in vSphere Client

During or after vCenter installation, you can join multiple vCenter machines into a Linked Mode group. When vCenter Servers are connected in Linked Mode, you can:

- Log in simultaneously to all vCenter Servers for which you have valid credentials.
- Search the inventories of all the vCenter Servers in the group.
- View the inventories of all the vCenter Servers in the group in a single inventory view.

Using peer-to-peer networking, the vCenter instances in a group replicate shared global data to the LDAP directory. The global data includes the following information for each vCenter instance:

- Connection information (IP and ports)
- Certificates and thumbprints
- Licensing information
- User roles

A vCenter instance can be joined to a Linked Mode group at the time of installation, or afterwards by modifying an existing deployment. Both of these methods are described in the ESX and vCenter Server Installation Guide.

Although you are able to view multiple vCenter inventories in one client, any operations are confined within a single vCenter inventory. For example, you cannot drag and drop a host between vCenter instances, nor a virtual machine between hosts on two different vCenter instances.

**Use Case:** Automatic Role Replication across vCenter instances

### 3.1.1. VMware Differentiators

Manage multiple vSphere datacenters from a single console with vCenter Linked Mode.

- Linked Mode allows a single vSphere Client to view, search, and manage data across multiple vCenter Server systems.
- A single vCenter Server can scale to support up to 300 vSphere hosts and 3,000 VMs. Linked Mode multiplies those limits to enable single-pane-of-glass management of truly huge vSphere deployments.
- Linked Mode uses a common directory of global vCenter Server data to permit sharing of administrative user roles and licenses across all linked vSphere datacenters.
- Linked Mode accommodates customized permissions ranging from limited access on just a single vCenter Server to global administrator access to every vSphere object in a Linked Mode group.
- Microsoft requires System Center Virtual Machine Manager to manage multiple Hyper-V hosts, but multiple SCVMM servers cannot be linked.
- Citrix XenCenter can manage multiple XenServer resource pools, but those pools are limited to just 16 hosts. All XenCenter users have full root-level access to every XenServer host, which is highly objectionable to any security-conscious enterprise. The Citrix Essentials Lab Manager component provides access controls only when users access VMs and not when XenServer hosts are accessed.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **VCENTER LINKED MODE** | | | |
| Single-pane-of-glass View of Entire Virtual Inventory—From a single vSphere Client, every vSphere VM and host managed by multiple vCenter Servers in a Linked Mode group can be controlled and object searched across the group | Yes | No, cannot link multiple SCVMM servers in a single console view | Limited, XenCenter can manage multiple XenServer resource pools, but pools limited to just 16 hosts |
| Global User Permissions—Each vSphere Client can access only the vCenter Server instances and objects on which they have valid permissions | Yes | Yes, requires trusted domains if SCVMM server are on multiple AD domains | No, all XenCenter users get full access to all managed XenServer hosts |
| Common Directory Spanning All Hosts—vCenter Linked Mode uses an LDAP directory for sharing of user roles and licenses across all vCenter Server in a Linked Mode group, even spanning Active Directory domains | Yes | Limited, special "Perimeter Host" process required to add hosts in different AD domain | No |

### 3.1.2. Linked Mode Hands-on Review

| | | | |
|---|---|---|---|
| Infrastructure Setup | Linked Mode | 3.1 Automatic Role Replication across vCenter instances and performing cross vCenter tasks<br>Automatic Role Replication across vCenter instances<br><br>1. Create a custom role<br>2. Grant role to user or group<br>3. Verify replication<br><br>Performing cross vCenter tasks<br>1. Remediate VMs with out of date VMware Tools<br>2. Identify Datastores with low free space | 20 minutes |

To demonstrate the functionality of Linked Mode, you can create a custom role on one vCenter instance, and then observe how it appears on the second one. The following steps walk you through this process.

**Step 1: Create a custom role**

1. Select one of the vCenter instances in the vSphere client and then click on the **Home** icon. This will display the main tasks page.

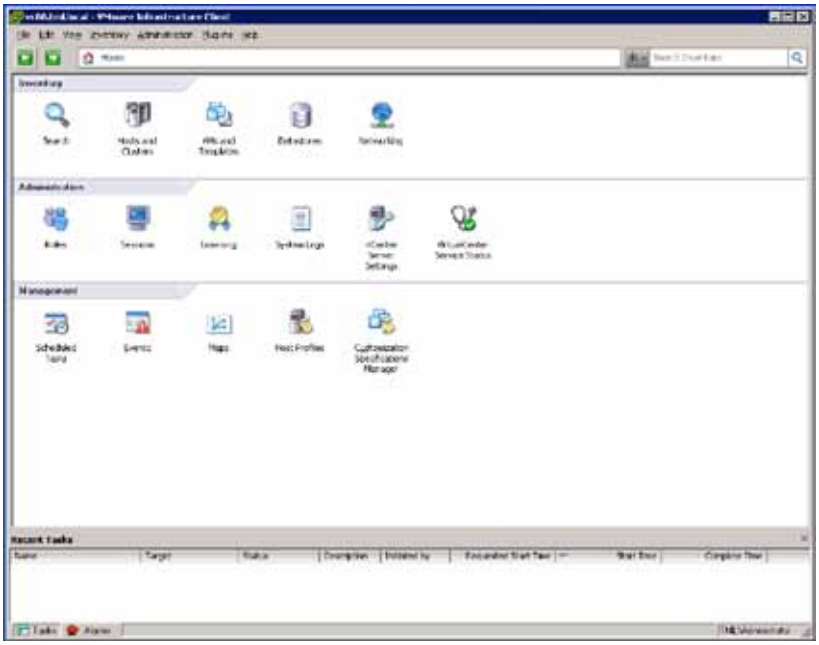


**Figure 3.1 b.** Home Screen

2. Click on **Roles** to take you to the Roles management screen. Then click on **Add Role**. Create a role with some arbitrary set of privileges selected (it does not matter which privileges are selected for this demonstration). The new role will appear in the list of roles on the left side of the screen.

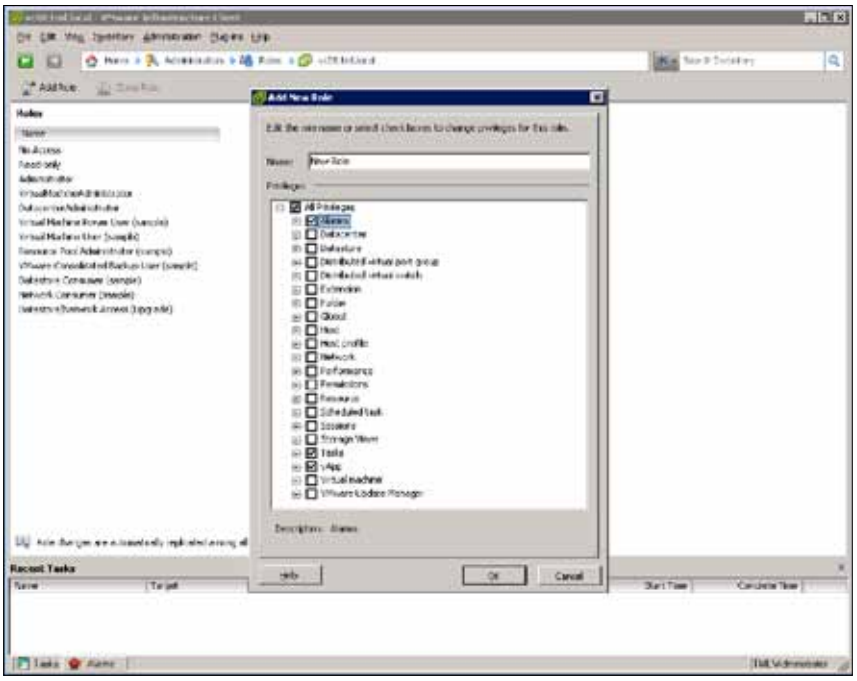


**Figure 3.1 c.** Creating a New Role

### Step 2: Grant this role to a user or group

Grant this newly created role to a user or group in your environment. For details on how to do this, please see the vSphere Basic System Administration Guide. After you have completed this step, navigate back to the Roles management screen, and confirm that these users or groups appear when you highlight this role.

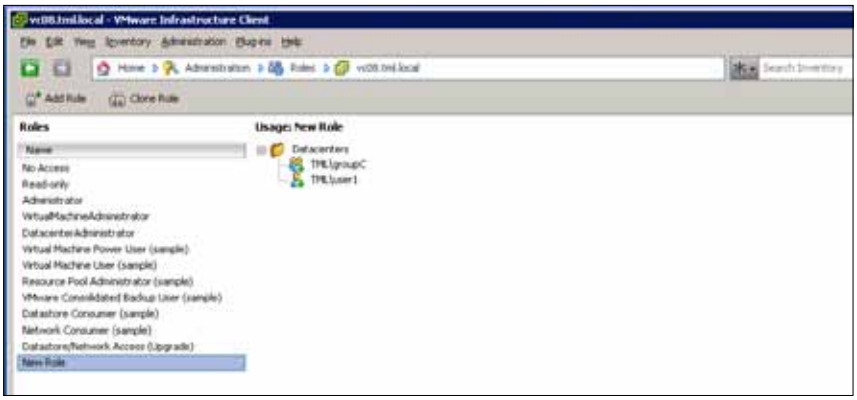



**Figure 3.1 d.** New Role With User Assignment

### Step 3: Verify Replication

From the dropdown in the upper navigation bar, select the other vCenter instance. Within a few minutes, the role you created will be visible there.

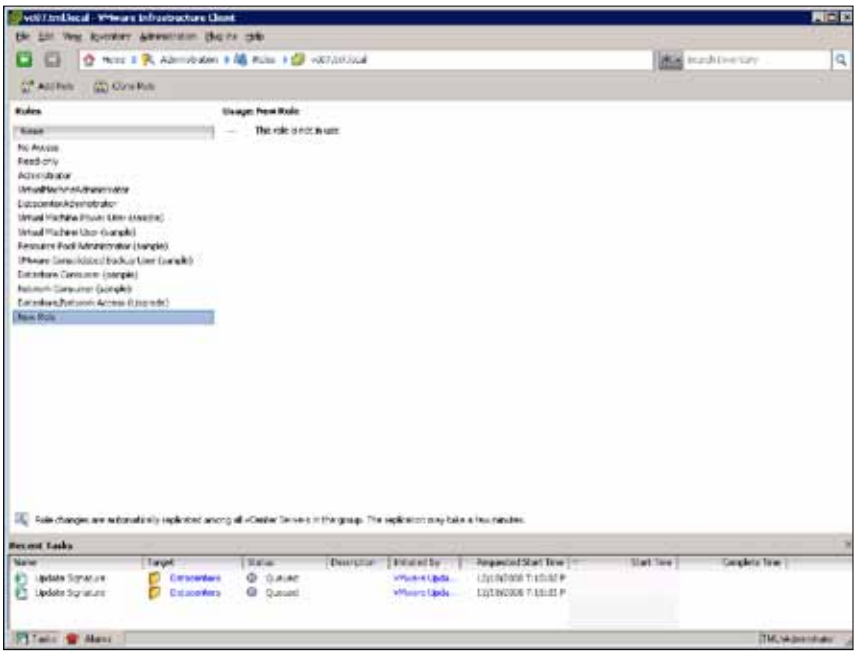


**Figure 3.1 e.** New Role Without User Assignment

You will notice that it shows the role as not in use. This is because only the Roles definition is replicated between vCenter instances; the actual roles assignment is still maintained independently on each vCenter. This allows you to define a global set of roles, but have different sets of people responsible for different vCenter instances.

### Performing Cross vCenter Tasks

The vSphere Client allows you to search your VMware Infrastructure inventory for virtual machines, hosts, datastores, or networks that match specified criteria. If the vSphere Client is connected to a vCenter server that is part of a connected group, you can search the inventories of all vCenter servers in that group.

You can perform basic searches by entering information in the search field in the upper right corner of the vSphere client and selecting object type from the dropdown menu. You can also perform advanced searches with multiple criteria by selecting the **Search** task from the Home screen.

The results from searches done in your environment depend upon the details of your setup. Here are examples based upon the setup shown earlier in Figure 3.1 a.

The following shows an example of searching for a VM that contains the string "W2K" in its name.

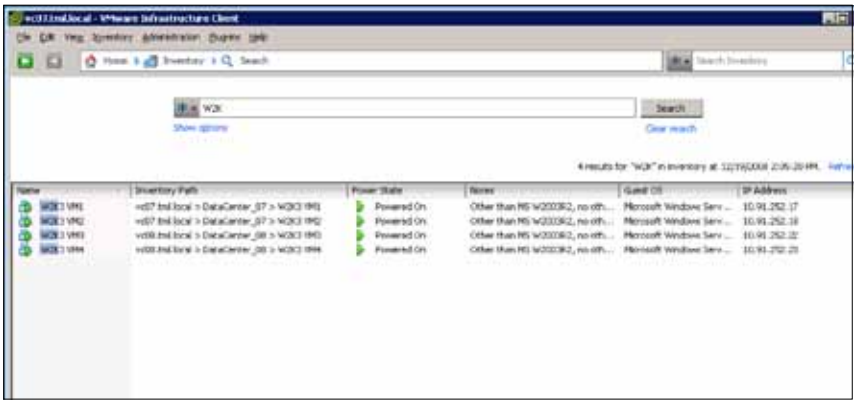


**Figure 3.1 f.** VM Search Result

The list of search results provides a context-sensitive menu when you right click on an item. This allows for useful workflows to be implemented from within a search, as shown in the following examples.

**Use Case:** Remediate VMs with out of date VMware Tools

The following example shows how to upgrade VMware Tools on running guests of a particular operating system type.

**Step 1: Configure search with the appropriate criteria**
Below you can see how to configure a search to return all virtual machines with the following criteria:

- Guest OS containing the string 2003, to match "Windows Server 2003"
- VMware Tools out-of-date (from the latest version)
- Currently running

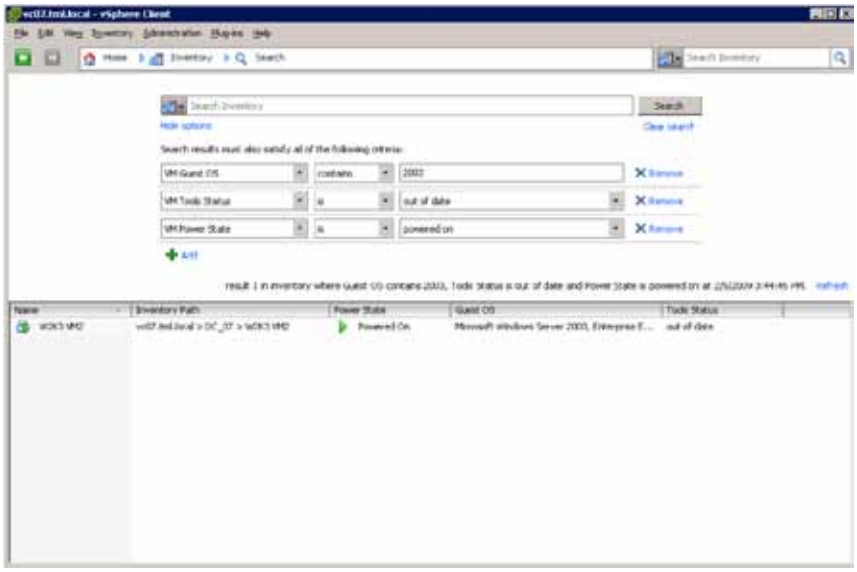


**Figure 3.1 g.** VM With Out of Date VMware Tools

### Step 2: Remediate VMs

Right-click the result to see the virtual machine context menu, and select **Guest** > **Install/Upgrade VMware Tools**.

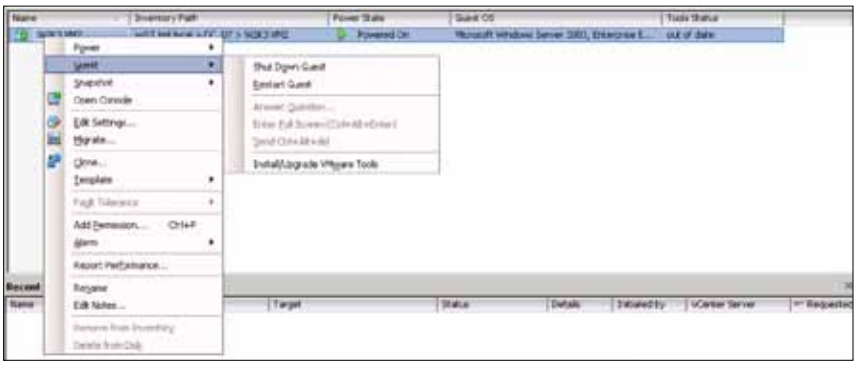


**Figure 3.1 h.** Updating Tools Within Search Result

**Use Case:** Identify Datastores with low free space

The following example shows how to list all datastores that are low on free space, allowing the administrator to browse each one to investigate further.

1. Right-click on a datastore to open the menu and select **Browse Datastore...**

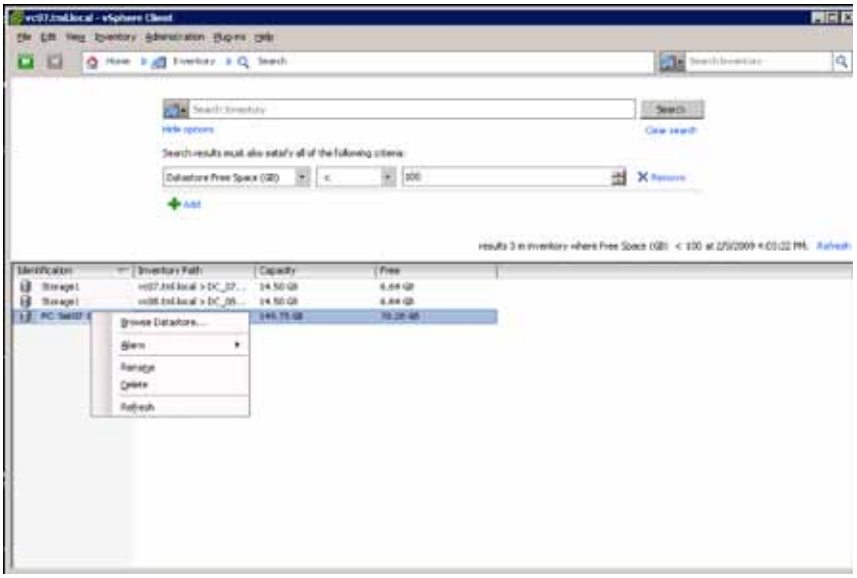


**Figure 3.1 i.** Datastores With Low Free Space

## 3.2. vNetwork Distributed Switch (vDS)

**What it is:** A VMware vNetwork Distributed Switch simplifies virtual machine networking by enabling you to set up virtual machine networking for your entire datacenter from a centralized interface. A single vNetwork Distributed Switch spans many ESX hosts and aggregates networking to a centralized datacenter level. A vNetwork Distributed Switch abstracts the configuration of individual virtual switches and enables centralized provisioning, administration and monitoring through VMware vCenter Server.

**Use Case:** Migrating from a Standard Switch to a vNetwork Distributed Switch

### 3.2.1. VMware Differentiators

The vNetwork Distributed Switch (vDS) simplifies management of a virtualized network infrastructure.

- **Only VMware vSphere offers the operational efficiencies of a distributed virtual switch.**
- A vDS acts as a single vSwitch across all associated hosts in a datacenter allowing virtual machines to maintain consistent network configurations as they migrate between hosts.
- With a vDS, administrators no longer need to manually configure hosts with identical network settings to ensure successful VMotions.
- A vDS enables *Network VMotion* where the state of a VM's network ports follow it as it is VMotioned between hosts. Port state includes settings for VLANs and private VLANs, bidirectional traffic shaping and NIC teaming as well as network performance counters.
- The vDS is the basis for the optional Cisco Nexus 1000V, which provides vSphere with an extended Cisco Nexus/Catalyst feature set plus the familiar IOS interface. With the Nexus 1000V, it's easy for network administrators familiar with Cisco environments to manage a virtualized net work infrastructure.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **VNETWORK DISTRIBUTED SWITCH** | | | |
| Distributed Virtual Switch—Virtual switch and its port configurations span multiple hosts. No need to manually configure virtual switches for compatibility with migrated VMs. | Yes | No | No |
| Network VMotion—Consistent network settings are presented to migrated VMs. Port state and performance counters migrate with VMs. | Yes | No | No |
| Supports Third-Party Virtual Switches—Network switch vendors can implement a distributed switch presenting their proprietary features and management interfaces | Yes, Cisco Nexus 1000V | No | No |

### 3.2.2. vDS Hands-on Review

| | | | |
|---|---|---|---|
| Infrastructure Setup | vNetwork Distributed Switch | 3.2 Migrate from Standard Switch to a vNetwork Distributed Switch<br><br>Per Host Manual Migration to vDS<br><br>1. Create vDS<br>2. Create DV Port Groups<br>3. Add host to vDS and migrate vmnics and virtual ports<br>4. Delete Standard Switch<br>5. Repeat Steps 3 & 4 for remaining Hosts<br><br>Configuration and Deployment of vDS using Host Profiles<br>1-4 Migrate Reference Host to vDS using Step 1-4 of Manual Migration<br>5. Create Host Profile of Reference Host<br>6. Attach and apply Host Profile to Candidate Hosts<br>7. Migrate VM Networking to vDS | 90 minutes |

You will use two methods for migrating a four-host Standard Switch environment to a vNetwork Distributed Switch (vDS). Method one involves creating a vDS and the DV Port Groups, migrating the vmnics to the vDS, and then migrating the VM networks and virtual ports. Method two leverages this first host migration in creating a host profile for migrating a large number of hosts.

This section covers the following:

1. Creation of a vNetwork Distributed Switch (vDS)
2. Migration of resources from the Standard Switch to the vDS. i.e. vmnics, VMs using:
   a. Per Host Manual Migration
   b. Host Profiles
3. Using the vDS
4. Creating and using Private VLANs
5. Basic Network Troubleshooting using the vDS

*Configuration of Example Evaluation Environment*
The example evaluation environment shown in the following sections is comprised of the following:

1. Single vSphere Data Center (Datacenter_09)
2. Two ESX 4 Servers (esx09a.tml.local; esx10a.tml.local)
3. Two VMware ESXi 4 Servers (esx09b.tml.local; esx10b.tml.local)
4. Eight Virtual Machines (Microsoft Windows XP) with single vnic attachment to the vSwitch
5. Three VM networks (VM01; VM02; VM02)

The starting host inventory and virtual switch configuration from one of the ESX hosts is shown here:

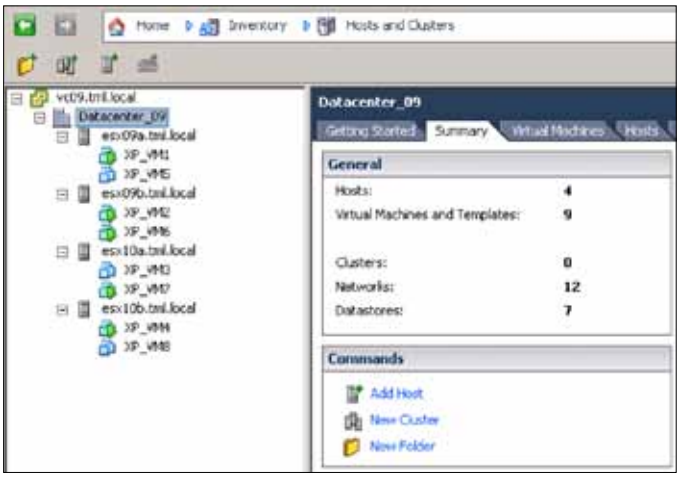



**Figure 3.2 a.** Example Host Inventory from vSphere Client

Each ESX and VMware ESXi server is configured in the default environment with Port Groups on Standard Switches as follows:

1. Three Port Groups for Virtual Machines
   - VM01—configured on VLAN 2936
   - VM02—configured on VLAN 2937
   - VM03—configured on VLAN 2999
2. Port Group for VMotion
   - VMotion01—configured on VLAN 2933
3. Port Group for iSCSI
   - iSCSI01—configured on VLAN 2934
4. Port Group for Fault Tolerance
   - FT01—configured on VLAN 2935

VMware ESX uses the Service Console (SC) for management whereas VMware ESXi servers use a VMkernel port for management. The VMware ESX hosts (esx09a and esx10a) use a Service Console port configured on VLAN 1 (no VLAN listed in Port Group definition) and the VMware ESXi servers (esx09b and esx10b) use a VMkernel port (vmk3) also configured on VLAN 1. (Please note: using VLAN 1 for management or any other purpose is not a networking best practice).

Refer to Figure 3.2 a. and Figure 3.2 b. for how the Port Groups are named and annotated for VLANs.

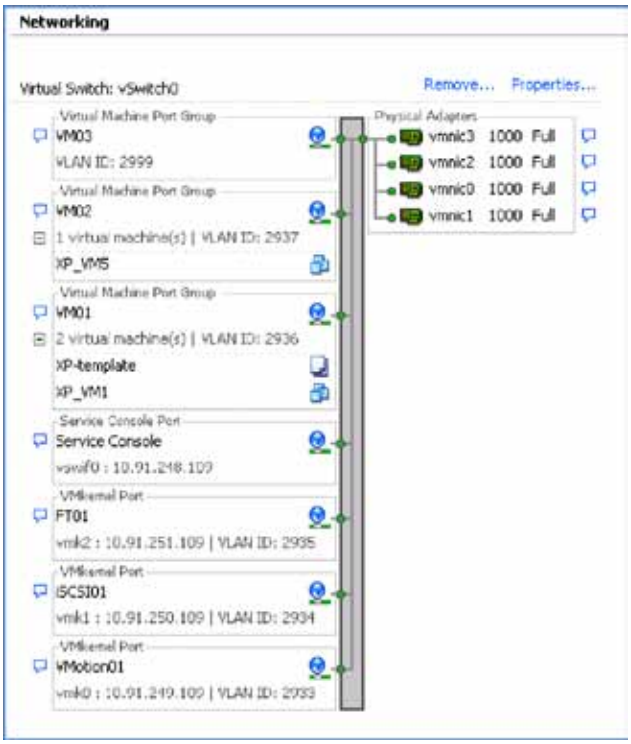



**Figure 3.2 b.** Starting Example Standard Switch Configuration for VMware ESX


**Figure 3.2 c.** Starting Example Standard Switch Configuration for VMware ESXi Server

*NIC Teaming Configuration*

In this example server configuration, the original standard switch, Port Groups, and physical adapters are configured in a common and close to best practice design.

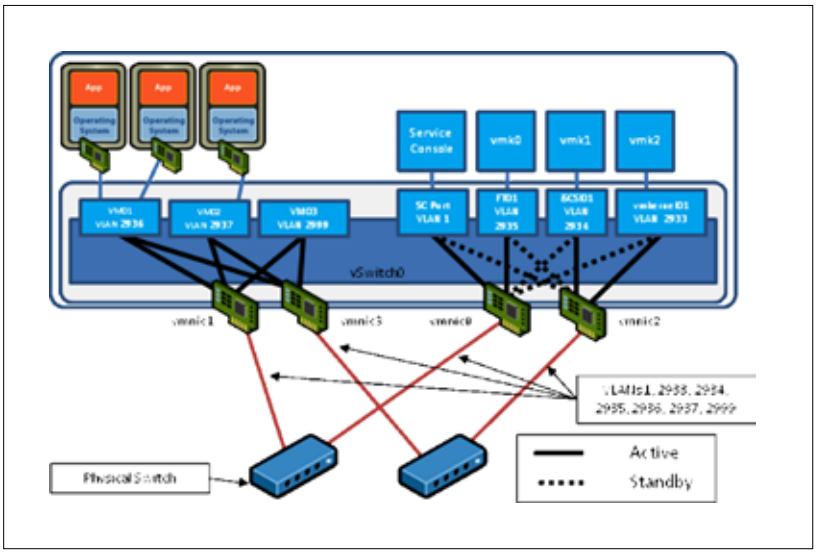



**Figure 3.2 d.** Example VMware ESX Showing NIC Teaming Configuration

1. All four vmnics are associated with a single standard switch (vswitch0) with policy overrides on each of the Port Group definitions.
2. The Virtual Machine Port Groups (VM01, VM02, VM03) are configured to override the vswitch settings and use:
   - "Route Based on the Originating Virtual Port ID" for the NIC Teaming load balancing policy
   - vmnic1 and vmnic3 as the "Active Adapters" (vmnic0 and vmnic2 are "Unused Adapters")
3. The Service Console (or vmkernel management port on VMware ESXi) and the FT01 Port Group are configured to:
   - "Use Explicit failover order" for the NIC Teaming Load Balancing policy
   - vmnic0 as the Active Adapter and vmnic2 as the Standby Adapter
4. The iSCSI01 and VMkernel01 Port Groups are configured to:
   - "Use Explicit failover order" for the NIC Teaming Load Balancing policy
   - vmnic2 as the Active adapter and vmnic0 as the Standby Adapter

You can see from the teaming configuration that each Port Group has two vmnics associated in either an "Originating Virtual Port ID" policy or "Explicit Failover Order." If one (and one only) vmnic was removed from each of these teams, connectivity would be maintained through the remaining vmnic.

*VLAN Assignment*
VLANs are assigned as shown Table 3. You will use these VLAN assignments, Port Group names, and Distributed Virtual Port Group names throughout the network section.

| PORT GROUP NAME | DISTRIBUTED VIRTUAL PORT GROUP NAME | VLAN |
|---|---|---|
| VM01 | dv-VM01 | 2936 |
| VM02 | dv-VM02 | 2937 |
| VM03 | dv-VM03 | 2999 |
| FT01 | dv-FT01 | 2935 |
| iSCSI01 | dv-iSCSI01 | 2934 |
| VMotion01 | dv-VMotion01 | 2933 |
| Management Network (VMware ESXi)<br>Service Console (ESX) | dv-management | Native (none) |

**Table 3 -** Port Group to DV Port Group mappings

*Target Configuration*
Our target configuration is as follows:

- A single vDS spanning the four hosts (2x ESX; 2x VMware ESXi)
- Distributed Virtual Port Groups spanning the four hosts with the same VLAN mapping as original environment (refer to Table 3 above)

*Migrating to a vNetwork Distributed Switch*
Two methods are available for migrating to a vNetwork Distributed Switch:

1. Manual Migration. This offers more per host control over migration, but is a longer process. Hosts do not need to be in maintenance mode so VMs can be powered up during migration.
2. Host Profiles. This uses a reference host template and is the preferred method for bulk vDS migration and deployment. Host Profiles requires the target hosts to be in maintenance mode (i.e. VMs powered down).

These two methods are detailed in the following sections.

**Method 1:** Per Host Manual Migration to vDS

The objective in this part of the evaluation exercise is to completely migrate the current server environment running the standard switches to a vNetwork Distributed Switch. This migration includes all uplinks (also known as physical adapters, pnics, or vmnics), all Virtual Machine Port Groups, all VMkernel Ports, and Service Console Ports (for VMware ESX).

Considerations for vDS Migration

Keep the following points in mind when migrating to a vDS:

1. Uplinks (physical nics or vmnics) can only be associated with one virtual switch (standard switch or vDS) at any one time. In this example, you will migrate all four vmnics from the Standard Switch to the vDS in one step.

*Note: if you must maintain VM connectivity (i.e. no outage) during migration, then you will need to migrate a subset of vmnics from the Standard Switch to the vDS so both switches have network connectivity. You will then have to migrate the virtual machines; and then finally, migrate the remaining vmnics. Note the intermediate step is critical for maintain VM connectivity.*

2. You need to maintain a management connection to the server in order to perform any configuration tasks, i.e. Service Console on VMware ESX, and the vmkernel Management Port on VMware ESXi. Pay special attention to the management port in the migration.
3. If migrating a subset of vmnics rather than all at once, note the NIC teaming arrangement when selecting the vmnic migration order. The most critical is the SC or management port. If migrating an existing SC or management port, it must have a network path on the standard switch and also the vDS. Otherwise, you can risk losing connectivity with the ESX or VMware ESXi Server after migration.

*Creation and Migration Overview*

The steps involved in per host manual migration of an existing environment using Standard Switches to a vDS are as follows:

1. Create vDS (without any associated hosts).
2. Create Distributed Virtual Port Groups on vDS to match existing or required environment.
3. Add host to vDS and migrate vmnics to dvUplinks and Virtual Ports to DV Port Groups.
4. Delete Standard Switch from host.
5. Repeat Steps 3 and 4 for remaining hosts.

*Creation and Migration Process*

The following steps detail the migration of the four-server example evaluation environment from standard switches to a single vNetwork Distributed Switch.

*Note: Step-by-step instructions for creating a vDS are shown in the ESX 4.0 Configuration Guide and VMware ESXi 4.0 Configuration Guides.*

**Step 1: Create a vDS**

vNetwork Distributed Switches are created at the datacenter level in the vSphere environment. A datacenter is the primary container for inventory objects such as hosts and virtual machines. The starting point is shown below, from a vSphere Client attached to a vCenter Server. In this example environment, the Datacenter is labeled "DC_09".

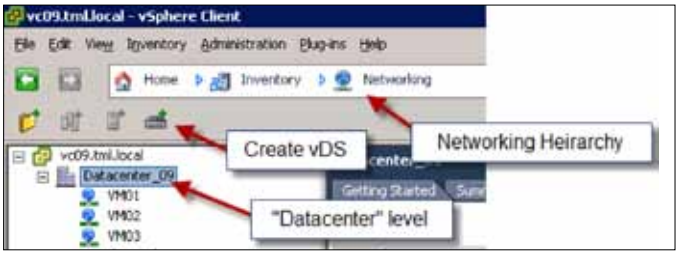



**Figure 3.2 e.** Starting Point in vSphere Client for Creating a vDS

After creating the vDS, the Networking Inventory panel will show a dvSwitch (the default name), and an Uplink Group for the uplinks (in this example, it was named dvswitch-DVUplinks-199). Note that both these new items can be renamed to conform to any local naming standards.

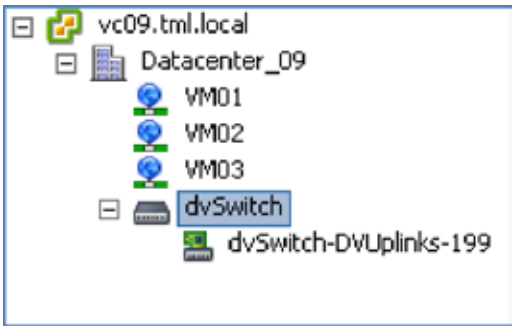



**Figure 3.2 f.** Networking Inventory After Creating a vDS

*What is an Uplink Group?*
An Uplink Group is a new feature with vDS. Much like a Port Group is a policy template for vnic attachment of VMs, vmkernel ports and service consoles, an Uplink Group is a policy template for the Uplinks on that vDS. Security policies, VLAN trunk ranges, traffic shaping, and teaming/failover settings can be set at this level for the entire vDS.

vDS uses dvUplinks to abstract the actual physical vmnics on each host. NIC teaming with vDS uses the abstracted dvUplinks, so it's important the underlying physical vmnic distribution matches what is desired with attachment to the adjacent physical switches. In this environment, you will want to preserve the same teaming arrangement, so you will manually choose the vmnic to dvUplinks assignments.

**Step 2: Create Distributed Virtual Port Groups on vDS to Match Existing or Required Environment**
In this step, you will create Distributed Virtual Port Groups on the vDS to match the existing environment and prepare the vDS for migration of the individual ports and Port Groups from the Standard Switches on each of the hosts.

*What is a Distributed Virtual Port Group?*
A Distributed Virtual Port Group on a vDS is similar to a conventional Port Group on a Standard Switch except that it can span multiple ESX and VMware ESXi Servers. Port Groups and Distributed Virtual Port Groups are port templates that define port policies for similarly configured ports for attachment to VMs, vmkernel ports and Service Console ports.

Port Groups and Distributed Virtual Port Groups define:

- VLAN membership
- Port security policies (promiscuous mode, MAC address changes, Forged Transmits)
- Traffic shaping policies (egress from VM)
- NIC teaming policies for load balancing, failover detection and failback

In addition to these features and functions, a Distributed Virtual Port Group also defines:

- Ingress (to VM) traffic shaping policies (enabling bi-directional traffic shaping)
- Port Blocking policy

*Port Group to DV Port Group Mappings*
In this sample environment, the same VLAN structure and allocation will be maintained as with the standard switch. To differentiate the DV Port Groups from the conventional Port Groups, they will be prefixed with "dv". Table 3 shows the mapping for port group names and corresponding VLAN associations.

*Note that in this example environment, the management traffic is untagged (meaning no VLAN tags) and as such uses the Native VLAN. By default with most physical switches, the Native VLAN is assigned to VLAN 1. Using the Native VLAN or VLAN 1 is not a best practice in many enterprises. A typical best practice network configuration would avoid use of VLAN 1 and the Native VLAN for all user and management traffic.*

*Creating the DV Port Groups*

1. From the Network Inventory view, select the vDS. This is labeled dvSwitch in the example environment. Then select **New Port Group...** This will bring up a "Create Distributed Virtual Port Group" panel.

The first panel in creating the dv-VM01 DV Port Group is shown below. Note the "Number of Ports." This defaults to 128 and is the number of ports that this DV port group will allow once created. As this DV Port Group will support VMs, it means up to 128 VMs can use this DV Port Group. Modify this to a higher number if you need to support more VMs within a single DV Port Group. In this example environment, 128 ports are quite adequate.

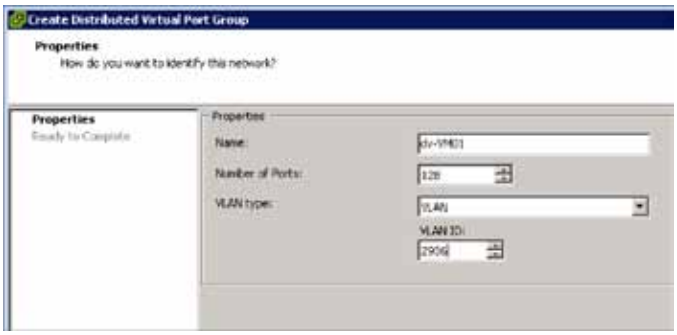



**Figure 3.2 g.** DV Port Creation

2. Continue creating the DV Port Groups according to the table. You will need to create DV Port Groups for each of the management and vmkernel ports as well.

After creating the DV Port Groups, the vDS panel should look like this:

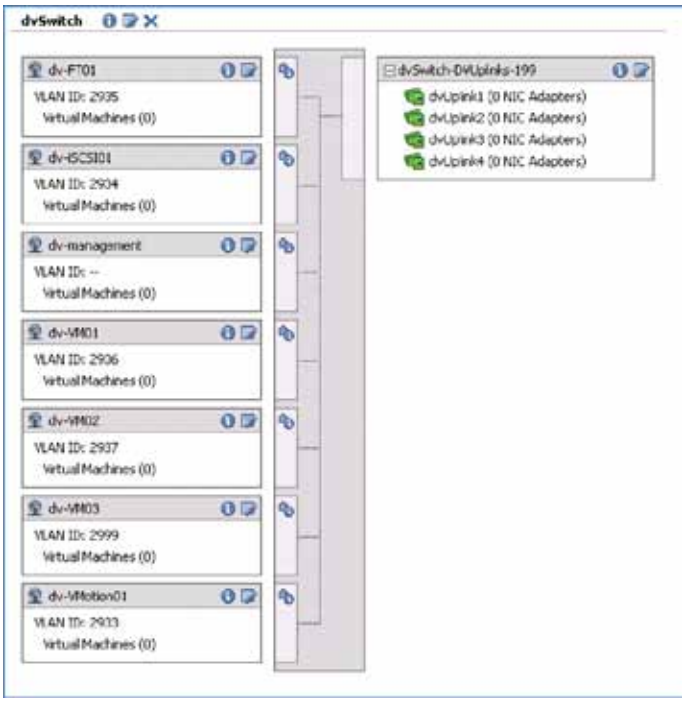



**Figure 3.2 h.** vDS After Creation of DV Port Groups

*Adjusting Distributed Virtual Port Groups Policies*

When creating the DV Port Groups above, only the VLAN number has been configured and not the NIC teaming policies. Each of the DV Port Groups is using the default NIC teaming assignments of Originating Virtual Port load balancing over all four dvUplinks. If you want to restore the NIC teaming policies used prior to the vDS migration (these are shown in Table 4), you need to edit each of the DV Port Group configurations.

Table 4 details the policies used in this example evaluation environment. These are the same policies used with the Standard Switches. See Figure 3.2 d for graphic representation of NIC teaming assignments.

The policies are selected in this manner to maintain availability upon any single point of failure from the physical network. Vmnic0 and vmnic1 are connected to one adjacent physical switch (switch#1); vmnic2 and vmnic3 are connected to another adjacent physical switch (switch#2). If either physical switch fails, the load balancing and failover policies will ensure each of the ports supported by the DV Port Groups will continue operation.

| DV PORT GROUP | VLAN | LOAD BALANCING | DVUPLINK1 (VMNIC0) SWITCH#1 | DVUPLINK1 (VMNIC0) SWITCH#1 | DVUPLINK1 (VMNIC0) SWITCH#1 | DVUPLINK1 (VMNIC0) SWITCH#1 |
|---|---|---|---|---|---|---|
| dv-VM01 | 2936 | Orig Virtual Port | Unused | Active | Unused | Active |
| dv-VM02 | 2937 | Orig Virtual Port | Unused | Active | Unused | Active |
| dv-VM03 | 2999 | Orig Virtual Port | Unused | Active | Unused | Active |
| dv-FT01 | 2935 | Explicit Failover | Active | Unused | Standby | Unused |
| dv-iSCSI01 | 2934 | Explicit Failover | Standby | Unused | Active | Unused |
| dv-VMkernel01 | 2933 | Explicit Failover | Standby | Unused | Active | Unused |
| dv-management | native | Explicit Failover | Active | Unused | Standby | Unused |

**Table 4** - DV Port Group Load Balancing Policies

*Editing DV Port Group Policies*

From the Networking Inventory view of the vDS, select the **notepad and pen** icon from each DV Port Group to edit the policy settings.

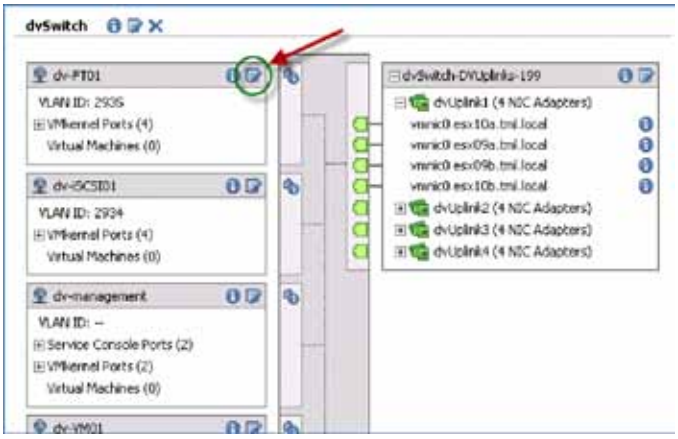



**Figure 3.2 i.** Editing DV Port Group Policies

Select the "Teaming and Failover" panel to adjust the Load Balancing and failover order of the links according to the policies shown in Table 4.

*How vDS Helps with Policy Adjustments*
Because you are using vDS and DV Port Groups, this last stage of adjusting the load balancing and failover policies requires a single edit for each port group you want to change. All hosts covered by the vDS are automatically updated with the new policies. Without vDS and using a standard switch environment (as in VI3), you would have to edit the Port Groups on each and every host.

In the four-host example environment, this means just eight changes for eight DV Port Groups with vDS versus 32 changes (4x8) for the corresponding Standard Switch environment. The vDS is now ready for migration.

**Step 3: Add host to vDS and migrate vmnics to dvUplinks and Ports to DV Port Groups**
In this step, you will migrate the Standard Switch environment of one host to the vDS and DV Port Groups created in steps 1 and 2.

1. Switch to the **Home** > **Inventory** > **Networking view**
2. Right-click the vDS and select **Add Host...**

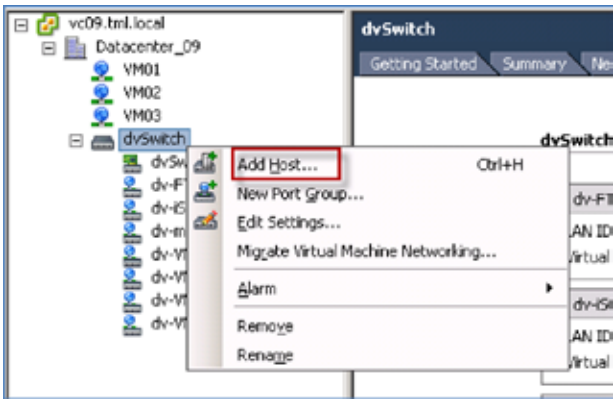



**Figure 3.2 j.** Adding a Host to a vDS

3. Next, select the host to migrate to vDS (esx09a.tml.local in the environment). For this example, choose to migrate all four vmnics from the Standard Switch on esx09a.tml.local to the vDS at one time.

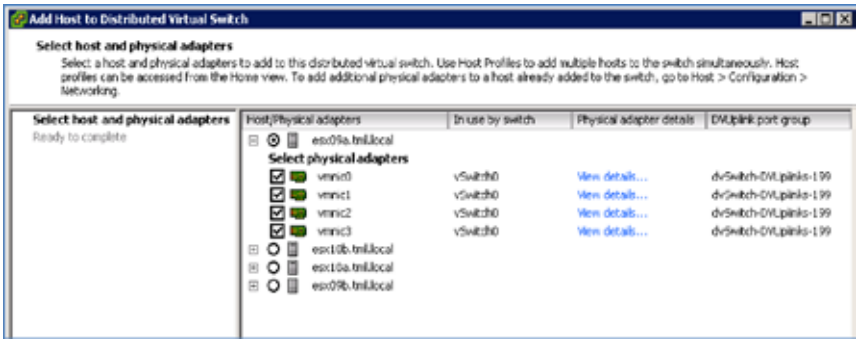



**Figure 3.2 k.** Selecting a Host and vmnics for Migration to vDS

4. Now you need to match up the virtual adapters on the Standard Switch with the DV Port Groups created in Step 2. You will match up the Port Groups and DV Port Groups. Double-check that the VLAN selected for the Management DV Port Group (dv-management in the example) matches that of the Service Console port (vswif0). Any mismatch or mistake with the service console definition could isolate the host and require ILO or console connection to restore connectivity.

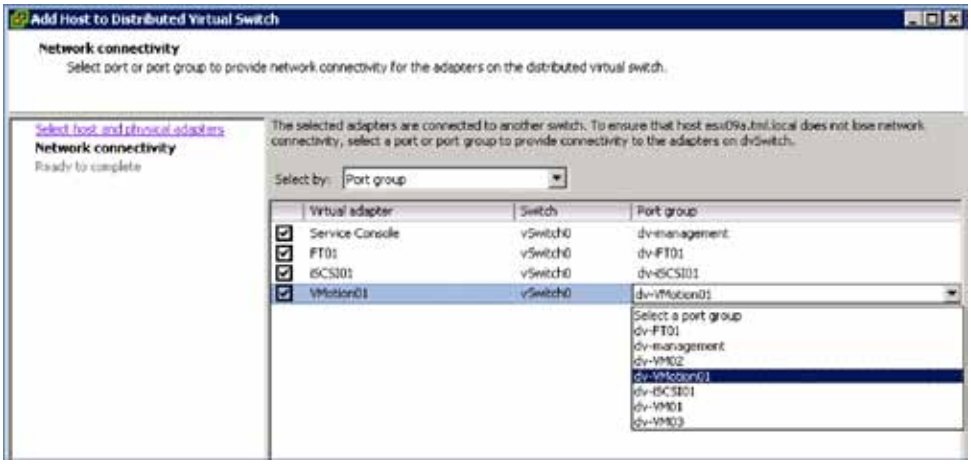



Figure 3.2 l. Selecting Virtual Adapters for vDS Migration

5. The vSphere Client will then present a preview of the changes to the vDS prior to actually executing them. These are shown as highlights on a vDS panel. See Table 3. Double-check the changes once again, particularly the management port (Service Console for ESX or vmkernel port for VMware ESXi).

6. Once checked, click **Finish** and wait for the operation to complete. You can track the status in the Recent Tasks panel at the bottom of the vSphere Client panel. This operation may take around a minute to complete. Note that this step does not transfer the Port Groups for the VMs—they are still associated with the Standard Switch. As you remove all the vmnics from the Standard Switch, these VMs will be disconnected from the network.

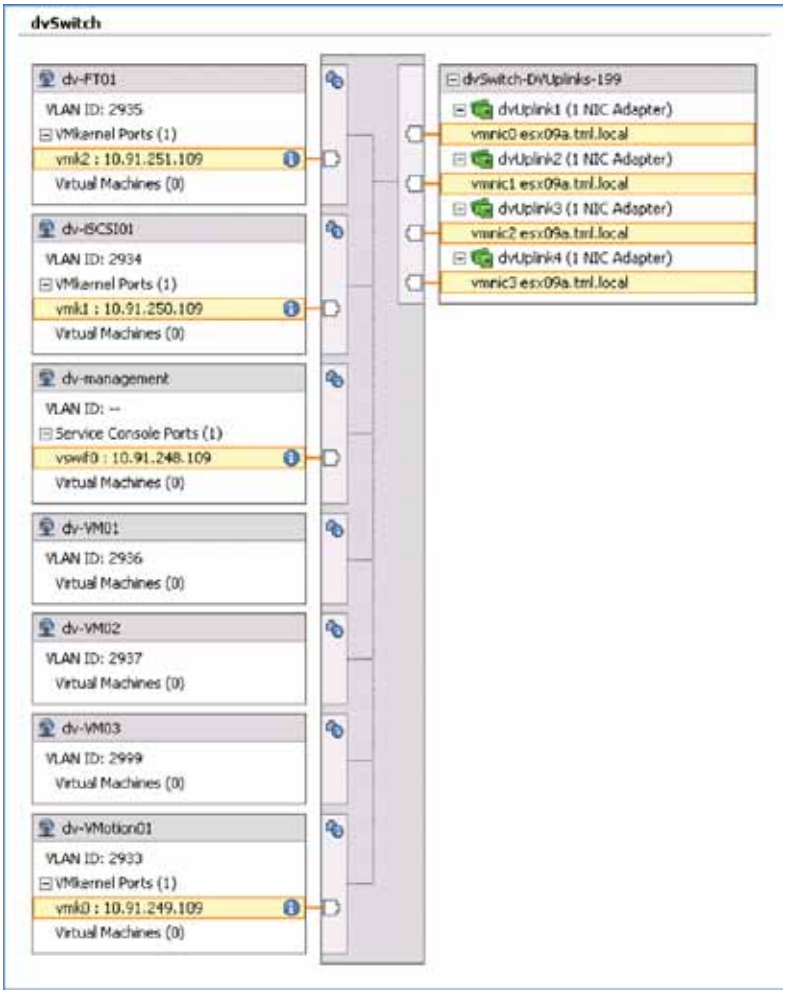



**Figure 3.2 m.** Preview of Changes to vDS Prior to Actual Migration Step

7. The vDS should now appear as shown below. All of the Standard Switch environment, except for the VMs, should now be transferred to the vDS.

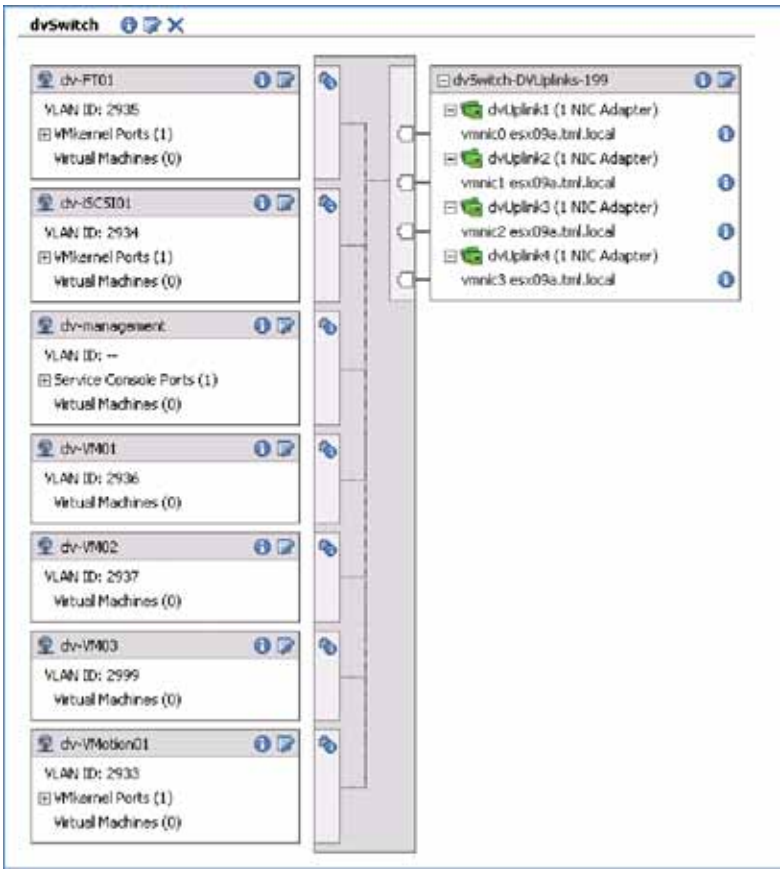



**Figure 3.2 n.** vDS After Migration of One Host

8. Now you can migrate the VMs to the vDS (The VMs on Port Groups VM01, VM02, and VM03 in this environment). If you are migrating a number of hosts to a vDS, you can leave this until last as you can migrate all Virtual Machine Networking for all hosts on the vDS at once.

To begin the process,

1. Right-click on the vDS from **Home** > **Inventory** > **Networking** panel and select **Migrate Virtual Machine Networking...** from the list (see below).
2. Select the source network from the standard switch and the destination network on the vDS. In this example, you have started with a migration of VM01 to dv-VM01.
3. Click the **Show Virtual Machines** button. This will present a list of eligible VMs on the source network on the migrated host (or hosts).
4. Select the VMs you wish to migrate (all of them in this case).

5. Repeat for each of the remaining VM networking Port Groups.

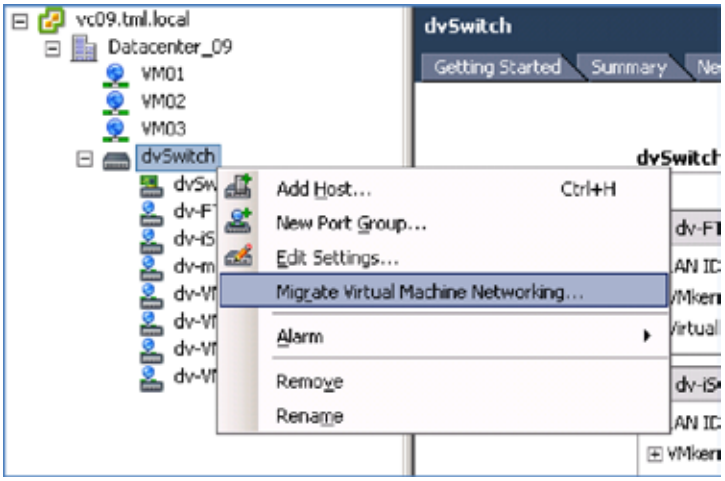



**Figure 3.2 o.** Migrating Virtual Machine Networking to vDS

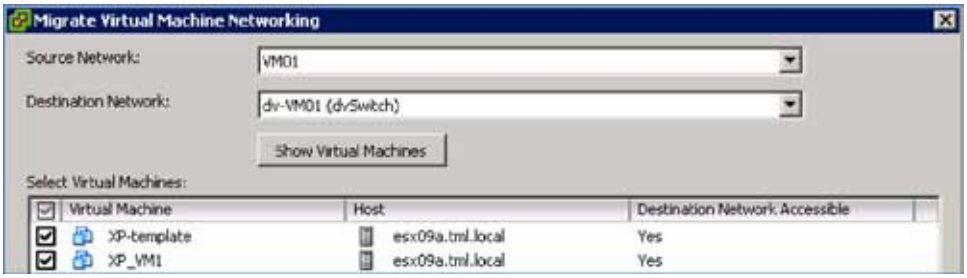



**Figure 3.2 p.** Migrating VM Networking—selecting VMs

### Step 4: Delete Standard Switch from Host

Deleting the Standard Switch from the host is not mandatory, but preferred as a way of cleaning up after the migration to the vDS.

To delete the Standard Switch (vSwitch0), do the following:

1. Go to the **Home** > **Inventory** > **Hosts and Clusters** view and select the **Configuration** tab, and then Networking from the Hardware box.
2. Select **Remove...** from the panel above the vSwitch0 graphic.

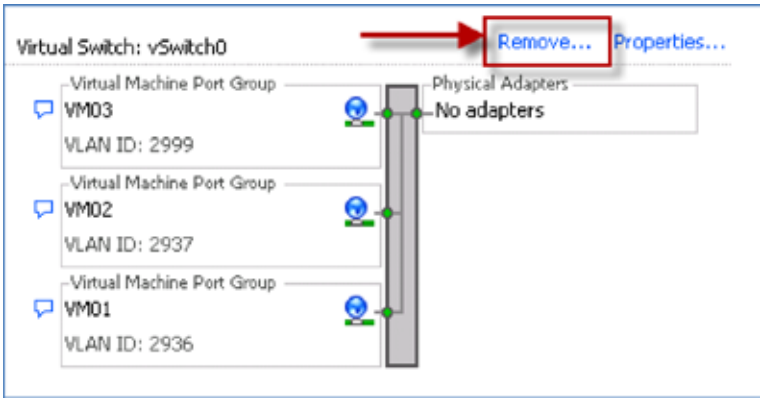



**Figure 3.2 q.** Removing a Standard Switch

**Step 5: Repeat Steps 3 and 4 for Remaining Hosts**

Steps 3 and 4 above migrated the Standard Switch environment to a vDS for one host. Repeat these steps to migrate more hosts to a vDS.

The process outlined above makes it easy to migrate individual or small numbers of hosts to a vDS. It also avoids the need for putting any hosts in Maintenance Mode. Note that Host Profiles provide a simpler way to migrate a large number of hosts in one step. The Host Profile method is described later in this document.

*Configuration and Deployment of vDS using Host Profiles*

In this section you will learn how to deploy a vNetwork Distributed Switch (vDS) using Host Profiles. Host Profiles is the preferred and easiest method for deploying a vDS across a large population of hosts.

*Considerations for using Host Profiles for Deploying vDS*

Note the following when using Host Profiles for deploying a vDS:

- Target hosts must be in Maintenance Mode. This means all VMs must be powered off on the target hosts. If this is a problem, consider a phased deployment or use the per host manual vDS migration method described earlier.
- An ESX Host Profile can be applied to ESX and VMware ESXi hosts. An VMware ESXi Host Profile can only be applied to an VMware ESXi Host. If you have a mix of ESX and VMware ESXi hosts, then create the Host Profile from an ESX host. The Host Profile feature in vCenter Server is able to translate and apply the ESX Service Console definition to an VMware ESXi vmkernel port for management access.

*Note: A full description on using Host Profiles is covered in the Host Profiles section of this evaluation guide.*

*Process Overview*

You will use the following procedure to migrate this evaluation environment to vDS. The starting point is four hosts, each with a single Standard Switch (formerly known as a vSwitch).

The first four steps are the same as the per host manual migration method previously described. At the completion of Step 4, you will have a single host with its networking environment completely migrated to vDS:

1. Create vDS (without any associated hosts)
2. Create Distributed Virtual Port Groups on vDS to match existing or required environment
3. Add host to vDS and migrate vmnics to dvUplinks and Virtual Ports to DV Port Groups
4. Delete Standard Switch from host

The next three steps apply only when using host profiles. They allow you to create a profile of this migrated host and then apply it to a number of hosts in one step (Step 7).

5. Create Host Profile of Reference Host
6. Attach and apply host profile to candidate hosts
7. Migrate VM networking for VMs and take hosts out of Maintenance Mode

It may seem more steps are involved in using Host Profiles versus the Per Host Manual Method described earlier. However, since the Host Profile applies to multiple hosts, the steps above are independent of the number of hosts.

**Step 1 to Step 4: Migrate Reference Host to vDS**

Select a host to use as a "Reference Host." If you wish to apply the Host Profile over a mixed ESX and VMware ESXi environment, then the reference host must be an ESX host. Follow Steps 1 to 4 of the Per Host Manual Migration method described earlier. At completion of Step 4, you should have a single reference host with its virtual networking environment entirely migrated to a VDS.

With this evaluation environment, esx09a.tml.local is the Reference Host.

### Step 5: Create Host Profile of Reference Host

With the vDS looking something like what is in Figure 3.2 n, you can now create a Host Profile of this host (esx09a) and then apply it across the other hosts in the cluster.

Follow these steps to create a Host Profile from the reference host:

1. Go to the **Home** > **Management** > **Host Profiles** view in the vSphere Client.
2. Click **Create Profile**.


**Figure 3.2 r.** Host Profiles Panel

3. Select **Create Profile from existing host**.
4. Select the desired Reference Host in the Create Profile Wizard.

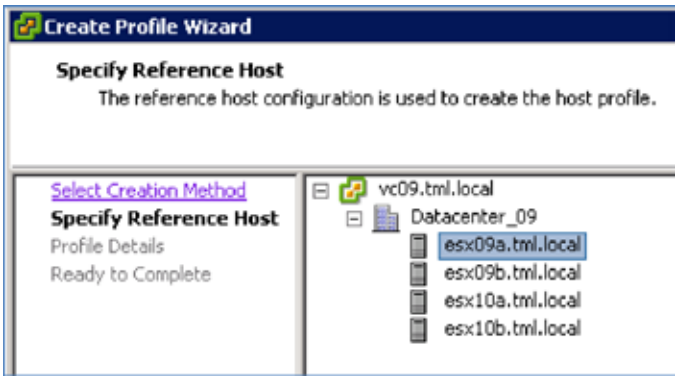



**Figure 3.2 s.** Specifying Reference Host for Host Profile

5. Create a meaningful name ("esx09a-vDS profile" is selected in this example) and description for the Host Profile and click **Next** and then **Finish**. After execution, a Host Profile will appear in the left panel.
6. At this point, you can edit, delete, or attach the host profile to a host or cluster. The edit capability allows fine-tuning of the profile to add or remove components or change settings.

### Step 6: Attach and Apply Host Profile to Candidate Hosts

Host Profiles can only be applied to hosts in Maintenance Mode. All VMs are powered down in Maintenance Mode. If you have powered-up VMs, either shut them down or migrate them to another host.

When the host profile is applied to each of the hosts, a dialog box will ask for the IP address of each of the virtual adapters that will be migrated with the host profile. To prepare for this, gather the IP addresses for the virtual adapters on each of the hosts. The IP addresses for the evaluation environment are shown in Table 5.

| HOST | MANAGEMENT | ISCSI01 | VMOTION01 | FT01 |
|---|---|---|---|---|
| esx09a (ESX) | 10.91.248.109 | 10.91.250.109 | 10.91.249.109 | 10.91.251.109 |
| esx09b (VMware ESXi) | 10.91.248.209 | 10.91.250.209 | 10.91.249.209 | 10.91.251.209 |
| esx10a (ESX) | 10.91.249.110 | 10.91.250.110 | 10.91.249.110 | 10.91.251.110 |
| esx10b (VMware ESXi) | 10.91.248.210 | 10.91.250.210 | 10.91.249.210 | 10.91.251.210 |

**Table 5** - IP Addresses of Virtual Adapters in Evaluation Environment

1. Put the hosts in Maintenance Mode. From the **Hosts** > **Inventory** > **Hosts and Clusters** panel, right-click on each host and select Enter Maintenance Mode. Select **Yes** in the confirmation dialog box.
2. Return to the **Home** > **Management** > **Host Profiles** panel, select the profile created in Step 5 above and click **Attach Host/Cluster**.
3. An Attach Host/Cluster window where you can select which hosts to attach to the selected host profile will open. Select each of the hosts to which you will apply the host profile and click **Attach**. Then click **OK**. Note: the profile is not yet committed to the hosts, so there is still time to back out.

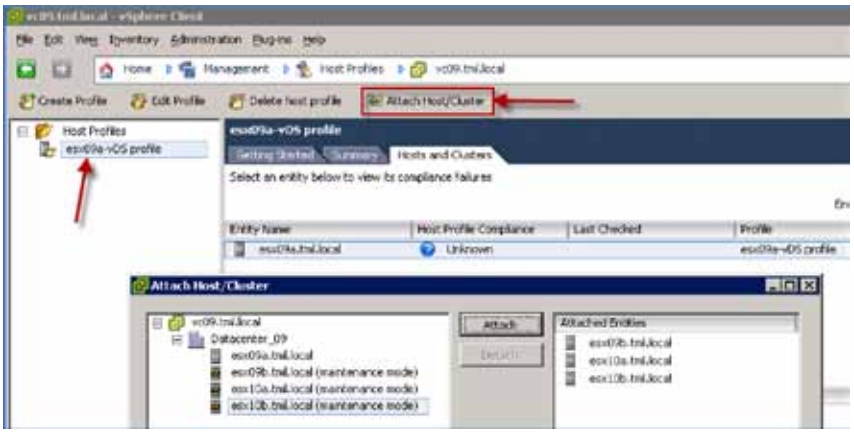



**Figure 3.2 t.** Attaching a Host/Cluster to Host Profile

4. At this point, you can apply the Host Profile to one or more hosts from the Host Profiles panel by control-clicking each host and then clicking **Apply Profile...**

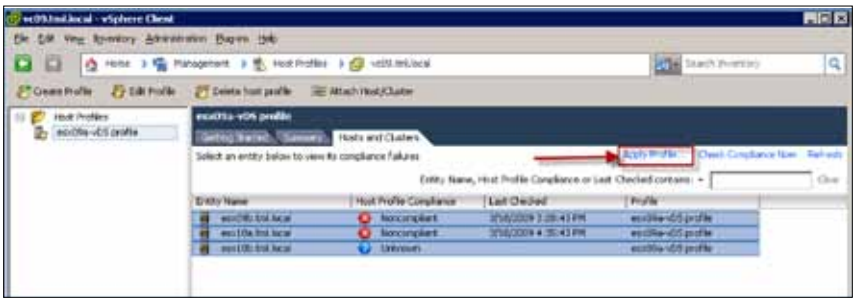


**Figure 3.2 u.** Selecting Hosts to Which to Apply a Host Profile

5. This will bring up the following panel. Insert the IP addresses and masks as prompted for each host. Use the address noted down earlier in Table 5.

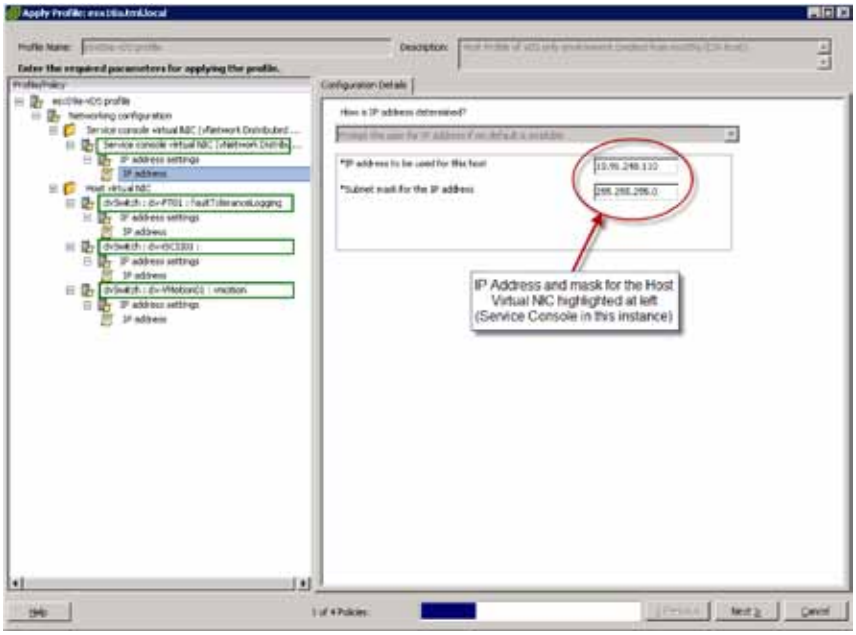



**Figure 3.2 v.** Filling in IP Address Details for Host Virtual NICs as the Host Profile is Applied to a Host

6. When you click **Next**, a panel will appear telling you what changes will be made by the host profile. Below is the report you will see when the host profile is applied to esx10b (VMware ESXi host).

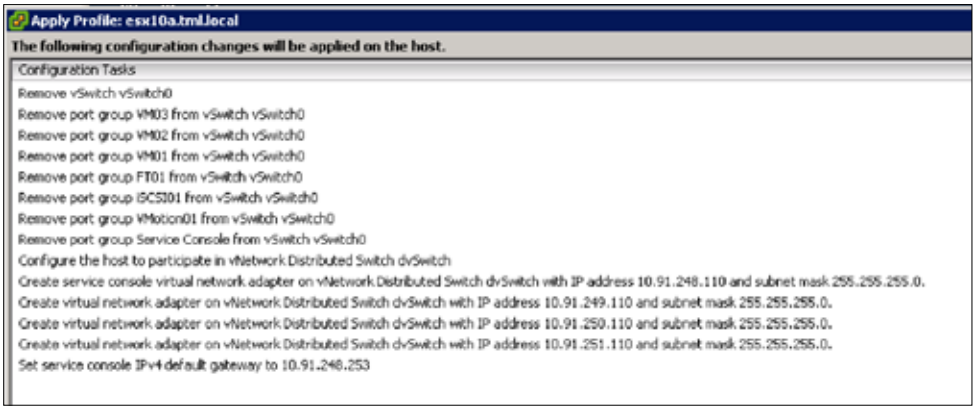



**Figure 3.2 w.** Report What the Host Profile Will Change Once Applied to the Host

### Step 7: Migrate VM Networking to vDS

Next you need to migrate the VMs from the Standard Switch Port Groups to the DV Port Groups.

Go to the **Home** > **Inventory** > **VMs and Templates** panel and right-click on each VM and select **Edit settings**. Select the appropriate DV Port Group on the "Network Label," e.g. dv-VM01.

Variation on Using Host Profiles for Migration:

The process outlined above can be time consuming for a large number of VMs. An alternative method that reduces the per-VM edit process, but requires a re-application of a modified host profile, would be as follows:

- Retain the Standard Switch on each host (and hence the Port Groups) during migration using Host Profiles, i.e. do not perform Step 4 (so you create a host profile of a host with a Standard Switch and a vDS and then apply that profile to the hosts).
- Right-click on the vDS and select **Migrate Virtual Machine Networking...** and then migrate all VMs for each Port Group in one step per Port Group.
- Delete the Standard Switch from the host profile using the edit host profile function (or just delete the Standard Switch from the reference host and create a fresh host profile).
- Re-apply this host profile to the hosts in the cluster. Note that as you have already migrated the virtual adapters, you do not need to re-enter any of the IP addresses.

*vDS After Migration*

After using either of the methods (Per host manual method or Host Profile method) described above, the vDS should appear as shown below.

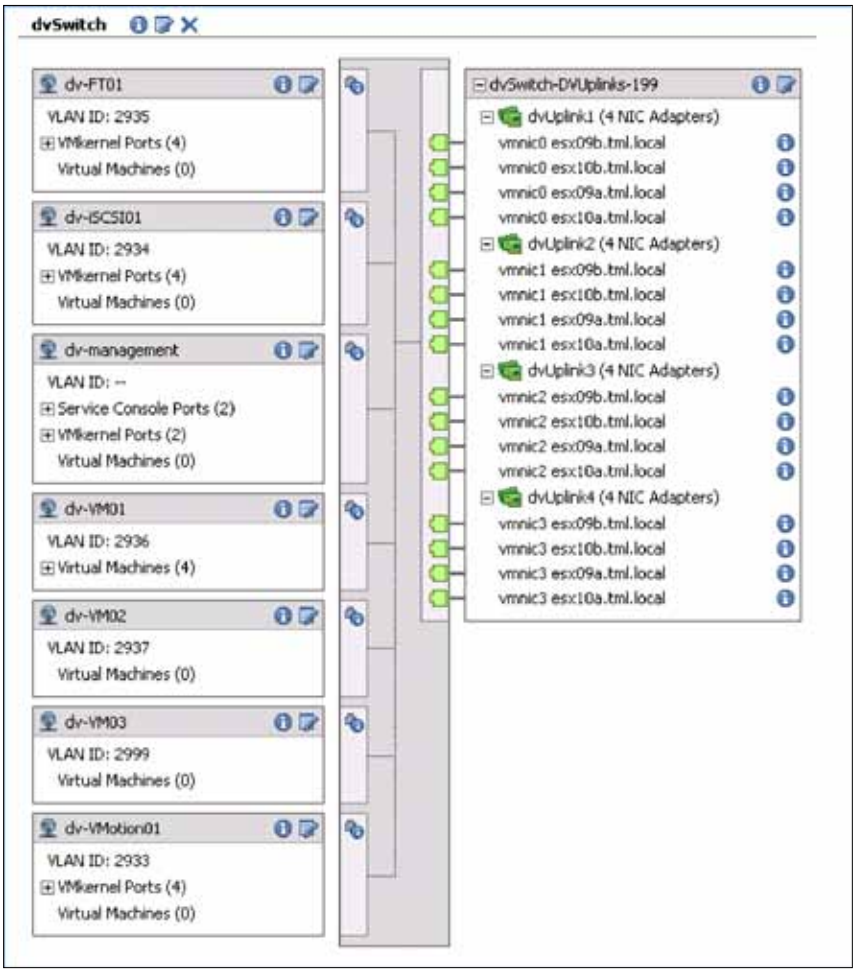



**Figure 3.2 x.** vDS after Complete Migration of All Ports and Uplinks in Evalution Environment

*Using the vDS*
Now that you have a vDS configured across the four hosts, it's time to take a closer look at its capabilities.

The vNetwork Distributed Switch simplifies virtual network administration, particularly across a large number of hosts. As described above, simple changes to port groups that would formerly require the same change across all hosts to keep consistency (when using VMotion, for example), now only require a single change to a distributed port group.

To illustrate this, the following is a simple example of changing the VLAN assignment for a set of VMs. Using this environment, the VLAN for all the VMs will be changed using VLAN 2999 to VLAN 2995. The approach to changing this for a Standard Switch versus a vDS is explained in the following section.

*Changes using the Standard Switch*
In this example environment, VM03 is used as the Port Group for all VMs on VLAN 2999. To change to VLAN 2995, and ensure VMotion would continue to work without issue, you would need to change the Port Group on each and every host.

This is not a difficult exercise in this sample four-host environment, although it does require four separate changes—one for each host. For example, in an environment with 50 hosts, the burden of 50 individual changes becomes much more significant, time consuming and raises the likelihood of human error.

*Changes using the vNetwork Distributed Switch*
The per host change burden goes away when using a vDS with a Distributed Port Group. A single change to the Distributed Virtual Port Group applies to all hosts using that vDS.

In the example where you are changing the VLAN from 2999 to 2995, you would change this on the Distributed Virtual Port Group in much the same manner you would change this on a Standard Switch Port Group.

Figure 3.2 y shows the vDS and where you would click to edit the Distributed Port Group settings. Figure 3.2 z shows where you would change the VLAN ID in the "dv-VM03" Distributed Virtual Port Group settings. Once you change the VLAN ID and click **OK**, the change would be applied to all the hosts almost instantaneously with a minimum of disruption.

Note that you could have changed any of the Distributed Virtual Port Group parameters using the same procedure with a single change, e.g:

- Port Security settings
- Ingress and Egress traffic shaping
- Teaming and Failover
- Port Blocking
- VLAN ID

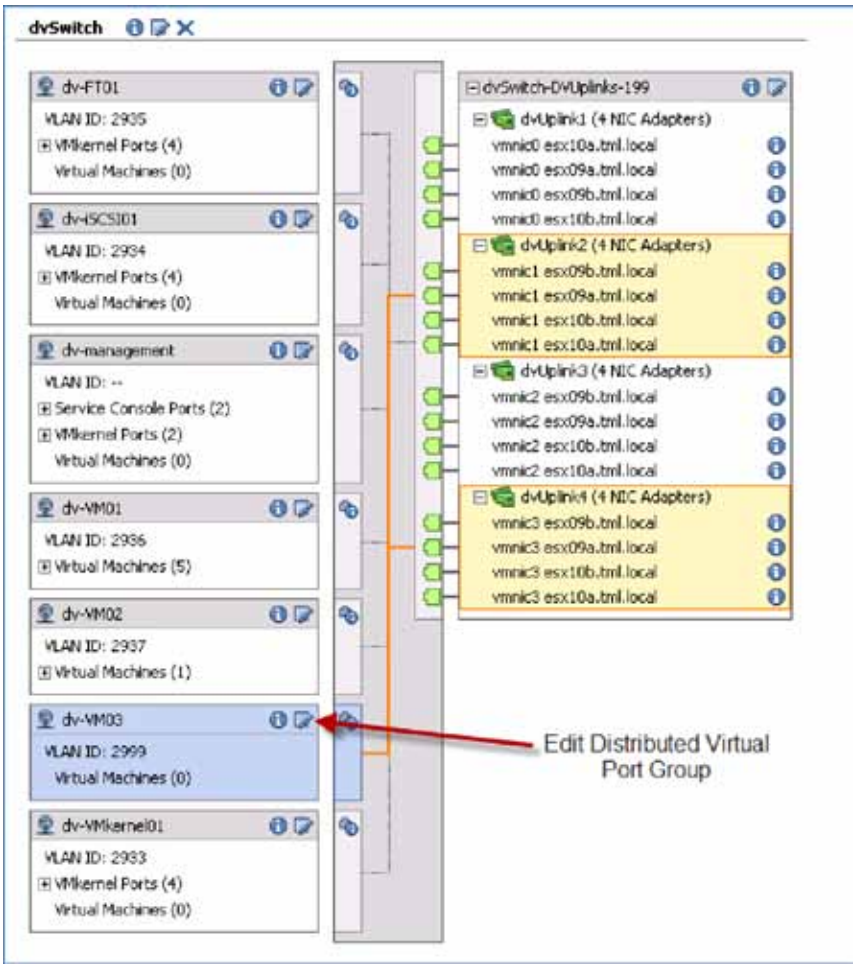



**Figure 3.2 y.** Editing a Distributed Virtual Port Group

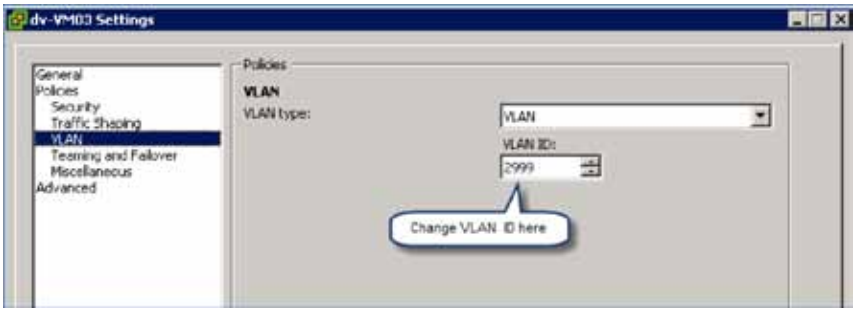



**Figure 3.2 z.** Changing the VLAN id on a Distributed Virtual Port Group

## 3.3. Private VLAN

**What It Is:** Private VLANs (PVLANs) are a new feature introduced in vDS. PVLANs provide a simple way of isolating hosts from each other without exhausting IP subnet ranges and VLANs, or resorting to complex addressing masks.

Consult the ESX Configuration Guide and literature from your physical switch manufacturer for more information about Private VLANs.

**Use Case:** Create and use a Private VLAN on a vNetwork Distributed Switch

### 3.3.1. VMware Differentiators

Private VLAN support in the vNetwork Distributed Switch lets you extend networking best practices for isolation and IP address conservation to the virtual domain.

- **Only VMware vSphere supports Private VLANs**—Microsoft Hyper-V R2 and Citrix XenServer 5.5 are missing that feature.
- Private VLANs are in common use in datacenters to define private switch ports that are restricted to a single network uplink.
- Private VLANs also conserve IP addresses by isolating virtual switch ports from each other even though they belong to the same IP subnet.
- vSphere Private VLANs are easily configured as port groups on a vNetwork Distributed Switch.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| VNETWORK DISTRIBUTED SWITCH | | | |
| Basic 802.1q VLAN Support—Define VLAN IDs for virtual switch ports and port groups to isolate network packets from virtual machines on other switch ports | Yes | No | Limited, VLAN IDs can only be set from the Linux command line |
| Private VLAN Support—Enables configuration of primary and secondary Private VLAN IDs for vDS ports | Yes | No | No |
| Isolated Secondary Private VLAN Ports—A VM using a port can only communicate with primary Private VLAN ports | Yes | No | No |
| Community Secondary Private VLAN Ports—A VM using a port can communicate with other ports on the same secondary Private VLAN | Yes | No | No |

### 3.3.2. Private VLAN Hands-on Review

| | | | |
|---|---|---|---|
| Infrastructure Setup | Private VLANs with vNetwork Distributed Switch | 3.3 Create and use a Private VLAN on a vNetwork Distributed Switch<br><br>'1. Configure vDS for Private VLANs<br>2. Create new DV Port Groups for Private VLANs<br>3. Move VMs to new DV Port Groups | 30 minutes |

PVLANs require configuration on the vDS and the physical switch environment. Make sure your physical switches support Private VLANs and are configured to use them.

*Evaluation Environment for Private VLANs*
For this evaluation, you will configure two Private VLANs on a single host (esx09a). This host has five VMs (XP_VM1, XP_VM2, ..., XP_VM5). You will use the PVLAN assignments as follows:

| PVLAN TYPE | PRIMARY PVLAN (PROMISCUOUS) | SECONDARY PVLAN | VMS |
|---|---|---|---|
| Community | 4000 | 4001 | XP_VM1, XP_VM2 |
| Isolated | 4000 | 4002 | XP_VM3, XP_VM4, XP_VM5 |

The rules for Private VLANs are as follows:

- VMs on the Promiscuous PVLAN can communicate with all VMs in the promiscuous, isolated, and community PVLANs
- VMs on the Community PVLAN can communicate with each other and those in the promiscuous PVLAN, but not with VMs in the Isolated PVLAN.
- VMs in the Isolated PVLAN cannot communicate with each other or those in the community PVLAN, but can communicate with VMs in the promiscuous PVLAN.

**Step 1: Configuring a vDS for Private VLANs**
PVLANs can only be configured on a vDS. PVLANs are not supported on Standard Switches.

1. Start the PVLAN configuration process by editing the vDS Settings and selecting the Private VLAN tab.

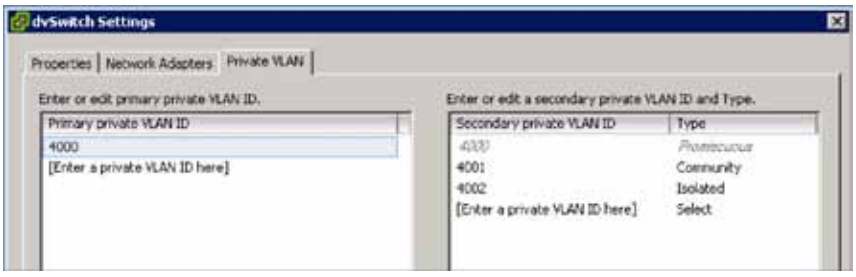



**Figure 3.3 a.** Configuring Private VLANs on vDS

**Step 2: Create new DV Port Groups for Private VLANs**

Once you have created the PVLAN structure, you need two new DV Port Groups to use these PVLANs—one for the Isolated PVLAN and one for the Community PVLAN.

1. Select **New Port Group...** and fill out the properties panel, making sure to select "Private VLAN" for VLAN type.

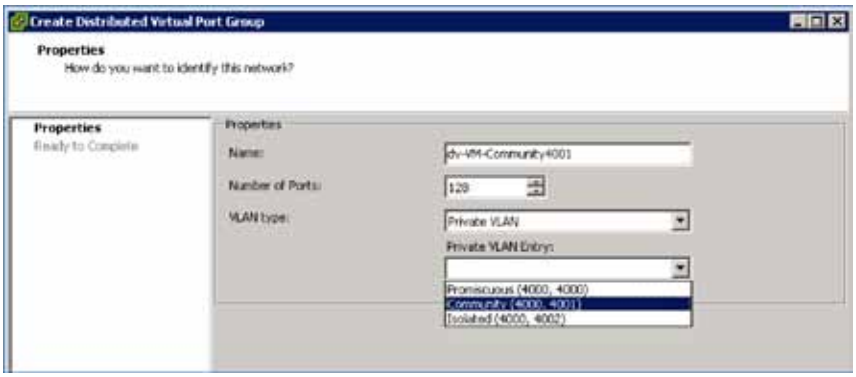



**Figure 3.3 b.** Adding a New DV Port Group for Private VLANs

### Step 3: Move VMs to new DV Port Groups

- Once the DV Port Groups are created, move some VMs to these Private VLANs by editing the VM properties to use one of the new DV Port Groups.
- Repeat this for each of the VMs to complete the process.

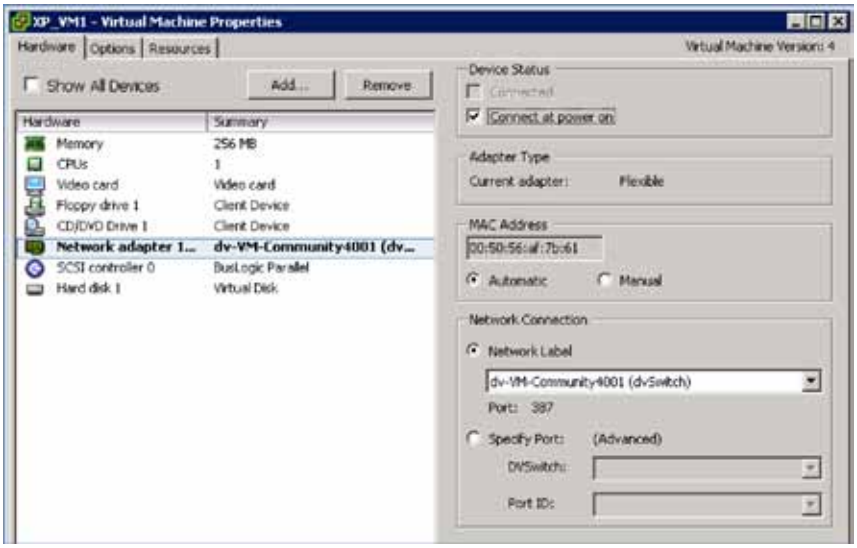



**Figure 3.3 c.** Editing the Network Label to Use Private VLAN

At this point you have created a primary promiscuous PVLAN plus a secondary isolated PVLAN and secondary community PVLAN. You have also created DV Port Groups for each of these PVLANs and allocated VMs to each. Use ping to check the connectivity or isolation between the VMs.

## 3.4. Hot Add

**What It Is:** Despite the extensive planning that goes into the initial sizing and configuration of a virtual machine, it can be difficult to predict and accommodate sudden changes in workload demands. With VMware Hot Add, capacity can be dynamically added to virtual machines while they are powered on. This enables applications to scale seamlessly without disruption or downtime.

**Use Case:** Hot Add Capacity to Powered-On Virtual Machines

### 3.4.1. VMware Differentiators

Increase VM resources with no downtime with hot add virtual CPU and memory.

- **Hot add virtual CPU and memory is an exclusive VMware vSphere feature.** Microsoft Hyper-V and Xen do not support hot add of virtual machine memory or CPU and those features are missing from the public roadmaps of both hypervisors.
- When virtual machines encounter a long-term workload increase, vSphere's hot add feature lets administrators add capacity with no need for downtime.
- When supported by recent guest OSs, such as Windows Server 2008, virtual machine RAM or virtual CPUs hot added to vSphere VMs can be immediately utilized without a reboot of the virtual machine.
- For short-term workload increases, vSphere's advanced resource management features allow VMs to temporarily consume more CPU and memory shares as governed by the proportional shares and limits you set.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **HOT ADD VIRTUAL CPUS,MEMORY AND DEVICES TO VIRTUAL MACHINES** | | | |
| Hot Add Virtual CPUs—Guest OSs supporting hot add CPU (Windows Server 2008) require no reboot to use added CPUs | Yes | No | No |
| Hot Add Virtual Machine Memory—Guest OSs supporting hot add memory (Windows Server 2003, 2008, RHEL 5, SLES 10) require no reboot to use added CPUs | Yes | No | No |
| Hot plug virtual devices (virtual disks and NICs) | Yes | Yes | Yes |

### 3.4.2. Hot Add Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Hot Add | 3.4 Hot add capacity to powered-on virtual machines:<br>1. Enable memory/CPU hotplug support<br>2. Hot add CPU and memory to a powered-on virtual machine | 10 minutes |

The following exercise will demonstrate how to hot add compute and memory resources to a powered-on Windows Server 2008 Datacenter Edition (64-bit) virtual machine with the following configuration: 1 VCPU, 512GB of memory, 10GB of disk.

The "Memory/CPU Hotplug" feature requires that you have a virtual machine with virtual machine version 7 and guest operating system that support this functionality. See the Guest Operating System Installation Guide for the list of operating systems for which this functionality is supported. If you do not meet these requirements, the Memory/CPU configuration fields will be grayed out in the Virtual Machine Properties Editor when the virtual machine is powered on.

**Step 1: Enable Memory/CPU Hotplug support**

In this step, you will change advanced virtual machine settings to enable Memory/CPU Hotplug support. The virtual machine will need to be in a powered off state, and VMware Tools must be installed for hot plug functionality to work properly.

1. Select a Windows Server 2008 Datacenter Edition (64-bit) virtual machine from the inventory, and verify that it has virtual machine version 7. Power off the virtual machine if it is not already.
2. Click **Edit Settings** to open the Virtual Machine Properties Editor.
3. Click the **Options** tab of the Virtual Machine Properties Editor.
4. Select **Advanced** > **Memory/CPU Hotplug**.
5. Select **Enable memory hot add** for this virtual machine to enable memory hot add. Note that not all guest operating systems may support memory hot add. Memory hot remove is not supported in this release.
6. Select **Enable CPU hot add** only for this virtual machine to enable CPU hot add.

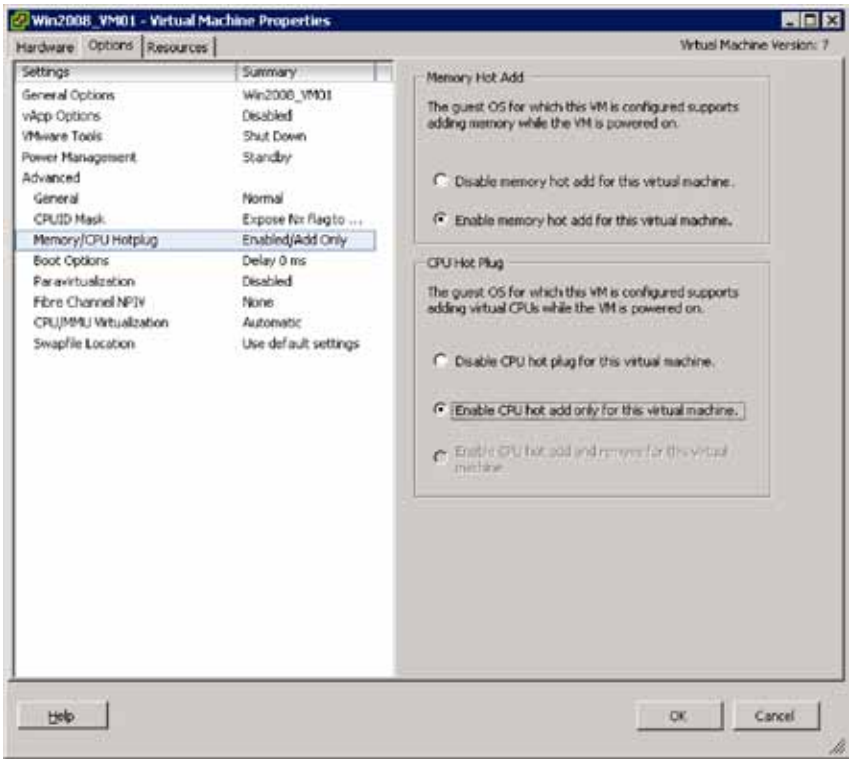



**Figure 3.4 a.** Enabling Memory/CPU Hotplug on a Windows 2008 virtual machine.

**Step 2: Hot add CPU and Memory to a powered-on virtual machine**

In this step, you will change the CPU and memory configurations of the powered-on virtual machine. Behind the scenes, the hot addition of CPU and memory are signaled to the guest operating system via ACPI events.

1. Power on the virtual machine.
2. Click **Edit Settings** to open the Virtual Machine Properties Editor.
3. To change the memory configuration:
   a. Click the **Hardware** tab in the Virtual Machine Properties Editor.
   b. Click **Memory** in the Hardware list.
   c. Adjust the amount of memory allocated to the virtual machine. Hot add memory adjustments can be done in 4MB to 1GB increments depending on the guest operating system.

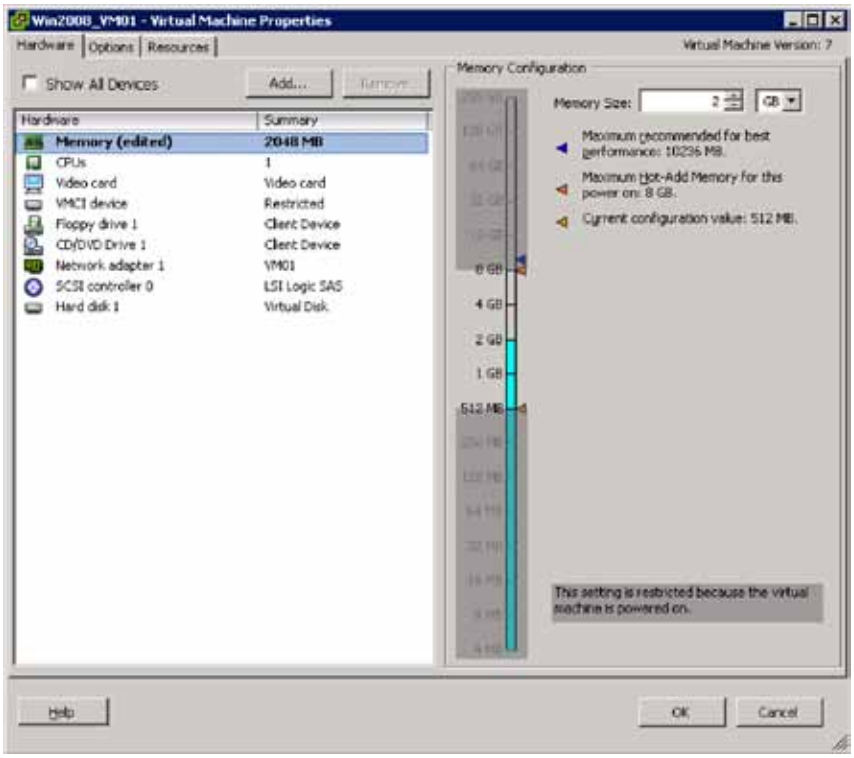



**Figure 3.4 b.** Hot adding memory from current 512MB configuration to 2GB on a powered-on Windows Server 2008 virtual machine

4. To change the CPU configuration:
   a. Click **CPUs** in the Hardware list.
   b. Select the number of virtual processors for the virtual machine. VMware ESX/VMware ESXi 4.0 supports hot add of virtual CPUs up to a total of 8 per VM.
   c. Click **OK** to save your changes and close the dialog box.
5. Verify that the hot-added CPU and Memory are visible to the virtual machine.

## 3.5. Dynamic Storage Management

**What It Is:** The vStorage VMFS Volume Grow and hot extend for virtual disks features allow dynamic expansion of both VMFS volumes and the virtual disks that reside on them without disrupting running virtual machines. Used together, these features provide maximum flexibility in managing growing vSphere capacity needs.

### 3.5.1. VMware Differentiators

Respond easily and non-disruptively to changing storage requirements.

- vSphere's unique ability to hot grow a VMFS volume to add capacity to a datastore and hot extend virtual disks allows administrators to respond to increasing virtual machine storage requirements without downtime.
- Microsoft Hyper-V and Xen products like Citrix XenServer and Oracle VM can't expand mounted storage devices. Storage expansions require unmounting the storage volumes, and since those products have no live storage migration capability, VM downtime is required.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| **DYNAMICALLY GROW STORAGE VOLUMES AND VIRTUAL DISKS** | | | |
| vStorage VMFS Volume Grow—Add capacity by dynamically expanding active VMFS datastores | Yes | No, must expand volumes offline using storage utilities | No, must expand volumes offline using storage utilities |
| Hot Extend Virtual Disks—Increase the size of VMFS virtual disks. No VM downtime required for partition expansion for guest OSs compatible with dynamic disk growth (like Windows Server 2008). | Yes | No, must shutdown VM prior to expanding virtual disk | No, must shutdown VM prior to expanding virtual disk |

### 3.5.2. Dynamic Storage Management Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Dynamic Storage Management | 3.5 Migrate virtual machines to fill up a datastore, trigger an alarm and then solve the issue by increasing the size of that datastore.<br><br>1. Use datastore views to confirm which virtual machines are in each datastore<br>2. Use Storage VMotion to fill up a datastore and trigger an alarm<br>3. Detect and investigate alarm that is triggered<br>4. Expand the Datastore using VMFS volume Grow<br>5. Notice Alarm is now no longer raised | 60 minutes |

*Migrate virtual machines to fill up a datastore, trigger an alarm and then solve the issue by increasing the size of that datastore.*

Managing storage in a vSphere environment is greatly enhanced with by the introduction of several new storage features. This section will highlight the use of:

1. Alerts and Alarms to provide a warning that certain shared storage resources need attention.
2. VMFS Volume Grow feature to enable dynamic increase of the shared storage resource.

All of these features are integrated into vCenter. Management of the datastores as objects within vCenter provides more centralized control with improved visibility and reporting on storage resource usage. Enabling permissions and limits on VM storage also provides greater control of how storage resources are allocated and used.

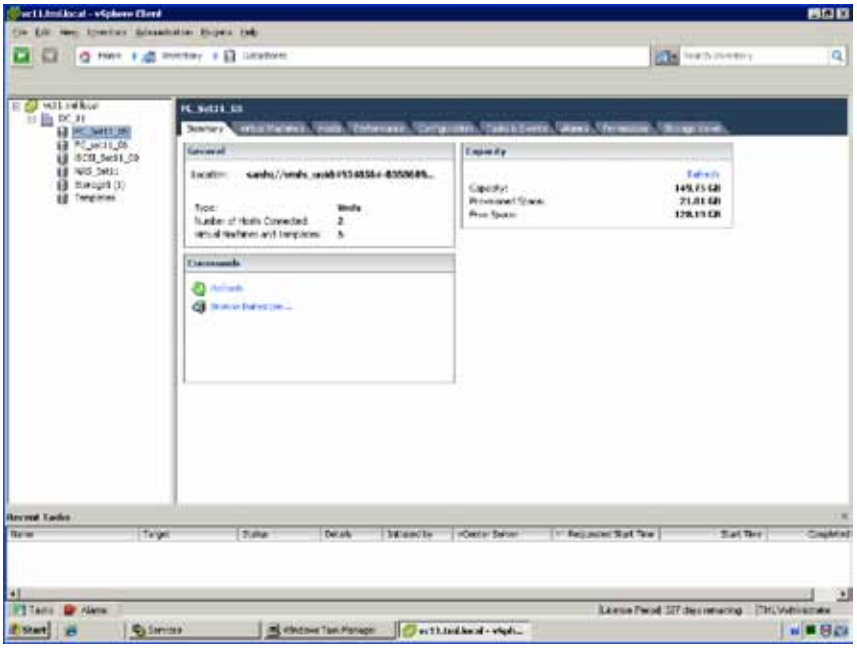
The following steps will walk you through these new storage management features in a logical way to get familiar with the features and their use.

**Step 1: Use datastore views to confirm which virtual machines are in each datastore**

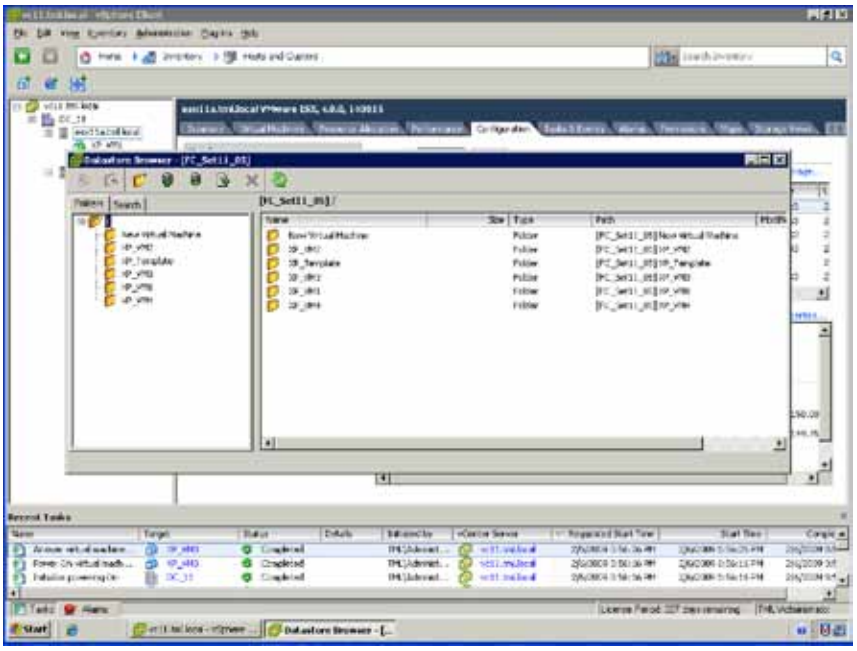
In the previous maturity section, you created a second datastore that occupied only a small portion of the FC LUN.

You will now fill up the 10GB datastore with VM homes to a point were it can't accommodate additional VMs. In doing so, you will trigger an alarm.

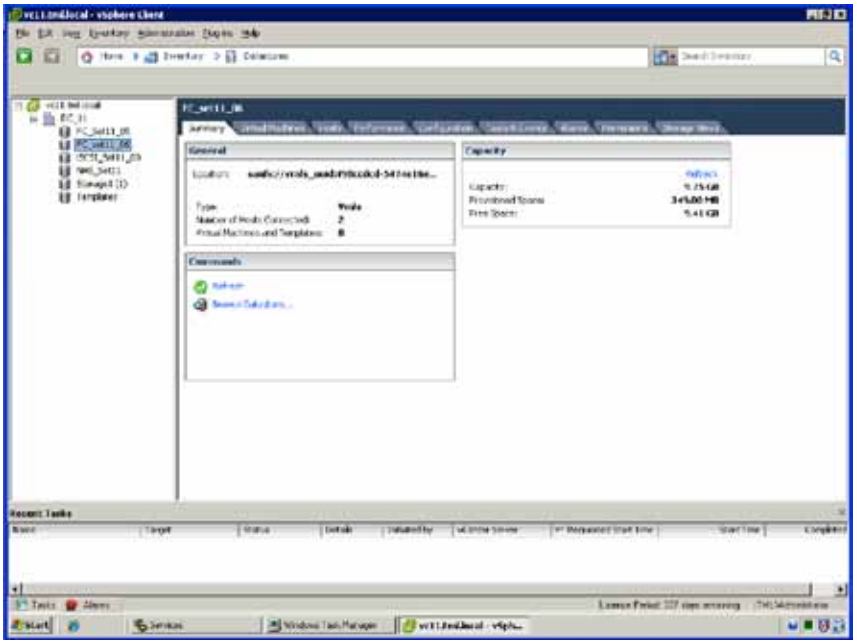
1. Start by looking at the contents of the VMs on the first datastore (FC_set11_05) in the summary tab for that datastore.



2. For more details about which VMs are in this datastore, browse the datastore. With the datastore highlighted, right-click and then select **browse datastore**.



3. The summary screen of the second datastore (FC_set11_06) indicates that there are no VMs residing in this datastore.

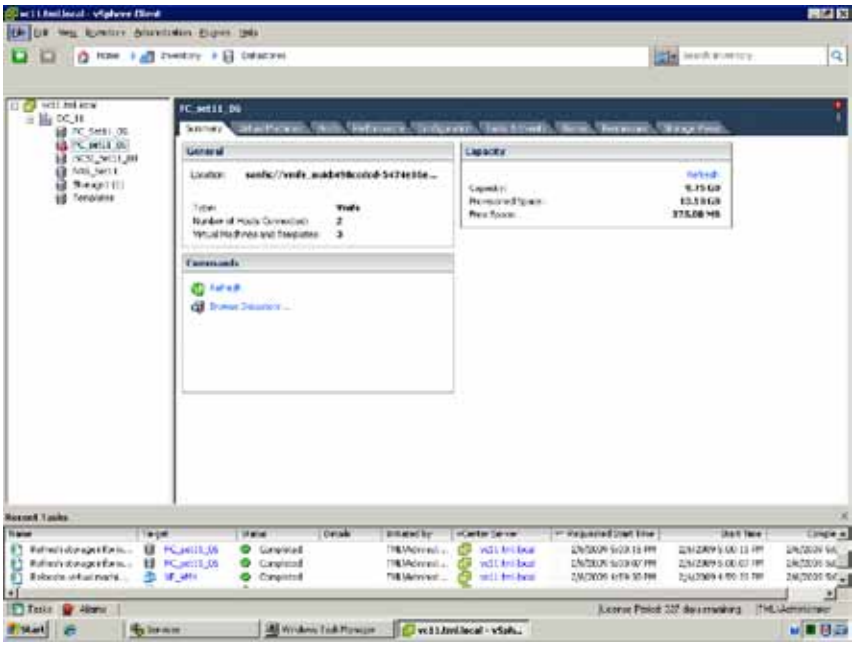


**Step 2. Use Storage VMotion to fill up a datastore and trigger an alarm.**

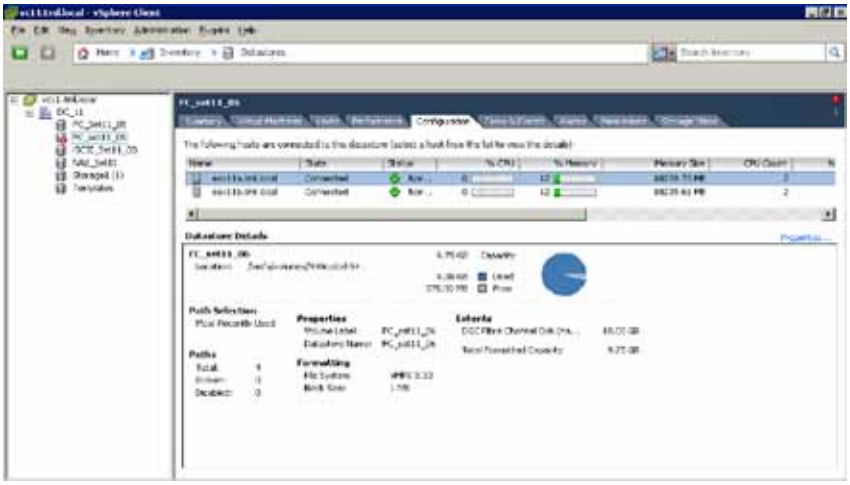
1. Use Storage VMotion to move three VMs from FC_set11_05 to FC_set11_06
2. Change inventory view to **Hosts and Clusters**, select **VMs** and right-click as done in the Medium Maturity Level exercise.

**Step 3. Detect and investigate alarm that is triggered**

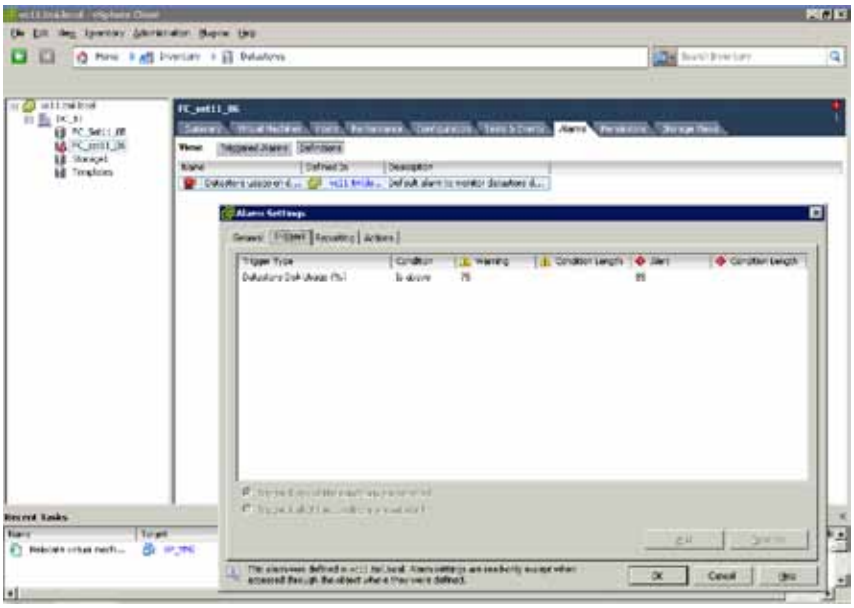
1. Notice that the alarm has been triggered because the free space on the new datastore is now below the percentage set in the alarm.



2. To see more details look at the datastore details by selecting the **Configuration** tab.



3. To find more information about why the alert was triggered, select the **Alarms** tab for datastore, then choose **Triggered Alarms and Triggers**.

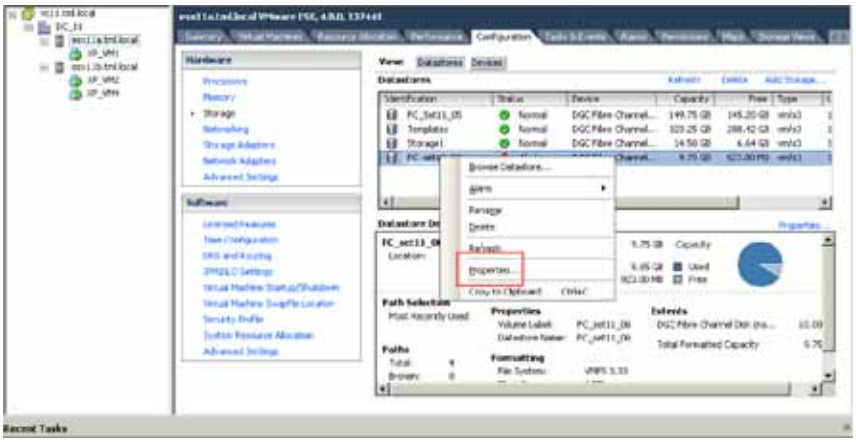


4. You can see or change the datastore alarm settings in the datastore view. The default settings are for a warning to be issued when it is over 75% full and an alert to be raised when its usage gets over 85% of capacity. In this case, the datastore is over 90% full. This is a default alarm that is turned on for all datastores, but can be customized (see alarm section for more details).

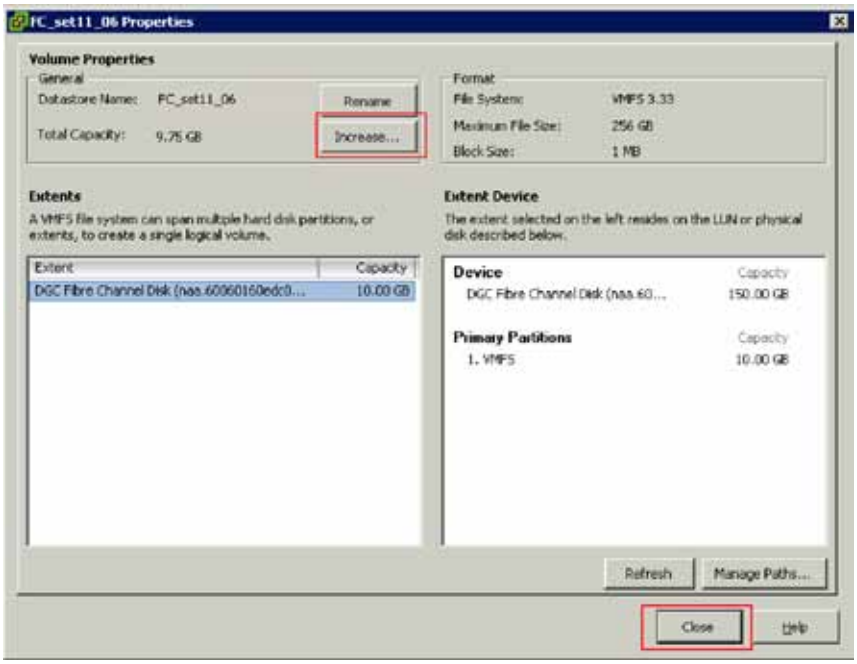
**Step 4. Expand the Datastore using VMFS Volume Grow**

Increase the size of the VMFS volume/datastore using the VMFS Volume Grow feature that has been introduced in VSphere.

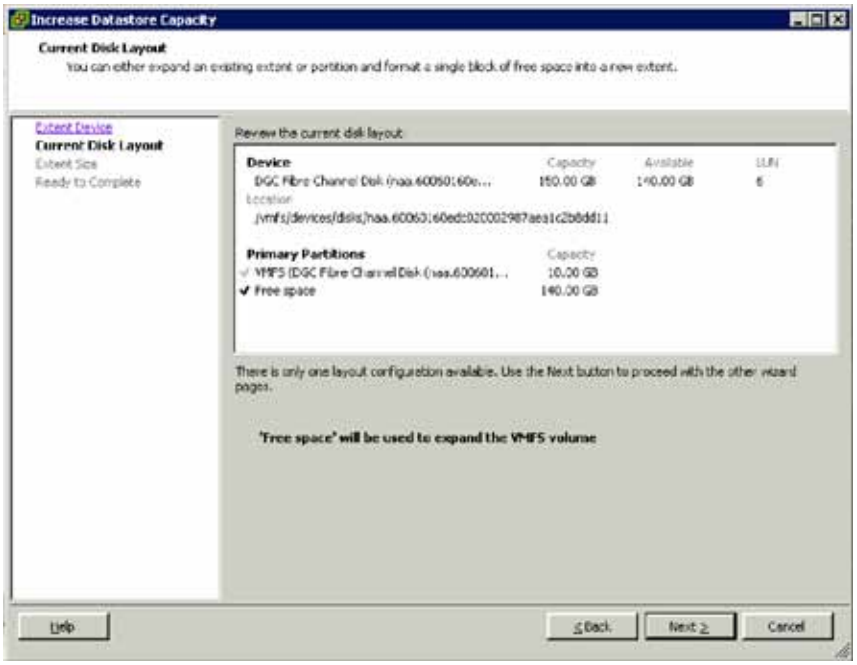
- To grow the VMFS volume FC_set11_06 by selecting the datastore, right-click and select the properties from the list.



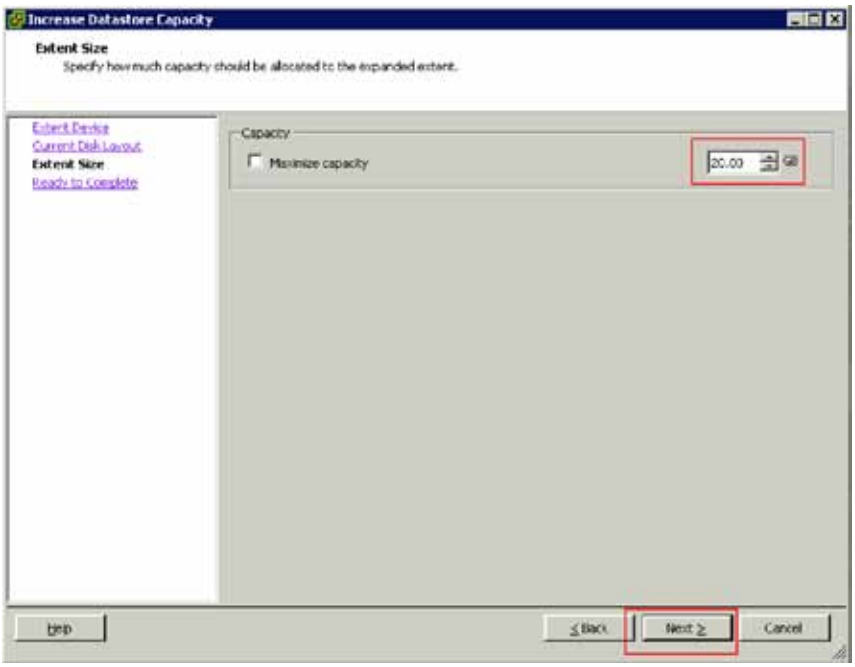
- Click **Increase**.



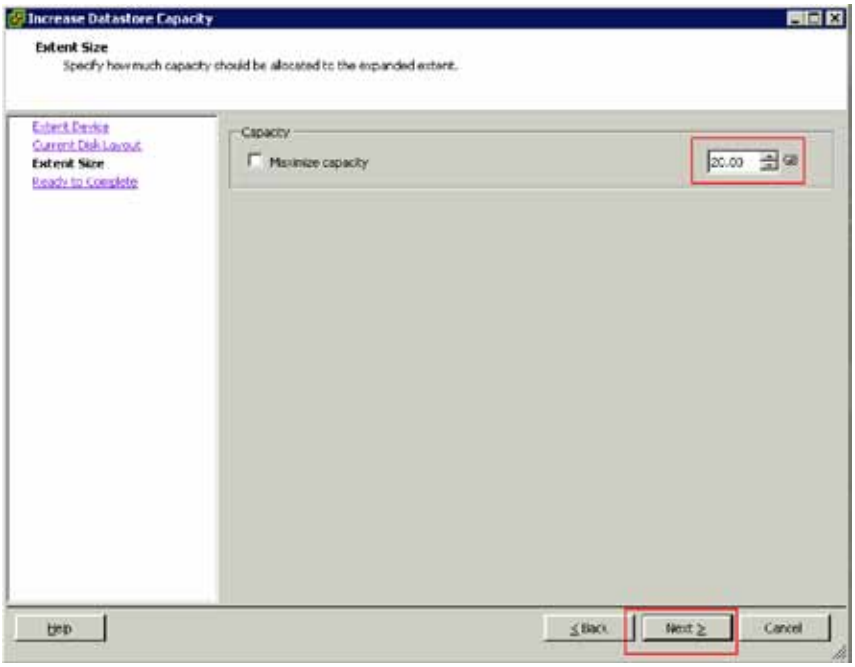

- This will display the extent size and layout of the space that this extent can be expanded into. Review this information and click **Next**.



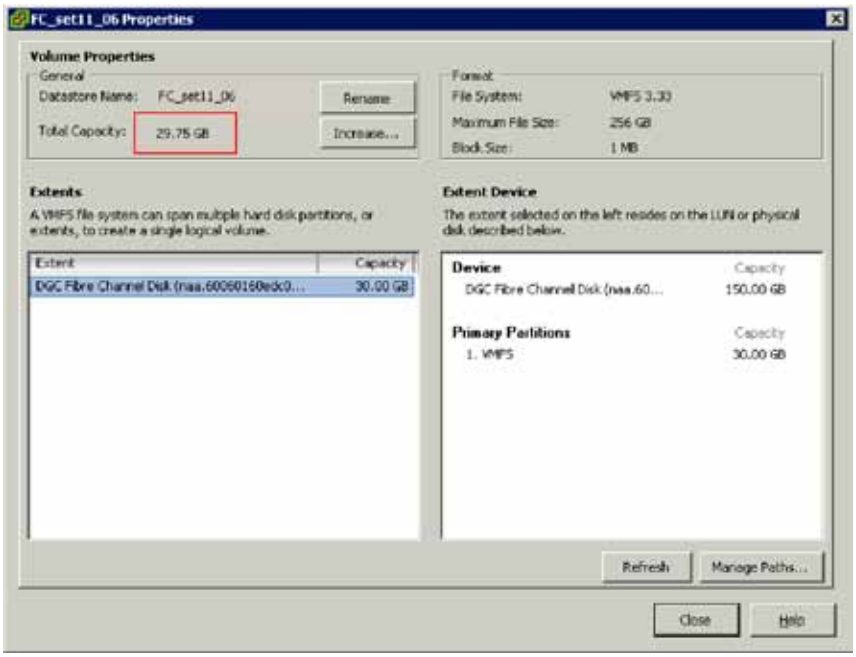
- You can either accept the default and increase the extent to the maximum size or deselect the check box and enter a smaller amount if you want to grown the extent again at a later time. Note this value is the incremental additional capacity. Click **Next** when your are finished.




- Review the details on the Ready to complete screen and click **Finish** to complete the process of expanding the VMFS Volume.



- Once completed, the the upper left of the properties screen will reflect the larger capacity for the datastore.




**Step 5. Notice Alarm is now no longer raised**

As you have now increased the size of the datastore from 10GB to 30GB, the alarm will be turned off. It may take a minute or two for vCenter to reflect this. Or you can select the refresh option on the datastore view to initiate that update.

## 3.6. Alarms

**What It Is:** Alarms are specific notifications that occur in response to selected events or conditions on an object. For example, you can configure alarms to occur when a virtual machine is powered off, a datastore exceeds a set capacity, or when a host's networking redundancy is compromised due to a NIC failure.

### 3.6.1. VMware Differentiators

vSphere provides powerful and tightly integrated alarm features.

- vSphere provides easily configured alarms that can be triggered by hundreds of customizable events and conditions. Low-level hardware and host events are displayed and can trigger alarms. vSphere lets you minimize false alarms due to transient events with configurable time conditions for alarms.
- vSphere's alarm features are fully integrated into the vCenter and the vSphere Client interface.
- Flexible vSphere alarm actions let you notify administrators and management systems of alarm conditions and take actions to automatically remediate problems.
- XenServer offers only three basic alarm trigger conditions and email alerts. It provides no automated alarm actions.
- To support alarms, Microsoft requires separate installation of System Center Operations Manager with its own servers, databases and management interfaces. SCOM alarms and rules are flexible, but the broad scope of SCOM complicates configuration of alarms specific to Hyper-V.

*Feature Function Comparison*

| FEATURE | VMWARE VSPHERE 4 | MICROSOFT HYPER-V R2 WITH SYSTEM CENTER | CITRIX XENSERVER 5.5 WITH XENCENTER |
|---|---|---|---|
| ALARMS | | | |
| Integrated Alarm Functions—Configuration of alarm triggers and actions is integrated into the vSphere Client under the "Alarms" tab | Yes | No alarms feature in Hyper-V or SCVMM. Requires SCOM installation (additional servers, DBs and UIs). VMware alarms are not visible from SCVMM or SCOM. | Yes, alarms Integrated in XenCenter |
| Flexible Alarm Triggers—Hundreds of alarm triggers at VM, host, datastore, and datacenter level | Yes | SCOM offers many triggers, but most are unrelated to virtualization | Limited - alerts only on host/VM CPU, host/VM network, and VM disk activity. |
| Multiple Alert Methods—Alarm alerts presented in vSphere Client, via email, or to other management agents via SNMP | Yes | Yes (requires SCOM) | No, Email only |
| Automated Actions for Alarm Remediation—Run a defined script or take any of nine default host and VM level actions to correct problems | Yes | Yes (requires SCOM) | No automated tasks based on alarms |

### 3.6.2. Alarms Hands-on Review

| | | | |
|---|---|---|---|
| Availability and Capacity | Custom Alarm Setup | 3.6 Using a custom alarm for network access<br>1. Configure a vNetwork Distributed Switch<br>2. Set up a custom network alarm<br>3. Trigger the alarm | 20 minutes |

An alarm consists of one or more triggers, and one or more actions.

- **Trigger**—A set of conditions that must be met for an alarm to register.
- **Action**—The operation that occurs in response to the trigger. Alarms generate warnings and alerts in the vSphere Client when the specified criteria are met, but you can also configure a wide range of other actions.

Alarms have three types of triggers

1. Condition triggers monitor metrics for a host, virtual machine, or datastore. These metrics include values such as: Host CPU Usage (%), VM Snapshot Size (GB), and Datastore Disk Usage (%).
2. State triggers monitor the current state of a host, virtual machine, or datastore. Examples include: VM Power State (on, off, suspended), Host state (connected, not responding, etc), and datastore connection state (disconnected from a host, etc).

3. Event triggers monitor events that occur on managed objects, the VirtualCenter Server, and the License Server. Examples include: status changes (such as Host Exited Maintenance Mode), Access Control operations (such as Role Created), and license events (such as License Expired).

Condition and State triggers can be more finely defined by specifying details such as: amount of time a condition should exist to trigger the alarm (to avoid false alarms due to sporadic fluctuations) and tolerance range for a metric (to allow a different upper and lower threshold for an alarm value).

Some example actions that can be configured for alarms include:

- Send a notification email
- Send a SNMP notification trap
- Run a script or command
- VMotion, Power on, power off, suspend, reboot, shutdown or reset a VM
- Enter or exit maintenance mode or standby mode on a host
- Reboot or shutdown a host

vCenter comes with a wide variety of pre-defined alarms for various situations, some of which you have already seen in action.

**Use Case:** Creating a Custom Alarm for Network Access

Because virtual switches on the same ESX host are isolated from each other, it is possible to consolidate virtual machines that should reside on separate networks onto the same host or cluster. In this configuration, no virtual machine on one virtual switch is able to see network traffic flowing through any other virtual switch. Each virtual switch can be configured to send traffic off the ESX host either through separate VLANs or by separate physical NICs, depending on what is appropriate for the rest of the (physical) network infrastructure.

Although network isolation exists between virtual machines on different virtual switches, one concern would be that a virtual machine is inadvertently placed onto an inappropriate network. For example, an administrator could make an error and select the wrong network. In this case, particularly if one of the networks contains especially sensitive information, it would be very desirable to be alerted whenever a virtual machine is connected to a network. The admin could then verify if the virtual machine indeed belongs on that network, or if it should be taken off.

vCenter has the ability to alert for connection to a distributed switch. Therefore, to implement the scenario above, you would need to create a separate distributed switch for the monitored network.

*NOTE: You cannot set an alert for an individual port group on a distributed switch, only on the switch itself.*

**Step 1:** Configure a vNetwork Distributed Switch

To start, create two distributed switches, as described in Section 3.2. The configuration used in this example is described in the following table and illustrated in Figure 3.6 a.

| DISTRIBUTED SWITCH | PORT GROUPS | COMMENT |
|---|---|---|
| dvSwitch | dv-VM01, dv-VM02, dv-VM03 | Unmonitored networks |
| dvSwitch2 | dv-VM04 | Monitored Network |

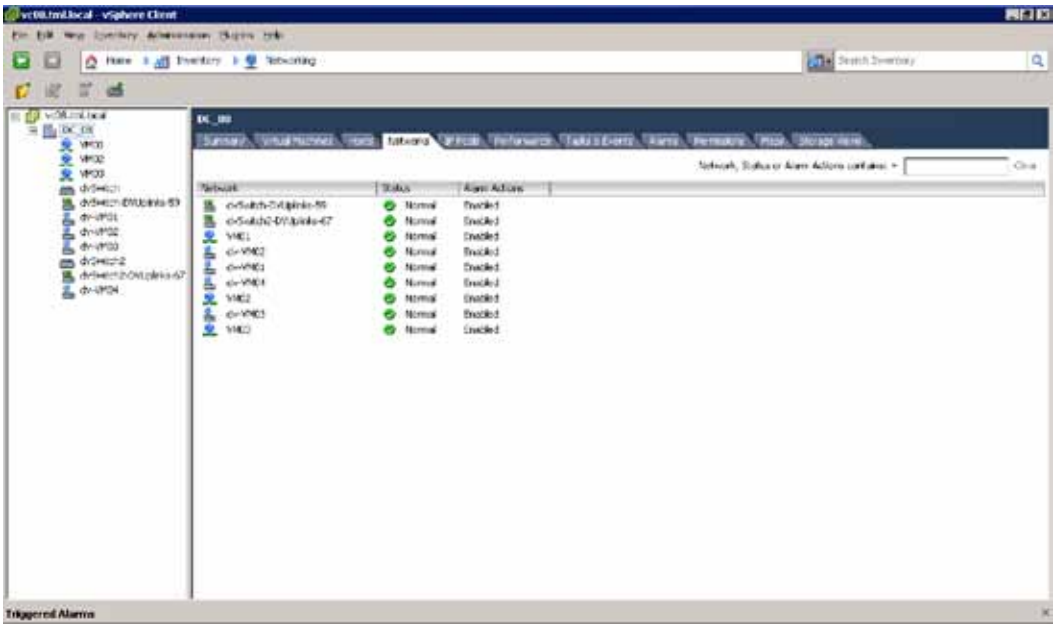


**Figure 3.6 a.** Configuration of Networks

**Step 2:** Set up a custom network alarm

- Navigate to the **Hosts and Clusters** view in the vSphere Client, clicking on the top level of the hierarchy in the left-hand tree (vc08.tml.local) and then selecting the **Alarms** tab.
- Start the creation of a new alarm, either by selecting the menu item **File** > **New** > **Alarm**, or by typing **Ctrl-M**.

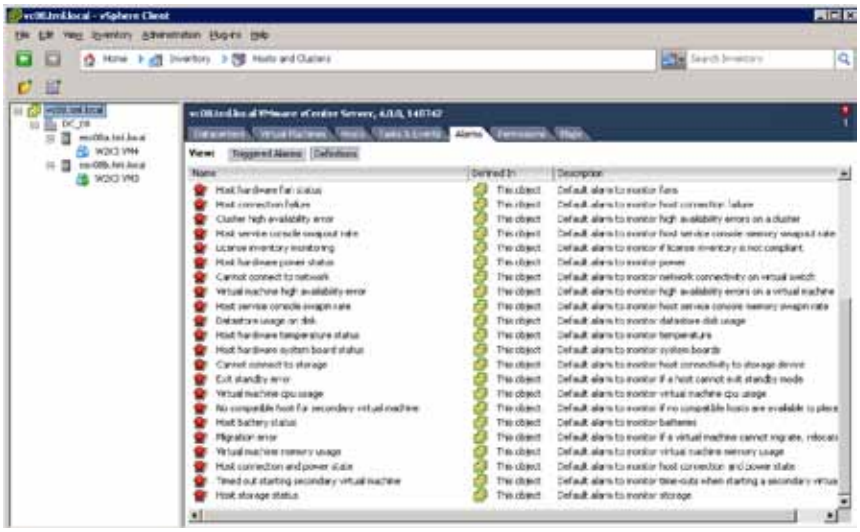


**Figure 3.6 b.** Alarms screen

- On the **General** tab, set Alarm type to monitor **Distributed Virtual Switches**.

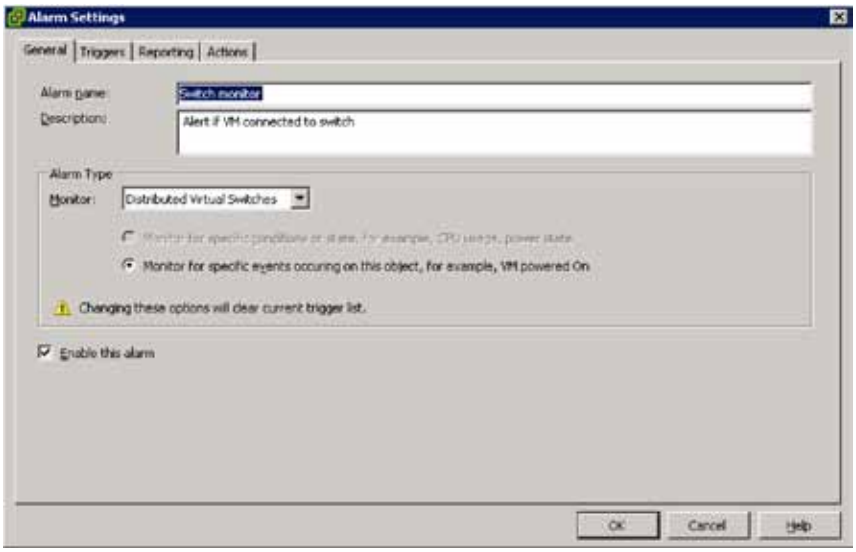



**Figure 3.6 c.** Setting Alarm Description and Type

- On the **Triggers** tab, click **Add** and then select **Distributed Virtual Switch port connected**.

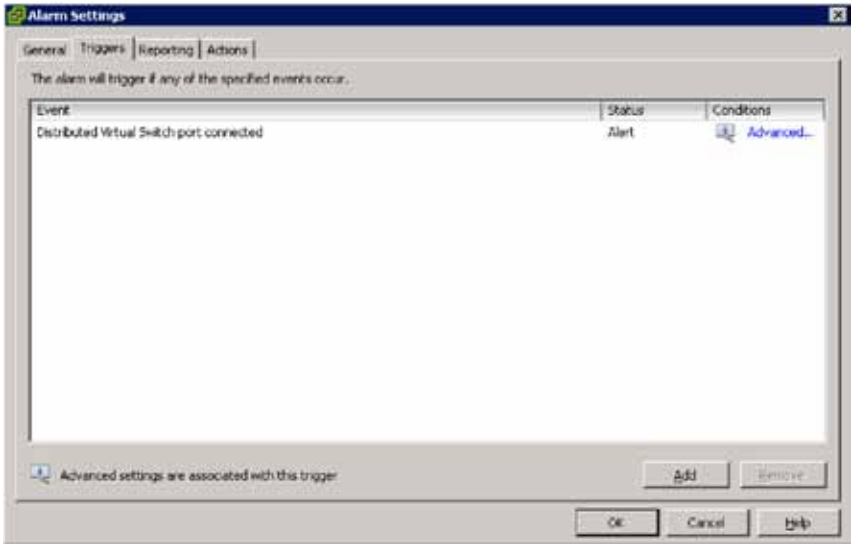



**Figure 3.6 d.** Setting the Alarm Trigger

- After adding the trigger, click **Advanced** and click **Add**. Create a line using the dropdown menus and text box which indicates "DVS Name", "equal to", "dvSwitch2"

*NOTE: Without the advanced setting, the alarm would be triggered for all distributed switches, not just the monitored one.*

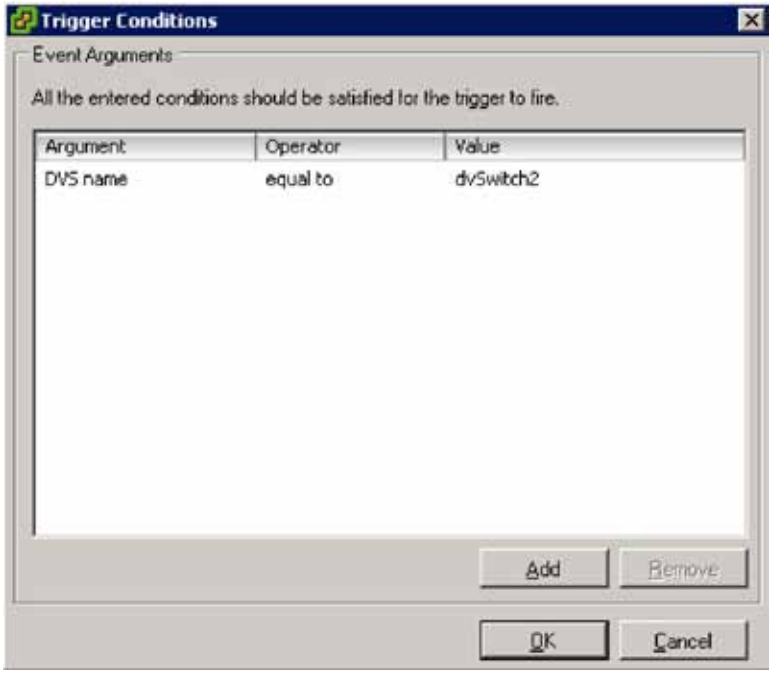



**Figure 3.6 e.** Configuring an Advanced Trigger Condition

### Step 3: Trigger the alarm

Now that the alarm has been configured, test it by re-configuring a virtual machine to use a network on the monitored switch. One virtual machine whose network is on an unmonitored switch, in this case, "dv-VM01" is shown below.

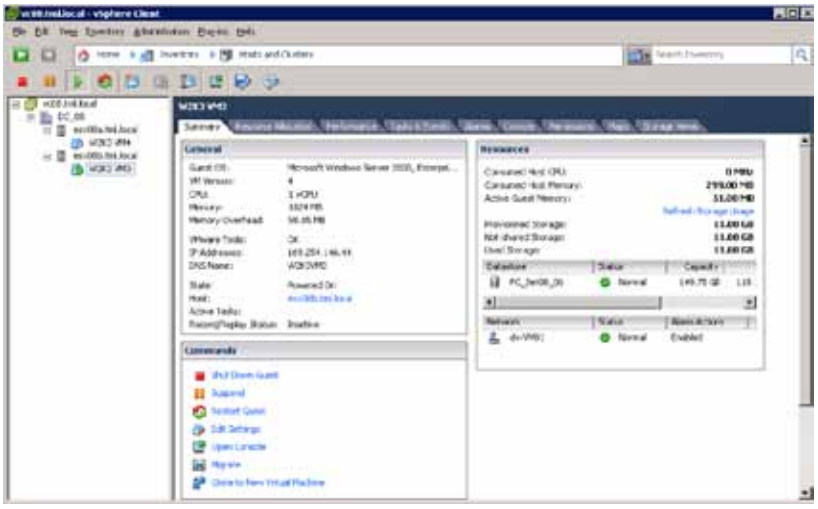


**Figure 3.6 f.** Virtual Machine on an Unmonitored Network

1. Click **Edit Settings** and in the Virtual Machine Properties window, select the **Network Adapter** item. From the dropdown menu under Network Label, select a port group on the monitored switch (in this case "dv-VM04"). After you click **OK**, the virtual machine will be reconfigured to use the selected network.

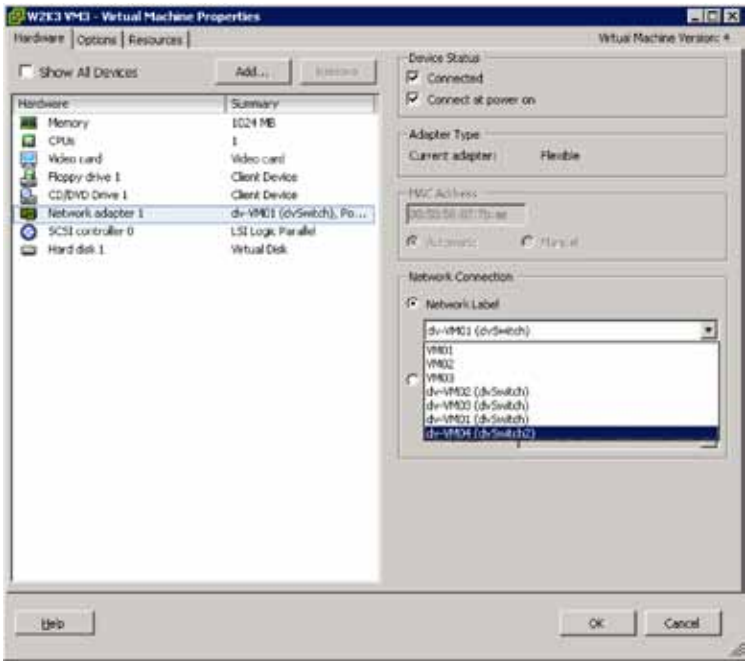



**Figure 3.6 g.** Selecting a Monitored Network

2. Click **Alarms** in the lower left corner of the vSphere client to show a list of currently triggered alarms. You should see the network monitor alarm listed as shown below.

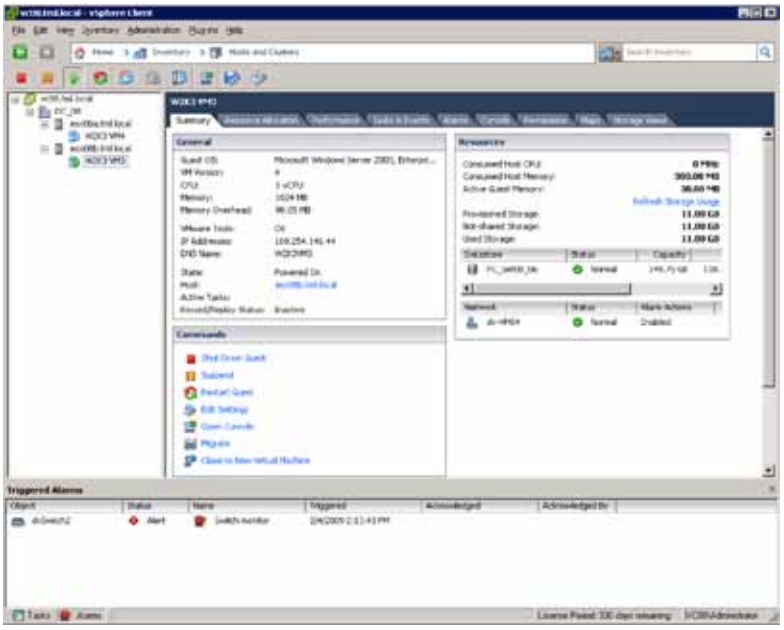


**Figure 3.6 h.** Triggered Alarm

## 3.7. Management Assistant (vMA)

| | | | |
|---|---|---|---|
| Programmability | vSphere Management Assistant (vMA) | 3.7 Using vMA to interact remotely with ESX and ESXi<br><br>Adding a vSwitch to an ESX host, creating a portgroup and adding an uplink<br>1. Adding target hosts to vMA<br>2. List the vSwitches on the host<br>3. Add a vSwitch to the host, add a portgroup and an uplink | 10 minutes |
| | | Gathering logs from multiple ESX and ESXi hosts<br><br>1. Adding target hosts to vMA<br>2. Setting Up Log Collection for ESX/ESXi Hosts | 10 minutes |

**What It Is:** The vSphere Management Assistant (vMA) is a virtual machine that enables administrators to run scripts that interact with ESX/VMware ESXi and vCenter Server without requiring explicit authentication for each script. vMA can also gather logging information from ESX/VMware ESXi and vCenter Servers and collect the log files on vMA for analysis. In addition, VMware partners are developing agents designed to interact with ESX/VMware ESXi and vCenter Server, and to be deployed on vMA.

VMware recommends using vMA as a single standard, consistent environment where administrators can deploy scripts and agents that can access multiple ESX/VMware ESXi and vCenter Servers.

In this section you will:

1. Add a vSwitch to an ESX host, create a port group and add an uplink
2. Gather logs from multiple ESX and VMware ESXi hosts

For instructions on how to install and configure vMA, please see the vSphere Management Assistant guide.

**Use Case:** Adding a vSwitch to an ESX host, creating a port group and adding an uplink

vMA can be used to run vSphere Command-Line Interface (vSphere CLI) commands that can connect to multiple ESX and VMware ESXi hosts to perform network management. The following shows how a vSphere CLI command can be used in vMA to add a vSwitch, add a port group and enable an uplink for the port group.

The vSphere authentication component of vMA (vi-fastpass) supports unattended authentication to ESX/VMware ESXi and vCenter Servers. After vi-fastpass has been enabled, applications can use the vSphere CLI without user intervention.

When you add an ESX/VMware ESXi host as a target host, vi-fastpass creates two users with obfuscated passwords on the ESX/VMware ESXi host:

1. vi-admin (user with administrator privileges)
2. vi-user (user with read-only privileges)

vi-fastpass stores the users' obfuscated password information for the host on vMA.

**Step 1:** Adding target hosts to vMA

1. Login to vMA as the administrator user (vi-admin).
2. Run **addserver** to add a host as a vi-fastpass target.
   **sudo vifp addserver <servername**>

3. Run the vMA command vifpinit to initialize vi-fastpass for the use of vSphere CLI scripts on the target hosts.vifpinit <targetserver>

**Step 2:** List the vSwitches on the host
Run **vicfg-vswitch --list** to list all the current vSwitches and port groups configured on the host.

**vicfg-vswitch --server <servername> --list**

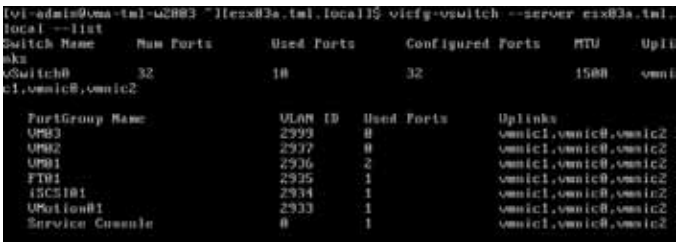



**Figure 3.7 a.** Listing all the vSwitches and port groups on a host

**Step 3:** Add a vSwitch to the host, add a port group and an uplink

1. Run **vicfg-vswitch --add** to create a new vSwitch on the host.

   vicfg-vswitch --server <servername> --add <vSwitch_name>

2. Run **vicfg-vswitch --add-pg** to create a new port group on the vSwitch.

   vicfg-vswitch --server <servername> --add-pg <PortGroup_name> <vSwitch_name>

3. Run **vicfg-vswitch —link** to add an uplink adapter (physical NIC) to the virtual switch.

   vicfg-vswitch —-server <servername> --link <vmnic_name> <vSwitch_name>

4. Run **vicfg-vswitch --list** to verify that the new vSwitch is now created on the host.

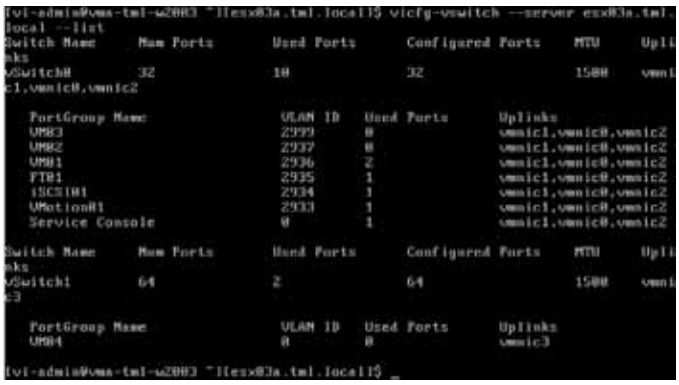



**Figure 3.7 b.** Listing of vSwitches on the VMware ESXi host showing newly added vSwitch1, port group VM04 and uplink vmnic3

**Use Case:** Gathering logs from multiple ESX and VMware ESXi Hosts

vSphere Management Assistant can connect to multiple ESX, VMware ESXi and vCenter Servers in the inventory and gather the logs of all the boxes.

You will add target ESX and VMware ESXi systems to vMA and gather the logs.

**Step 1:** Adding target hosts to vMA

1. Login to vMA as the administrator user (vi-admin).
2. Run **addserve**r to add a host as a vi-fastpass target.

   **sudo vifp addserver <servername**>
3. Next, you are prompted for the root user for the target host as follows:

   **root@<servername**>**'s password:**
4. Supply the root password for the ESX/VMware ESXi host you want to add.
5. Repeat steps 2 through 4 for each host that you wish to add as a vMA target host.
6. Run **vifp listservers** to verify that the target hosts have been added.


**Figure 3.7 c.** Adding target host to vMA

7. In this guide 2 target hosts have been added.
   a. 1 ESX 4.0 host
   b. 1 VMware ESXi 4.0 host

**Step 2:** Setting Up Log Collection for ESX/VMware ESXi Hosts
The vilogger interface can be used to have vMA collect log files from the target

ESX/VMware ESXi hosts according to the specified log policy.

1. Run **vilogger enable** for the hosts that you wish to enable logging for.

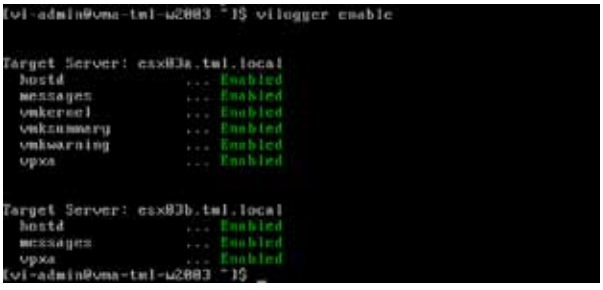



Figure 3.7 d. Enabling logging on target hosts

2. Run **vilogger list** to list the names of all the logs available for collection from the target hosts.

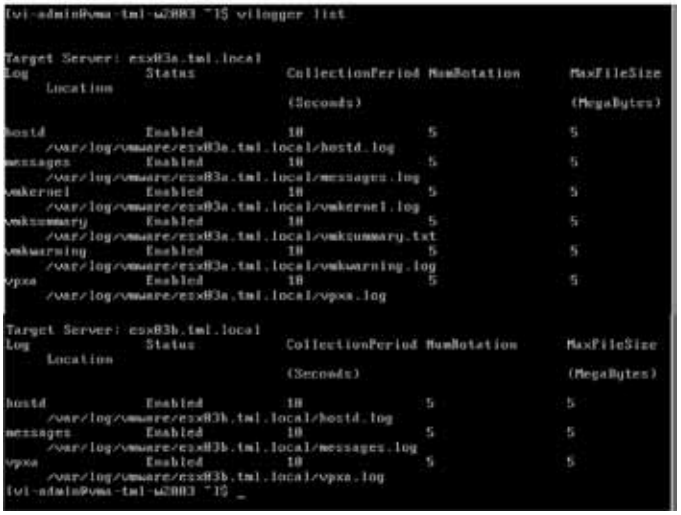



**Figure 3.7 e.** Listing showing location of logs in vMA, collection period, number of log rotations to maintain and maximum size log can grow before it is rotated.

## 3.8. PowerCLI

| | | | |
|---|---|---|---|
| Programmability | PowerCLI | 3.8 Using PowerCLI to perform vSphere management tasks<br><br>1. Enabling VMotion on all VMs<br>2. Storage VMotion with PowerCLI<br>3. Simple Automated Reporting with PowerCLI | 60 minutes |

**What It Is:** VMware vSphere PowerCLI is a powerful tool for managing and automating VMware vSphere. Graphical tools like VMware vSphere Client are very easy to use when configuring or deploying vSphere or the VMs within them. However, when you find that you need to do something dozens, or even hundreds of times, you need to automate. PowerCLI provides an extremely powerful command line environment, and along with the very active community VMware has built around it, it's one of the best ways to automate your vSphere environment.

VMware vSphere PowerCLI provides a rich set of functionality, but some of its most important uses include:

- Provisioning an enormous volume of VMs all at once
- Simultaneously transforming large numbers of VMs
- Adding storage to a mass of ESX hosts all at the same time
- Configuring network resources altogether across a multitude of ESX hosts

*System Requirements:*
1. Windows XP, 2003, Vista or 2008

*Hardware Requirements:*
1. 256MB of RAM or higher.
2. 500MHz CPU or higher.
3. 100MB of disk space.

*Software Requirements:*

1. Windows PowerShell (available as a free download from Microsoft).

*Getting Started with PowerCLI.*

PowerCLI is based on Microsoft Windows PowerShell, which is an automation framework used by Microsoft's server technologies. PowerShell offers an extensible framework that allows management packs called "snap-ins" to be easily added by Microsoft and by 3rd parties. Commands in PowerShell are called "cmdlets," and are small, reusable pieces of management logic that can be easily combined to form very powerful management applications.

PowerCLI adds 165 cmdlets to PowerShell that cover all aspects of managing and automating VMware vSphere.

PowerCLI is a standalone tool that can be downloaded by visiting http://vmware.com/go/powershell. Once you've installed PowerCLI you can launch it by navigating to **Start** > **VMware** > **VMware vSphere PowerCLI** > **VMware vSphere PowerCLI**.

The first time you launch PowerCLI, you will be prompted whether you want to run software from an untrusted publisher. The PowerCLI code is digitally signed by VMware, but chances are you don't have VMware in your list of trusted publishers. You can choose to "Run once" (R) or "Always run" (A). Choosing "Always run" is recommended. It will prevent you from having to answer this question in the future.

By default, PowerShell is configured with a very restrictive security policy that doesn't allow scripts to be run. Relaxing this policy is recommended, both because scripts are very useful, but also because you get a more user friendly experience if you allow running scripts. If you want to run scripts, you must first type this command at the prompt: Set-ExecutionPolicy RemoteSigned.

If you allow scripts and re-start PowerCLI, you will see this welcome screen:

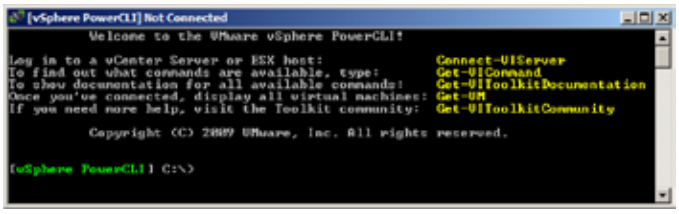



**Figure 3.8 a.** The Welcome Screen

From here, you can see a listing of all command shipped with PowerCLI by typing **Get-VICommand**. As mentioned before, there is quite a large set of cmdlets, 165 in total. In the remainder of this section, you will go through a number of samples that will give you an idea of the power of PowerCLI. Since it's impossible to cover such a large set of commands in such a short time, you will instead see a few useful examples that will give you a feel for what you can do with PowerCLI. Online resources that you can use to help you get started are mentioned at the end of this section.

The first thing you will need to do after starting PowerCLI is log in to your vCenter server or ESX host. You do this using the Connect-VIServer command. Connect-VIServer requires an argument that specifies the host name or IP address of your vCenter or ESX host. When you connect you will be prompted for credentials as depicted below. Log in using the same credentials you would use if you were using VSphere Client.

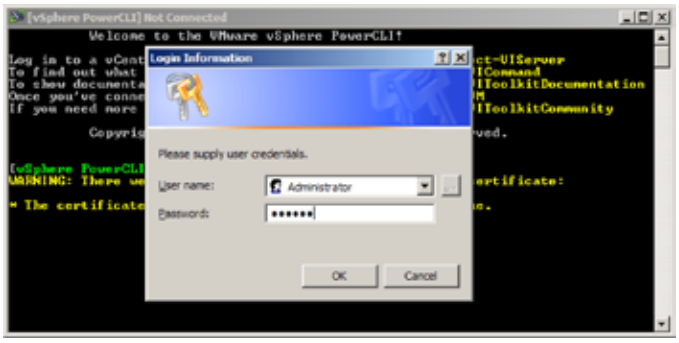



**Figure 3.8 b.** Log In

When you log in, you will see connection information in the window's title bar. Now that you are logged in, take a look at some of the power of PowerCLI.

**Step 1:** Enabling VMotion on all VMs

VMotion allows VMs to be moved from one ESX host to another while the VM is still running. However, if a VM has floppy or CD-ROM drives connected, VMotion can fail. This creates an operational challenge to using VMotion, because it's very difficult within the VSphere Client to determine if there are any connected CD-ROM drives within a large set of VMs. So in this section, you will take a look at how easy it is with PowerCLI to ensure that all CD-ROM drives are disconnected. Running scripts like this on a periodic basis gives you assurance that VMotion will work when you need it to.

First, see if there are any connected CD-ROM drives. Do this using the following command:

- Get-VM | Get-CDDrive | Select —Expand ConnectionState

(Note that PowerShell is case insensitive.) When you do that, you get output as shown here.

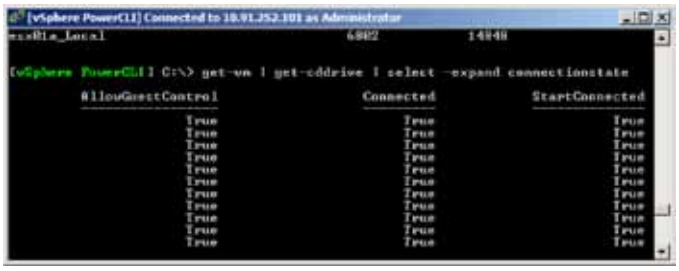



**Figure 3.8 c.** CD-ROM Connection State

You can do this in your environment to get a similar report. Notice that you have a number of connected CD-ROM drives. To disconnect all these drives run:

- Get-VM | Get-CDDrive | Set-CDDrive —connected:$false —confirm:$false

You can see the results of this command here.

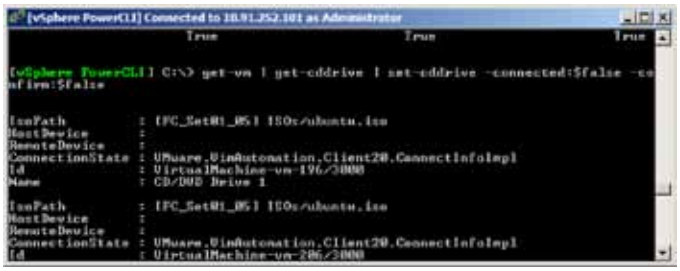



**Figure 3.8 d.** Detaching CD-ROM Drives

Finally, re-run the report to make sure the changes have been successful.

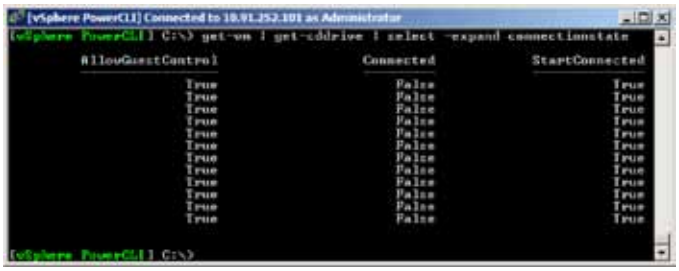



**Figure 3.8 e.** Updated Status with CD-ROM Drives Detached

**Step 2:** Storage VMotion with PowerCLI
The last example explained a bit about VMotion, which lets you move a VM from one ESX host to another. Storage VMotion is similar, but instead of changing the ESX host where a VM runs, it changes the storage that a VM uses. Storage VMotion is extremely valuable, for example if you have a VM on a storage array that is running out of space. With Storage VMotion, it is very easy to move the VM to another storage array while it is still running.

Because Storage VMotion relocates all VM data, it can take a very long time to execute, so if you need to move lots of VMs, it's great to be able to script it.

Below you see that the environment has one datastore that is nearly full, and one datastore that is hardly used at all.

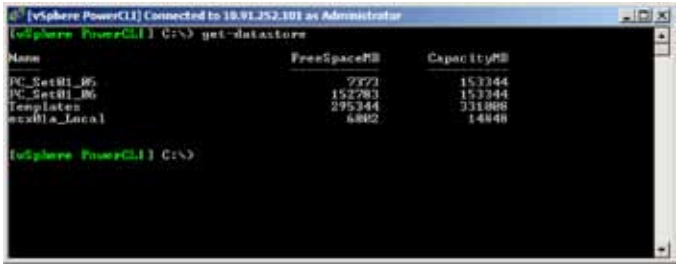



**Figure 3.8 f.** The Current State of Datastores

PowerCLI makes it easy to determine what VMs are located on a datastore using this command:

- Get-Datastore FC_Set01_05 | Get-VM

(If you want to try this for yourself, you should use your own datastore name in place of FC_Set01_05.)

The results of this are shown here:

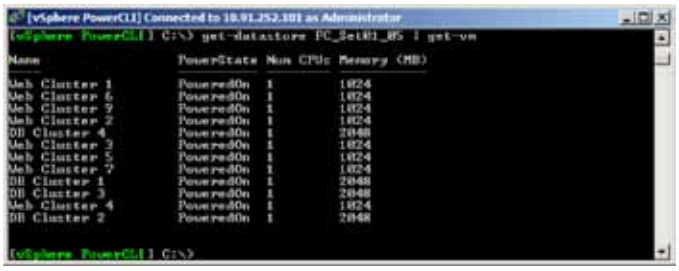



**Figure 3.8 g.** Listing all VMS on a Particular Datastore

Now you'll want to move a number of these VMs from the nearly-full datastore to the datastore that is almost empty. To do this use the Move-VM cmdlet as follows:

- Get-VM DB* | Move-VM —Datastore FC_Set01_06

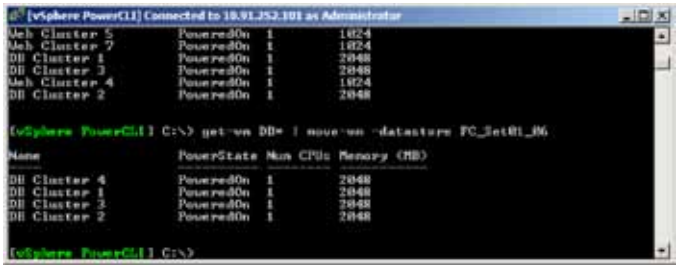



**Figure 3.8 h.** Storage Motion is Easy with the Move-VM cmdlet

Read this command starting at the beginning. First, get all VMs that start with DB (i.e. DB Cluster 1, DB Cluster 2, etc.). Then pipe those results into the Move-VM cmdlet. Give Move-VM a parameter of —Datastore FC_Set01_06, which instructs it to move these VMs to the new datastore.

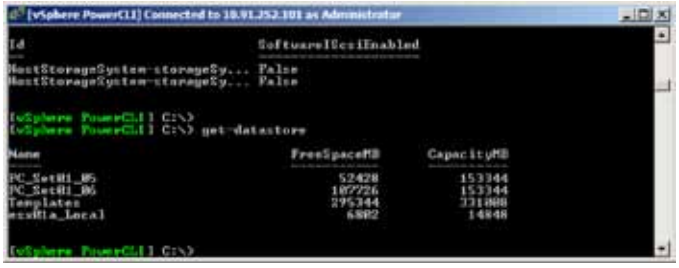



**Figure 3.8 i.** After Moving Several VMs, Storage Usage is More Balanced

After moving these VMs there is plenty of space on FC_Set01_05. The Move-VM cmdlet is extremely powerful. It also allows you to VMotion VMs, or to perform migration, and its ability to easily move multiple VMs makes it a very useful and powerful resource.

**Step 3:** Simple Automated Reporting with PowerCLI.

Many users have found PowerCLI to be a good tool for simple, automated reporting. PowerCLI scripts can be scheduled using the Windows Task Scheduler, and scripts can be written to email results directly to you. In this section, we'll take a look at some simple reports you can write with PowerCLI. Many more examples are available through online resources. This section goes through a number of simple reports users find extremely helpful.

The first report simply shows how to count up all VMs in your environment.

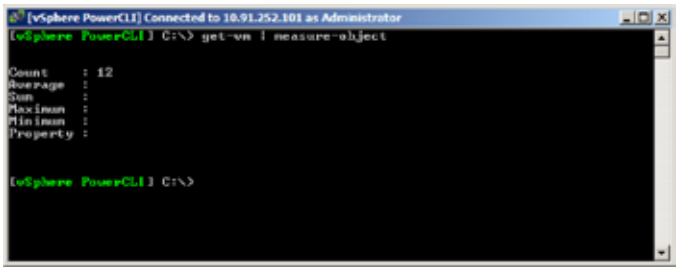



**Figure 3.8 j.** Counting the Total Number of VMs

There's no real magic here, but this same command works whether you have 1 host or 50 hosts, and when run periodically can help you keep an eye on VM expansion. The next example shows how to count up all snapshots. This example is a bit more interesting because snapshots tend to be hard to find.

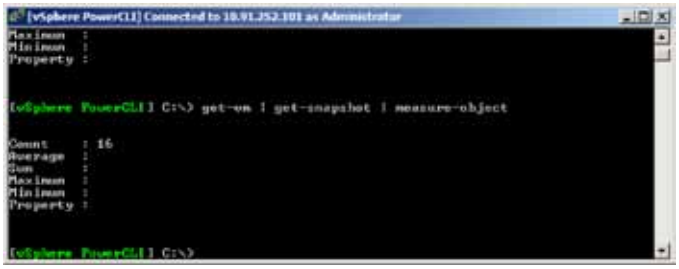



**Figure 3.8 k.** Counting the Number of Snapshots

PowerCLI also makes it easy to determine the age of snapshots, as follows:

- Get-VM | Get-Snapshot | Select Name, VM, Created

Snapshots that are more than a week old deserve special scrutiny, since it's easy to forget to clean them up, and they can fill up your datastores.

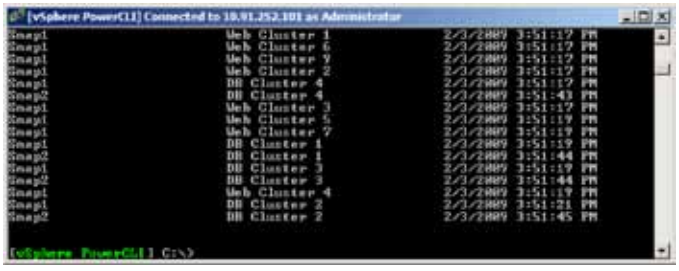



**Figure 3.8 l.** Showing the Age of Snapshots

To summarize, in addition to the extremely powerful automation capabilities PowerCLI brings, it's also a very handy tool for writing simple reports that can help you understand and monitor your environment.

# Conclusion

VMware vSphere provides virtualization, management, resource optimization, application availability, and operational automation capabilities in an integrated package. Its features are tailored for datacenters that require high availability, high performance, and low administration and operation costs. No other virtualization products provide the level of reliability, performance, feature richness, and cost savings that are available from vSphere. This guide covered details on how to configure and use these high performance vSphere features and how they compare to offerings from other vendors. After going through the evaluation exercises in this guide, it should be clear that VMware vSphere delivers capabilities far exceeding those of products from Microsoft, Citrix, and other virtualization competitors.

Figure 5 a provides a summary view of all the vSphere 4 features.

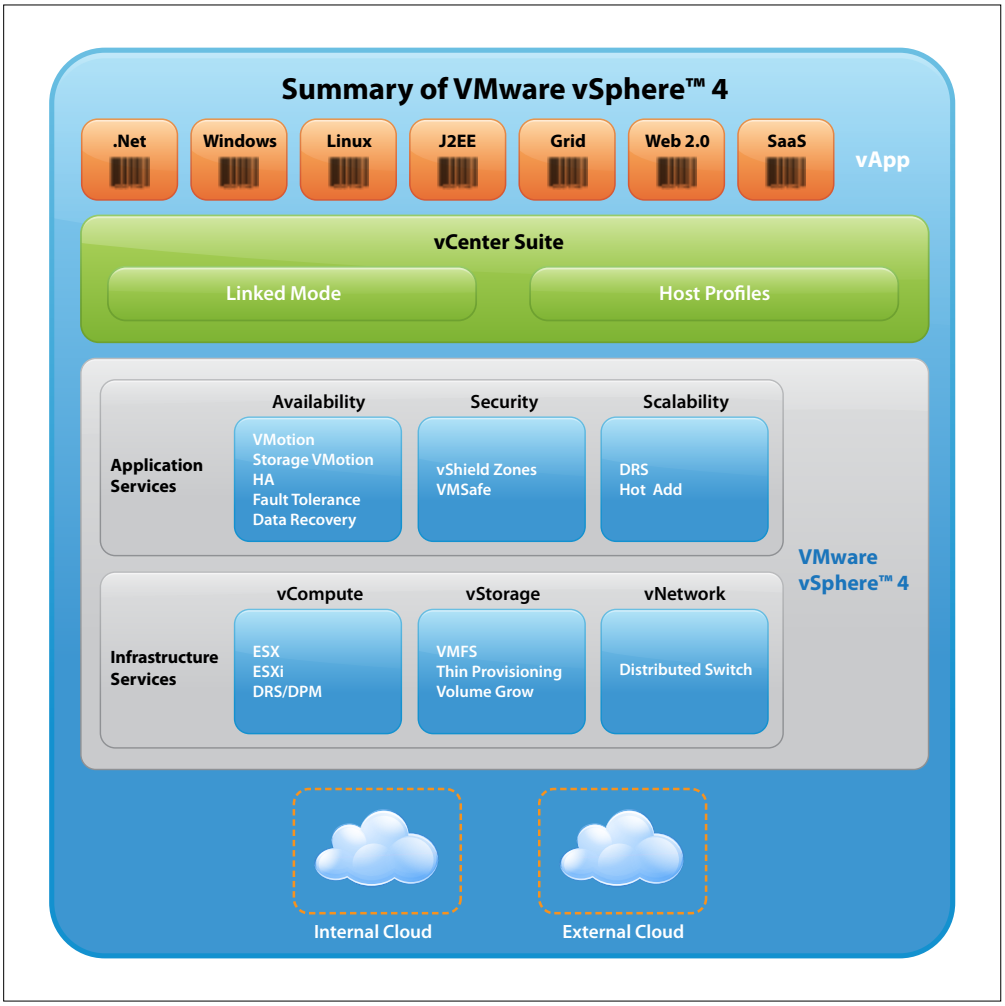



**Figure 5 a.** Summary of all vSphere 4 Features

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com