

VMware vSphere[®] 5.0 Evaluation Guide

Volume One

TECHNICAL WHITE PAPER V 1.1/UPDATED AUGUST 11 2011

vmware[®]

Table of Contents

About This Guide
Intended Audience
System Requirements 5
Hardware Requirements
Servers
Storage
Networking
Software and Licensing Requirements6
VMware vSphere
Guest Operating Systems6
Evaluation Guide Environment Setup
Server Configuration
Logical Network Setup
Storage Setup
Virtual Machine Setup
VMware vSphere 5.0 Evaluation Guide, Volume One - Worksheet
vSphere Evaluation Tasks 12
High Availability
Introduction
Prerequisites
Enabling HA
Connect to Virtual Server
Go to Cluster Summary14
Edit Cluster Settings
Wait for Task to Complete
Verifying VMware HA Enablement16
HA Status Screen
Virtual Machine Protection State 20
Host Protection State
VMware HA Advanced Options
Admission Control
Virtual Machine Options
Virtual Machine Monitoring
Storage Heartbeats
Validating VMware HA Operation 29
Host Failure

	Host Isolation	34
	Disabling VMware HA	.43
	Connect to a Virtual Server	.43
	Go to the Cluster Summary	44
	Edit Cluster Settings	.45
	Wait for Task to Complete	46
Getti	ing Familiar with the New Command-Line Interface	46
In	troduction	46
	The New esxcli Command	.47
	esxcli Command-Line Syntax	.47
	Remote esxcli Command Authentication	.49
	Enabling Access to the ESXi Shell	50
	Enabling the ESXi Shell from the DCUI	50
	Enabling the ESXi Shell from the vSphere Client	50
	Enabling SSH Access to the ESXi Shell	.51
	Enabling SSH from the DCUI	.51
	Enabling the SSH from the vSphere Client	.52
	vSphere Client Notification When the ESXi Shell and SSH Are Enabled	.53
	Installing the vCLI	.53
	Installing the vCLI on Windows	.53
	Installing the vCLI on Linux	.53
	Installing the vCLI with the vMA	.53
	Sample esxcli Commands Run Locally from the ESXi Shell	54
	Sample esxcli Commands Run Remotely from the vCLI	.56
	Formatting esxcli Output	58
	The localcli Command	.59
	Bringing It All Together	60
VS	Sphere PowerCLI by Example	.62
	Introduction	.62
	Prerequisites	.62
	Install vSphere PowerCLI	.62
	Getting Started with vSphere PowerCLI	.69
	Connecting to a vSphere Host or vCenter	.69
	Using vSphere PowerCLI	.71
	vSphere PowerCLI Summary	.81
E١	valuating the ESXi Firewall	.81
	Introduction	.81

Evaluation Overview	81
Prerequisites	81
Stopping SSH Service to Prevent Access	81
Testing Access with SSH Service Stopped	85
Creating Firewall Rules to Block SSH Access	86
Testing SSH Firewall Rules	89
Image Builder	
Introduction	
Image Builder Prerequisites	92
Preparation Tasks	92
Install vSphere PowerCLI	92
Download the ESXi Offline Bundle	92
Extract the ESXi Offline Bundle	92
Start an Image Builder vSphere PowerCLI Session	92
Import the ESXi Offline Bundle	94
Display Software Depots	
Display VIBs	95
Display Image Profiles	95
Create a New Image Profile	96
Create a New Image Profile by Manually Selecting Individual VIBs	96
Create a New Image Profile by Cloning an Existing Image Profile	98
Removing VIBs from an Image Profile	98
Compare Image Profiles	99
Export Image Profile	99
Export As an Offline Bundle	99
Export As a Bootable ISO Image	100
Product Documentation	100
Using Storage Performance Statistics	101
Introduction	101
Monitoring Performance Statistics of a Datastore	103
Help and Support During the Evaluation	105
VMware Contact Information	105
Providing Feedback	105

About This Guide

The purpose of the VMware vSphere 5.0 Evaluation Guide, Volume One, is to support a self-guided, hands-on evaluation of VMware vSphere[®] 5.0 ("vSphere") features usable by all VMware vSphere customers. The companion guide, the VMware vSphere 5.0 Evaluation Guide, Volume Two, is intended to highlight vSphere 5.0 features primarily targeted at larger, more complex deployment environments.

Intended Audience

This guide is intended to cover evaluation cases that are suitable for IT professionals who fulfill the following requirements:

- They understand the basics of server virtualization and want to evaluate the features in vSphere in a smallscale deployment.
- They have an existing VMware virtualization environment and want to evaluate features in vSphere that enable greater consolidation while maintaining service levels.

System Requirements

To ensure the best experience when using this guide, the user will need to configure hardware and software as detailed in the following section.

Hardware Requirements

This guide makes the following assumptions about your existing physical infrastructure:

Servers

You must have at least three dedicated servers capable of running VMware ESXi[™] 5.0 to provide resources for this evaluation.¹

Storage

You must have shared storage with enough space available to allow the creation of three 100GB dedicated datastores. Shared storage can be SAN or NAS. This document assumes SAN-based storage.

Networking

You must have at least three virtual networks configured to separate virtual machine, vMotion, and vSphere management. These networks can be set up on a single virtual switch with multiple port groups, or across multiple virtual switches. For the purpose of this evaluation guide, the configuration includes a single vSphere standard switch with three port groups.

^{1.} These servers must be on the VMware vSphere 5.0 Hardware Compatibility List (HCL).

HARDWARE	MINIMUM	WHAT'S USED IN THIS GUIDE
ESXi	Three ESXi/ESX servers CPU – Two processors of 2GHz Memory – 6GB Network – 2x 1GB network adaptor	Three ESXi servers (Cisco UCS 1.3.1) CPU – Two quad-core "Nehalem" processors of 2.6GHz Memory – 48GB Network – 4x 10GB network adaptor
Storage	One datastore (100GB)	Three datastores (Fibre Channel – 100GB each)
Network	One VLAN for carrying virtual machine traffic; one VLAN for carrying management traffic	Separate VLANs for ESXi management, vMotion, and virtual machine traffic

For more detailed requirements, see the following table.

Software and Licensing Requirements

This guide makes the following assumptions about your existing software infrastructure:

VMware vSphere

This volume of the *VMware vSphere 5.0 Evaluation Guide* requires vSphere 5.0 and licensing for Essentials Plus. If the user intends to also complete the exercises in Volume Two of the *VMware vSphere 5.0 Evaluation Guide*, a license for Enterprise Plus will be required. The vSphere 5.0 evaluation license available from the VMware evaluation portal provides Enterprise Plus functionality for 60 days and is the best choice for performing the vSphere 5.0 evaluations.

Guest Operating Systems

This volume of the VMware vSphere 5.0 Evaluation Guide does not place any specific requirements on guest operating systems, other than ensuring that you can deploy running virtual machines. The user is free to deploy any VMware-supported operating system (OS) in the virtual machines. The VMware vSphere 5.0 Evaluation Guide, Volume Two, will require five or six virtual machines running Windows 2003 or Windows 2008.

Evaluation Guide Environment Setup

The VMware Technical Marketing lab was built using a combination of Cisco UCS server hardware and EMC CLARiiON CX-4 Fibre Channel (FC) storage. The environment consisted of eight identical four-node "pods," with most pods configured as a three-node ESXi cluster and a fourth node for management. In many cases, additional resources have been configured in the Technical Marketing test-bed configuration to support other evaluation projects, and are present in the diagrams. The user can configure only what is called for in the following section and can safely ignore additional resources in screen shots and topology diagrams. The following picture shows the Technical Marketing test rack.



Server Configuration

The VMware vSphere 5.0 Evaluation Guide calls for three modern server-class systems with adequate processors and memory to host 6–8 minimally configured virtual machines used for testing. The servers used for this evaluation do not need to be overly powerful, just reliable and on the vSphere 5.0 HCL.

Each server must have at least 2x 1GB or 2x 10GB network adaptor and proper connection to shared storage. The following diagram summarizes the evaluation guide test-bed configuration.



Logical Network Setup

The VMware vSphere 5.0 Evaluation Guide, Volume 1, uses a very simple network configuration consisting of three logical networks. The first is for vSphere management traffic, including vSphere High Availability (VMware HA). The second is for VMware vSphere® vMotion® and the third is for virtual machine traffic. Each logical network is configured as a port group on a standard switch, with a corresponding VLAN configured to provide physical isolation of the network traffic.



On the vSphere side, the network configuration looks like the following:



Storage Setup

The VMware vSphere 5.0 Evaluation Guide, Volume One, uses a storage configuration consisting of three 100GB FC LUNs presented to each host, enabling creation of three datastores.

m-pod01-esx01.tmsb.local VMware ESXi, 5.0.0, 413596 Getting Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permissions Maps Storage Views Hardware Status							
Hardware	View: Datastores Devices						
Processors	Datastores			Refresh	Delete	Add Storage R	escan All
Memory	Identification	Status	Device	Drive Ty	Capacity	Free Type	Last Upd
 Storage 	· · · · ·		in the second second				
Networking	TM-POD01-ESX01-Local	🤝 Normal	FUJITSU Serial Attached SCSI Disk (naa	Non-SSD	132.00 GB	131.04 GB VMFS5	6/14/201
Storage Adapters	👔 tm-pod01-sas300-sp	🤣 Normal	DGC Fibre Channel Disk (naa.60060160	Non-SSD	99.75 GB	26.69 GB VMFS5	6/14/201
Network Adapters	tm-pod01-sas600-sp-01	🤣 Normal	DGC Fibre Channel Disk (naa.60060160	Non-SSD	99.75 GB	45.63 GB VMFS5	6/14/201
Advanced Settings	🗊 tm-pod01-sas600-sp-02	🤣 Normal	DGC Fibre Channel Disk (naa.60060160	Non-SSD	99.75 GB	58.65 GB VMFS5	6/14/201
Power Management							
Software							
Licensed Features							
Time Configuration	•						F
DNS and Routing				-			
Authentication Services	Datastore Details					F	roperties
Power Management							
Virtual Machine Startup/Shutdown							
Virtual Machine Swapfile Location							
Security Profile							
Host Cache Configuration							
System Resource Allocation							
Agent VM Settings							
Advanced Settings							
L							
	I						

Virtual Machine Setup

The VMware vSphere 5.0 Evaluators Guide, Volume One, uses a total of six to seven virtual machines for testing. These can be Linux or Windows virtual machines. It is up to the user to configure virtual machines that can be brought up to a running state for testing. The following diagram shows VM_01 through VM_07 configured in the Technical Marketing test lab:



VMware vSphere 5.0 Evaluation Guide, Volume One - Worksheet

You can use the following worksheet to organize your evaluation process.

HARDWARE CHECKLIST:	
All hardware has been validated against the VMware vSphere 5.0 Hardware Compatibility List (HCL).	
Each server has 2x 1GB or 2x 10GB network cards connected to a common switch (this will be configured as a network adaptor team).	
Each server has the required HBA/network adaptor to access shared storage.	

SOFTWARE CHECKLIST:	
VMware vSphere/VMware ESXi installation media is available.	
VMware vCenter™ Server appliance is downloaded.	
VMware vSphere® Client™ is installed.	
ESXi host 1 hostname.	
ESXi host 2 hostname.	
ESXi host 3 hostname.	
Subnet, netmask and default gateway for management network.	
Subnet, netmask and default gateway for virtual machine network.	
Subnet, netmask and default gateway for vMotion network.	

STORAGE CHECKLIST:	
All servers can see at least three common 100GB LUNs (or NFS exports).	
Datastore 1 name.	
Datastore 2 name.	
Datastore 3 name.	

vSphere Evaluation Tasks

High Availability

Introduction

Ensuring the availability of virtual machines within an environment is of paramount concern to administrators. VMware HA alleviates these concerns by providing protection from failures within the following three key layers:

• The infrastructure layer

At this layer, VMware HA monitors the health of the virtual machine and will attempt to restart the virtual machine when a failure, such as the loss of a physical host, occurs. This protection is independent of the OS used within the virtual machine.

• The OS layer

Through the use of VMware Tools installed within the OS, VMware HA can monitor the OS for proper operation. This protects against such failures as an unresponsive OS.

• The application layer

With some customization or with a third-party tool, an administrator can also monitor the application running within the OS for proper operation. In the event of a failure of the application, HA can be triggered to restart the virtual machine hosting the application.

In this section, you will learn how to enable, configure, and test the operation of HA to provide basic high availability services for your virtual machines at the infrastructure layer.

Prerequisites

Before continuing, it is important that the environment be configured properly. Refer to the "System Requirements" section of this document and verify that the environment you are using is configured as documented. Specific areas of interest include the following:

- Ensure that you have a working management network with all hosts in the environment.
- Verify that all of the virtual machines are online.
- Have at least one virtual machine running on each host.
- Validate that you have access to VMware vCenter™ utilizing the vSphere Client.

Enabling HA

Enabling HA is a straightforward process that simply entails editing the properties for the cluster. The following steps will guide you through this process.

Connect to Virtual Server

🕜 VMware vSphere Client	
vmware [.] VMware vSphere Client	
To directly manage a sing To manage multiple hosts, vCenter Server.	e host, enter the IP address or host name. , enter the IP address or name of a
IP address / Name:	tm-pod01-vc01
User name:	root
Password:	*******
	Use Windows session credentials
😲 Connecting	Login Cancel Help

Figure 1. Connecting to Virtual Server

Using the vSphere Client, connect to your virtual server instance.

🕗 tm-pod01-vc01 - vSphere Client						
File Edit View Inventory Administration Plug-ins Help						
C E Home D B Inventory D B Hosts and Clusters						
li e si						
tm-pod01-vc01 bemoDatacenter-01 bemoCluster-01 bemoCluster-01 tm-pod01-esx01.tm	DemoCluster-01 Getting Started Summary Virtu	al Machines Hosts DRS Resour	ce Allocation Performance			
tm-pod01-esx02.tm	General		vSphere DRS			
 tm-pod01-esx03.tm VM_01 VM_02 VM_03 VM_04 VM_05 VM_06 VM_07 	vSphere DRS: vSphere HA: VMware EVC Mode: Total CPU Resources: Total Memory: Total Storage: Number of Hosts: Total Processors:	On Off Disabled 57 GHz 143.80 GB 1.41 TB 3 24	Migration Automation Li Power Management Au DRS Recommendations DRS Faults: Migration Threshold: Target host load stand Current host load stand View Resource Distribut View DRS Troubleshoo			
	Total Processors: Number of Datastore Clusters: Total Datastores: Virtual Machines and Templates: Total Migrations using vMotion: Commands	24 1 7 13 ¹ ² ² ² ² ² ² ² ²	Storage Storage resources TM-Gobal-Interd TM-POD01-ESX0 TM-POD01-ESX0 TM-POD01-ESX0 TM-POD01-SaS0 tm-pod01-sas60 tm-pod01-sas60 TM-POD01-sas60 TM-POD01-Sas60 TM-PO			

Go to Cluster Summary

Figure 2. Cluster Summary

Once connected to your virtual server instance, select your cluster by clicking on its name on the left-hand panel. Select the **Summary** tab to bring up the cluster summary screen.

🕗 DemoCluster-01 Settings		×
Cluster Features VMware EVC Swapfile Location	Name DemoCluster-01 Features Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance.	
	 Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, groups, and virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies. vSphere DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing. 	
Help	OK Canc	el

Edit Cluster Settings

Figure 3. Editing Cluster Settings

In the cluster summary screen, select the **Edit Settings** option. This will bring up a wizard that you can use to modify the settings of the cluster. Click the check box next to **Turn On vSphere HA** and select OK. This will close the wizard and the system will initialize VMware HA.

Recent Tasks					
Nam	e	Targ	et	Sta	tus
*	Configuring vSphere HA	-	tm-pod01-esx02.tmsb.local	50)%
*	Configuring vSphere HA	-	tm-pod01-esx03.tmsb.local	Ð	In Progress
*	Configuring vSphere HA	-	tm-pod01-esx01.tmsb.local	Ð	In Progress

Figure 4. Initializing VMware HA

Under the Recent Tasks pane of the vSphere Client, you can observe the progress of the initialization of HA on the systems within the cluster. You'll notice that the configuration tasks occur in parallel among all the hosts within the cluster.

Wait for Task to Complete

Name	Target
Configuring vSphere HA	tm-pod01-esx02.tmsb.local
Configuring vSphere HA	tm-pod01-esx03.tmsb.local
Configuring vSphere HA	tm-pod01-esx01.tmsb.local

Figure 5. Tasks Showing Completed Status

Wait until all the tasks show a **Completed** status. This should only take a minute. At this point, VMware HA is now providing protection for the virtual machines that are powered on.

Verifying VMware HA Enablement

At this point, WMware HA should be enabled within your cluster. This section will demonstrate several methods you can use to verify that HA is enabled.

HA Status Screen

🖉 tm-pod	101-vc01 - vSphere Clien	:				
File Edit	ile Edit View Inventory Administration Plug-ins Help					
	🔥 Home 🕨 🚮	inventory 🕨 🇊 Hosts and Clusters				
t 🗗	e #					
- 🕑 tm-	pod01-vc01 DemoDatacenter-01	DemoCluster-01 Getting Started Summary Virtu	ual Machines Hosts Resource Allo	cation Performance Tasks & Events Alarms Permi		
	Im-pod01-esx02.1 Im-pod01-esx03.1 WM_01 VM_02 VM_03 WM_04 VM_04 VM_05 WM_06 WM_06 WM_07	vSphere DRS: vSphere HA: VMware EVC Mode: Total CPU Resources: Total Memory: Total Storage:	Off On Disabled 57 GHz 143.80 GB 1.41 TB	Admission Control: Enabled Current Failover Capacity: 2 hosts Configured Failover Capacity: 1 host Host Monitoring: Enabled VM Monitoring: Enabled Application Monitoring: Disabled Advanced Runtime Info Enabled		
		Number of Hosts: Total Processors:	3 24	Cluster Status Configuration sues		
		Number of Datastore Clusters: Total Datastores:	1 7	Storage Storage resources		
		Virtual Machines and Templates: Total Migrations using vMotion:	7 13	Image: TM-Gobal-Interch Image: Normal Normal Normal Image: TM-POD01-ESX01 Image: Normal Normal Normal Image: TM-POD01-ESX02 Image: Normal Normal Normal Image: TM-POD01-ESX03 Image: Normal Normal Normal Image: TM-POD01-ESX03 Image: Normal Normal Normal		

Figure 6. Configuration of HA

After enabling HA, you will notice that a section for HA is now shown under the cluster summary screen. This will show you general information about the configuration of HA. There is also an option for **Cluster Status** here. Click this to bring up the HA Cluster Status screen.

🕗 vSphere HA Cluster Status F	or DemoCluster-01
Hosts VMs Heartbeat Data	stores
Host Operational Status	
Master: Hosts connected to master:	tm-pod01-esx01.t. 2 tm-pod01-esx01.tmsb.local
	Capacit
	749.75 0
	132.00 G
	132.00 G
	131.75 0
	99.75 0
	99.75 0
Help	ОК

Figure 7. VMware HA Cluster Status Screen

Under this screen, you will notice three tabs. There is one tab each for Hosts, VMs, and Heartbeat Datastores. On the Hosts tab, you will see the system that is acting as the Master node. You will also see the number of hosts that are currently connected to this Master. The number shown should equal the number of hosts that are contained within you cluster, minus one for the Master.

🖉 vSpl	nere HA	Cluster Status F	or DemoClus	ster-01		×
Hosts	VMs	Heartbeat Data	stores			
	rotection	n Summary —				[
0	Protecte	ed:		7		
•	Unprote	cted:		0		
He	elp				OK	

Figure 8. Summary of Virtual Machine Protection States

Under the **VMs** tab, a summary of the virtual machine protection states is displayed. The virtual machines that were powered on when VMware HA was enabled are in the **Protected** state.

🖉 vSp	here HA Cluster Status Fo	r DemoCluster-01		×
Hosts	VMs Heartbeat Datas	tores		
Datas	tores Used for Heartbeating	ļ		
Nam	e	Datastore Cluster	Hosts	
	tm-pod01-sas300-sp	Datastore Cluster	3	
	tm-pod01-sas600-sp-02	Datastore Cluster	3	
۲ 📄				•
Hosts	Using Selected Datastores f	for Heartbeating		
Nam	e			
	tm-pod01-esx02.tmsb.loc	al		
	tm-pod01-esx03.tmsb.loc	al		
	tm-pod01-esx01.tmsb.loc	al		
Н	elp		ОК	

Figure 9. Heartbeat Datastores Information

Clicking the Heartbeat Datastores tab will display information about the datastores that were selected as heartbeat datastores. Heartbeat datastores allow a secondary means of communication between the hosts in case of a loss of the management network. By selecting a particular datastore, you will display a list of all the hosts that are using the selected datastore as a heartbeat datastore.

Click **OK** to exit the cluster status screen.

Ø tm-pod01-vc01 - vSphere Client File Edit View Inventory Administration Plug-ins Help Image: Sphere Plug Inventory P Image: Plug Hosts and Clusters

	-	🛕 Home 👂 🛃 Inv	rentory 🕨 🛐 Hosts and Clusters					
ī,	6	8 H						
	tm-pod	01-vc01 noDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm tm-pod01-esx02.tm	DemoCluster-01 Getting Started Summary Virtual N	Machines Hosts Res	ource Allocation Perform	mance	2 Tasks & Events Alarms F	⁹ ermissi
	i	tm-pod01-esx03.tm	Name	State	vSphere HA Protection	Ch-	Stur. Hort	-
	đ	VM_01	™_02	Powered On	Protected	~	Name	sx01.t
	ģ	VM_02	M_05	Powered On	Protected	~	State	_sx03.t
	9	VM_03	M_06	Powered On	Protected	~	vSphere HA Protection	sx03.t
	9	VM_04	M_07	Powered On	Protected	~	Status	sx03.t
		VM 06	M_03	Powered On	Protected	~	Host	sx02.t
	2	NM_07	➡ VM_01	Powered On	Protected	~	Provisioned Space	sx02.t
		-	VM_04	Powered On	Protected	~	Used Space	sx02.t
						~	Host CPU - MHz	
						~	Host Mem - MB	
						~	Guest Mem - %	
							Guest OS	

Figure 10. Viewing the Current VMware HA Protection State

Another method you can use to see the protection state of the virtual machines would be to select the **Virtual Machines** tab for a cluster. Right-clicking the title bar enables you to select the **vSphere HA Protection** field. Once the field is selected, you will see a column that displays the current VMware HA protection state for every virtual machine within the cluster.

🕗 tm-pod01-vc01 - vSphere Client		
File Edit View Inventory Adminis	tration Plug-ins Help	
🖸 🔝 🏠 Home 🕨 🚮 Inve	ntory 🕨 🛐 Hosts and C	Clusters
II > S 20 m	🚯 😫 🕪 🧇	B /2
tm-pod01-vc01 DemoDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm tm-pod01-esx02.tm	VM_01 Getting Started Summa	Resource Allocation Performance
 tm-pod01-esx03.tm VM_01 VM_02 VM_03 VM_04 VM_05 VM_06 VM_07 	Guest OS: VM Version: CPU: Memory: Memory Overhead: VMware Tools: IP Addresses:	Microsoft Windows Server 2008 R2 (64 7 2 vCPU 4096 MB 56.85 MB OK 10.91.35.63 View all
	DNS Name: EVC Mode: State: Host: Active Tasks: vSphere HA Protection:	w2k8r2-tmpl N/A Powered On tm-pod01-esx02.tmsb.local

Figure 11. HA Protection State for an Individual Virtual Machine

You can also identify the HA protection state for an individual virtual machine by selecting the virtual machine on the navigation tree and then clicking the Summary tab.

Virtual Machine Protection State

Host Protection State

🕗 tm-pod01-vc01 - vSphere Client		
File Edit View Inventory Adminis	tration Plug-ins Help	
💽 💽 🏠 Home 🕨 🚮 Inve	ntory 👂 🗊 Hosts and Clusters	
et et net		
tm-pod01-vc01 DemoDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm	tm-pod01-esx01.tmsb.local VMw Getting Started Summary Virtu	vare ESXi, 5.0.0, 413596 al Machines Performance Conf
tm-pod01-esx02.tm	General	
tm-pod01-esx03.tm	Manufacturer:	Cisco Systems Inc
₩_02	Model:	N20-B6625-1
🝈 VМ_03	CPU Cores:	8 CPUs x 2.393 GHz
₩_04 ₩ VM_05	Processor Type:	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
M_06	License:	VMware vSphere 5 Enterprise Plus - Licensed for 2 physic
vii0/	Processor Sockets:	2
	Cores per Socket:	4
	Logical Processors:	16
	Hyperthreading:	Active
	Number of NICs:	4
	State:	Connected
	Virtual Machines and Templates:	1
	vMotion Enabled:	Yes
	VMware EVC Mode:	Disabled 🖓
	vSphere HA State	🕏 Running (Master) 🛛 🖓
	Host Configured for FT:	Yes
	Active Tasks:	
	Host Profile:	
	Image Profile:	N/A
	Profile Compliance:	🛜 N/A
	DirectPath I/O Gen. 2:	Supported 📮

Figure 12. Viewing the VMware HA State for the Host

The VMware HA state can be identified for an individual host by selecting the desired host from the navigation tree and selecting the Summary tab. Here you will see the VMware HA state for the host as well as the role that this node plays within the cluster. In the preceding example, the host is the master node for the cluster.

🕗 tm-pod01-vc01 - vSphere Client	tm-pod01-vc01 - vSphere Client				
File Edit View Inventory Admin	stration Plug-ins Help				
🖸 🔝 🏠 Home 🕨 🛃 Inv	entory 👂 🗊 Hosts and Clusters				
e e e					
	DemoCluster-01 Getting Started Summary Virt	ual Machines Hosts	Resource Allocation Pe	rformance Tasks & Events Alarms Per	
₩_01 ₩ VM_02 ₩ VM_03 ₩ VM_04 ₩ VM_05 ₩ VM_06 ₩ VM_07	 tm-pod01-esx02.tmsbJocal tm-pod01-esx03.tmsbJocal tm-pod01-esx01.tmsbJocal 	Connected @ Connected @ Connected @	O Connected (Slave) Connected (Slave) Running (Master)	 Name State vSphere HA State Status % CPU % Memory Memory Size 	

Figure 13. Displaying the HA State for All Hosts Within a Cluster

To display the VMware HA state for all of the hosts within a cluster, select the cluster from the navigation tree and then click the Hosts tab. Right-click the title bar and ensure that the vSphere HA State column is enabled.

VMware HA Advanced Options

VMware HA provides a user with the ability to change various options based on their individual needs. This section provides an overview of the most commonly used options.

🖉 t	m-poo	d01-v	c01 - vSph	ere Client							
File	Edit	Viev	w Invento	ory Adminis	tration Plug-ins Help						
F	₽		🔥 Home	▶ 📲 Inve	ntory 🕨 🕅 Hosts and Clusters						
	6										
	🛛 tm-	pod0	1-vc01		DemoCluster-01						
'	= <u> </u> =	Dem	oDatacente)emoCluste	r-01 r-01	Getting Started Summary Virtu	al Machines Hosts Resource A	Allocation	Performance Tasks 8	& Eve	nts Alar	ms Peri
			tm-pod0	1-esx01.tm	General		vSp	phere HA			
			tm-pod0	1-esx03.tm	vSphere DRS:	Off	Ad	mission Control:		Er	abled
		<u> </u>			vSphere HA:	On	Cu	rrent Failover Capacity:		2	nosts
			VM 03		VMware EVC Mode:	Disabled	Co	onfigured Failover Capacit	y:	1	nost
		-	VM_04		Tatal CBL Bessurges	57 CH-	Ho	st Monitoring:		En	abled
		-	VM_05		Total Memory:	143.80 GB	VM	1 Monitoring:		Er	abled
			VM_06		Total Storage:	1.41 TB	Ap	plication Monitoring:		Di	sabled
			VM_07				Ad	vanced Runtime Info			
					Number of Hosts:	3	Clu	uster Status			
L					Total Processors:	24	Co	onfiguration Issues			
					Number of Datastore Clusters:	1	Sto	orage			
					Total Datastores:	7	St	orage resources 🛛 🖂	Stat	us	Drive
					Virtual Machines and Templates:	7	6	TM-Gobal-Interch	۲	Normal	Non-
					Total Migrations using vMotion:	13	6	TM-POD01-E5X01	۲	Normal	Non-
							6	TM-POD01-E5X02	۲	Normal	Non-
								TM-POD01-E5X03	۲	Normal	Non-
					Commands		6	tm-pod01-sas300	0	Normal	Non-
						0.0		tm-pod01-sas600	۲	Normal	Non-
					New Virtual Machine	Provide the Wew Datastore Cluster	1	tm-pod01-sas600	۲	Normal	Non-
					Add Host	🐴 Edit Settings	•				

Figure 14. Editing Settings

Click Edit Settings.

🕗 DemoCluster-01 Settings	
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	Name DemoCluster-01 Features ✓ Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a cluster. Core functionality includes host and virtual machine monitoring to minimize downtime when heartbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance.
	 Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, groups, and virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies. vSphere DRS and VMware EVC should be enabled in the cluster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing.
Help	OK Cancel

Figure 15. Cluster Settings Wizard

This brings up the wizard that allows you to edit the cluster settings. Once VMware HA is enabled, additional settings are displayed allowing for the configuration of VMware HA.

Admission Control

DemoCluster-01 Settings	
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	Host Monitoring Status ESX hosts in this cluster exchange network heartbeats. Disable this feature when performing network maintenance that may cause isolation responses. IV Enable Host Monitoring
	Admission Control The vSphere HA Admission control policy determines the amount of cluster capacity that is reserved for VM failovers. Reserving more failover capacity allows more failures to be tolerated but reduces the number of VMs that can be run. © Enable: Disallow VM power on operations that violate availability constraints © Disable: Allow VM power on operations that violate availability constraints
	Admission Control Policy
	C Percentage of duster resources reserved as failover spare capacity: 25 % CPU
	C Specify failover hosts: 0 hosts specified. Click to edit.
	Advanced Options
Help	OK Cance

Figure 16. Host Monitoring Status and Admission Control Attributes

In the cluster settings dialog box, select vSphere HA from the navigation tree on the left. This allows you to edit the Host Monitoring Status and Admission Control attributes.

Host monitoring enables VMware HA to take action if a host fails to send heartbeats over the management network. During maintenance operations on the management network, it is possible that the hosts will not be able to send heartbeats. When this occurs, you should unselect this option to prevent VMware HA from believing the hosts are isolated.

Admission control is used to ensure that adequate resources within the cluster are available to facilitate failover if needed. It also serves to ensure that the virtual machine reservations are respected. Three options are available to specify the desired admission control policy. These include the following:

Host failures

This option attempts to reserve enough capacity within the cluster to provide for the failure of any host within the cluster.

Percentage

As with the host failures option, this also attempts to reserve enough capacity within the cluster. However, this option allows you to specify a percentage of CPU and memory that you want reserved.

• Failover hosts

Alternately, you can specify particular hosts within the cluster that will be used as a preferred target host to start any virtual machines that were protected on a failed host. In the event of a failure, vSphere HA will first attempt to restart the protected VMs on these hosts before trying others. Additionally, vSphere HA prevents VMs from being moved to these hosts, or powered on by the user or vSphere Distributed Resource Scheduler (DRS) on these hosts.

Virtual Machine Options

🕗 DemoCluster-01 Settings				×
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	Set options that define the l Cluster Default Settings – VM restart priority: Host Isolation response: Virtual Machine Settings – Cluster settings can be over	behavior of virtual mac Medium Disabled Low Medium High erriden for specific virtu	hines for vSphere HA.	
	Virtual Machine Image: VM_02 VM_05 VM_06 VM_07 VM_03 VM_01 VM_04	VM Restart Priority Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting	Host Isolation Response Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting	
Help			ОК	Cancel

Figure 17. Defining the Behavior of Virtual Machines for VMware HA

Select Virtual Machine Options from the left-hand navigation pane. Here, you can define the behavior of virtual machines for VMware HA. The two settings you can edit are the VM restart priority and the Host Isolation response.

The VM restart priority enables you to specify the order that virtual machines will be started in the event of a failure. In cases where there might not be enough resources available within the cluster to accommodate the restart of a series of virtual machines, this setting allows a level of prioritization, allowing the most important virtual machines to be restarted first. Notice that this can be set on a per-virtual machine basis as well.

🕑 DemoCluster-01 Settings				×
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	Set options that define the -Cluster Default Settings VM restart priority: Host Isolation response -Virtual Machine Settings Cluster settings can be ov	Medium Medium Leave pow Power off Shut dowr verriden for specific virtu	hines for vSphere HA.	
	Virtual Machine Image: VM_02 VM_05 VM_06 VM_07 VM_03 VM_01 VM_04	VM Restart Priority Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting	Host Isolation Respons Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting Use cluster setting	e
Help			OF	Cancel

Figure 18. Host Isolation Response

Host Isolation Response specifies the behavior that HA will take in the event that a host is determined to be isolated. Host isolation occurs when a host loses the ability to communicate through the management network to the other hosts within the environment and is unable to ping its configured isolation addresses—this is the default gateway. In this event, the host is still functioning, although it is not able to communicate. The default setting for this is **Leave powered on**.

DemoCluster-01 Settings Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	VM Monitoring Status VM Monitoring restarts individ within a set time. Application application heartbeats are no VM Monitoring: VM Monito Disabled Default Cluster Se VM Monito VM and Ap Monitoring sensitivity: Lo vSphere HA will restar VM has not been recei the VM after each of t	ual VMs if their VMware tools hee Monitoring restarts individual VM t received within a set time. ring Only plication Monitoring pw High t the VM if the heartbeat betwee ved within a 30 second interval. he first 3 failures every hour.	artbeats are not received is if their VMware tools
	Virtual Machine Settings		
	Virtual Machine	VM Monitoring	Application Monitoring
	🔂 VM_02	Use cluster settings	N/A
	🔂 VM_05	Use cluster settings	N/A
	M_06	Use cluster settings	N/A
	M_07	Use cluster settings	N/A
	🔂 VM_03	Use cluster settings	N/A
	M_01	Use cluster settings	N/A
	M_04	Use cluster settings	N/A
Help		-	OK Cancel

Virtual Machine Monitoring

Figure 19. Virtual Machine Monitoring

Selecting VM Monitoring from the left-hand navigation pane enables you to change settings related to the monitoring of the OS or application running within a virtual machine. In order to use this feature, you must have VMware Tools installed within the virtual machine.

Period DemoCluster-01 Settings			×	
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	VM Monitoring Status VM Monitoring restarts individual VMs if their VMware tools heartbeats are not received within a set time. Application Monitoring restarts individual VMs if their VMware tools application heartbeats are not received within a set time. VM Monitoring: VM Monitoring Only VM Monitoring sensitivity: Low Image: Pailure interval: 30 Image: Pailure interval: 1 Image: Pailure interval: 1 Image: Pailure interval: 3 Image: Pailure interval: 3 <t< td=""></t<>			
	Virtual Machine Settings			
	Virtual Machine	VM Monitoring	Application Monitoring	
	M_02	Use cluster settings	N/A	
	M_05	Use cluster settings	N/A	
	∰ VM_06	Use cluster settings	N/A	
	I I M _07	Use cluster settings	N/A	
	₩ VM_03	Use cluster settings	N/A	
	₩ VM_01	Use cluster settings	N/A	
		Use cluster settings	N/A	
Help			OK Cancel	

Figure 20. Selecting Custom Option for VM Monitoring

By selecting the Custom option, you can exert a fine level of control over the various parameters involved. You can specify these settings on a per-virtual machine basis.

Cluster Features	
vSphere HA	vSphere HA uses datastores to monitor hosts and VMs when the management network he failed, vCenter Server selects 2 datastores for each host using the policy and datastore
Virtual Machine Options	preferences specified below. The datastores selected by vCenter Server are reported in th
VM Monitoring	<u>Cluster Status dialog</u> .
Datastore Heartbeating	C. Select only from my professed detectors
VMware EVC	Select only from my preferred datastores
Swapfile Location	 Select any of the cluster datastores
	$\ensuremath{\mathbb{C}}$ Select any of the cluster datastores taking into account my preferences
	Datastores available for Heartbeat. Select those that you prefer
	Name Pod Hosts Mounting Datastore
	TM-Gobal-Inte 3
	🔲 🗊 tm-pod01-sas Datasto 3
	🔲 🗊 tm-pod01-sas Datasto 3
	🔲 🗊 tm-pod01-sas Datasto 3
	Hosts Mounting Selected Datastores
	Name

Figure 21. Datastore Heartbeating Window

Storage heartbeats provide a secondary communication path in the event of a failure of the management network. This is advantageous, because it provides another level of redundancy and allows for the determination of failure between a network and a host failure. By default, two datastores will be chosen based on the connectivity they have to other hosts and the type of storage. This attempts to provide protection against array failures and allows for the highest number of hosts to utilize the heartbeat datastore. The datastores utilized can be manually specified if desired.

Validating VMware HA Operation

In order to see VMware HA in action, we need to inject faults into the environment. This section will demonstrate the ways in which to do this for the most common failure cases, so that you can validate the operation of VMware HA and can test ways to recover from a failure.

Host Failure

The most common failure case involves the failure of a physical host. This can be for a variety of reasons, such as a loss of power to the host or a motherboard failure.

When this event occurs, VMware HA will identify the failure of the host and will attempt to restart the protected virtual machines on a functional host.

💋 tm-pod01-vc01 - vSphere C	lient						
File Edit View Inventory	dministration Plug-ins	Help					
🖸 🔝 🏠 Home 🕨 🛓	🛐 Inventory 🕨 🛐 Hos	sts and Clusters					
I 🗗 🧉 🔠							
tm-pod01-vc01	01.tm 02.tm	L Summary Virtual	Machines Hosts DRS Re	esource Allocation \ Pe	erformance Tasks & Events A	larms Permissions	Maps Profile
tm-pod01-es>	03.tm Name	State	vSphere HA Protection	Status	Host	Provisioned Space	Used Space
WH_01 WH_02 WH_03 WH_04 WH_04 WH_05 WH_05 WH_06	 VM_01 VM_02 VM_05 VM_06 VM_03 VM_04 	Powered On Powered On Powered On Powered On Powered On Powered On	 Protected Protected Protected Protected Protected Protected Protected Protected 	 Normal Normal Normal Normal Normal Normal Normal 	tm-pod01-esx01.tmsblocal tm-pod01-esx01.tmsblocal tm-pod01-esx03.tmsblocal tm-pod01-esx03.tmsblocal tm-pod01-esx02.tmsblocal tm-pod01-esx02.tmsblocal	36.05 GB 36.05 GB 17.05 GB 17.05 GB 36.05 GB 17.05 GB	36.05 GB 36.05 GB 3.03 GB 3.02 GB 36.05 GB 3.03 GB

Figure 22. Checking Virtual Machines

First, use the vSphere Client to examine the virtual machines hosted within the cluster. In this example, we are going to cause the system tm-pod1-esx01.tmsb.local to fail. You need to check the virtual machines in your environment and ensure that at least one is online on the host that you are going to fail.

🖉 ti	m-po	od01-\	/c01	L - vSphere Client									
File	Edit	it Vie	w	Inventory Admini	istra	atio	n Plug-ins Help						
	-			Home 🕨 🚮 Inv	ent	tory	Hosts and Cl	usters					
_∎*	6	† (3	86									
	? tr = <u> </u>	n-pod Dem)1-v IoDa Den	c01 atacenter-01 noCluster-01 <i>tm-pod01-esx01.tm</i> tm-pod01-esx02.tm	D	Getti	oCluster-01 ing Started Summar	ry Virtual Machin	ies H	osts DRS	Resource Allocation Performance	e Tasks & Ev	ents Alar
				tm-pod01-esx03.tm	N	Vame	<u>م</u>	State	Stat	us	% CPU	% Memory	Last Time
		ć		VM_01 VM_02			tm-pod01-esx01.t… tm-pod01-esx02.t…	Not responding Connected	•	Alert < Normal	0	9 6	Never Never
				VM_03 VM_04 VM_05 VM_06			tm-pod01-esx03.t	Connected	0	Normal	0	4	Never

Figure 23. Removing Power from a Host

Next, remove the power from one of your hosts. By looking at the hosts within the cluster, you will see that VMware HA will detect the failure of the host and generate an alert.

🕗 tm-pod01-vc01 - vSphere Client				
File Edit View Inventory Administ	tration Plug-ins Help			
💽 💽 🏠 Home 🕨 🚮 Inver	ntory 🗅 🛐 Hosts and Clusters			
d e ut				
E C tm-pod01-vc01	tm-pod01-esx01.tmsb.local VMware ESXi, 5.0.0, 413596			
DemoDatacenter-01	Getting Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permiss	sions Maps Stor		
tm-pod01-esx01.tm	View: Tasks Events			
tm-pod01-esx02.tm				
Tm-podul-esx03.tm	Show all entries 👻			
WM 02	Description	Туре		
🔂 VM_03	Alarm 'vSphere HA host status' on tm-pod01-esx01.tmsb.local changed from Green to Red	👔 info		
👘 VM_04	The vSphere HA availability state of this host has changed to Host Failed	🗊 info		
👘 VM_05	vSphere HA detected a possible host failure of this host	error		
Image: Image	Alarm 'Host connection failure': an SNMP trap for entity tm-pod01-esx01.tmsb.local was sent	👔 info		
	Alarm 'Host connection failure' on tm-pod01-esx01.tmsb.local triggered an action	👔 info		
	Alarm 'Host connection failure' on tm-pod01-esx01.tmsb.local changed from Gray to Gray	🕦 info		
	Alarm 'Host service console swap rates' on tm-pod01-esx01.tmsb.local changed from Green to Gray	🕦 info		
	Alarm 'Host memory usage' on tm-pod01-esx01.tmsb.local changed from Green to Gray	🕦 info		
	Alarm 'Host cpu usage' on tm-pod01-esx01.tmsb.local changed from Green to Gray	👔 info		
	Alarm 'Host connection and power state' on tm-pod01-esx01.tmsb.local changed from Green to Red	👔 info		
I	Up Changed resource allocation for VM_U1	🚹 info		
	VM_01 is disconnected	🚯 info		
	🖏 Host is not responding	🔶 error		
	Of Changed resource allocation for VM_02	🚹 info		
	A ticket for VM_01 of type mks has been acquired	📵 info		

Figure 24. Failure Detection by VMware HA

By examining the events, you will see messages similar to the ones demonstrated in the preceding figure validating that VMware HA has detected the failure.

💋 tm-pod01-vc01 - vSphere Client						
File Edit View Inventory Admin	istration Plug-ins	Help				
🖬 🔝 🔥 Home 🕨 🛃 Inv	ventory 🕨 🛅 Hosts	s and Clusters				
🖬 🖻 😂 👫						
	DemoCluster-01 Getting Started	Summary Virtual Mac	hines Hosts DRS Re	source Allocation Per	formance Tasks & Events A	larms Permissic
tm-pod01-esx03.tm	Name 🗠	State	vSphere HA Protection	Status	Host	Provisioned Sp
W_01	WM_01	Powered On	Protected	Normal	tm-pod01-esx02.tmsb.local	36.05 GB
VM_02	VM_02	Powered On	Protected	Normal	tm-pod01-esx03.tmsb.local	36.05 GB
WM_03	M_03	Powered On	Protected	🤣 Normal	tm-pod01-esx02.tmsb.local	36.05 GB
VM 05	M_04	Powered On	Protected	🦁 Normal	tm-pod01-esx02.tmsb.local	17.05 GB
₩_06	VM_05	Powered On	Protected	🦁 Normal	tm-pod01-esx03.tmsb.local	17.05 GB
	™_06	Powered On	Protected	📀 Normal	tm-pod01-esx03.tmsb.local	17.05 GB

Figure 25. Virtual Machine View of a Cluster After Restart Attempt

After a failure of a host has been detected, HA will attempt to restart the virtual machines that were running on the failed host on other available hosts within the cluster. Go back to the virtual machine view of your cluster and notice that the virtual machines that were previously on the failed host are now online on other hosts.

🕑 tm-pod01-vc01 - vSphere Client	29 tm-pod01-vc01 - vSphere Client						
File Edit View Inventory Adminis	File Edit View Inventory Administration Plug-ins Help						
💽 💽 🏠 Home 🕨 🚮 Inve	entory 🗅 🛅 Hosts and Clusters						
s e :::							
E 🛃 tm-pod01-vc01	tm-pod01-esx02.tmsb.local VMware ESXi, 5.0.0, 413596						
DemoDatacenter-01	Getting Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permi	ssions	Maps Stor				
tm-pod01-esx01.tm	View: Tasks Events		·				
tm-pod01-esx02.tm							
tm-pod01-esx03.tm	Show all entries 👻						
VM_02	Description	Type	•				
➡ VM_03	🍏 The vSphere HA agent on this host cannot reach some of the management network addresses of other hosts,	0	info				
👘 VM_04	and HAmay not be able to restart VMs if a host failure occurs: tm-pod01-esx01.tmsb.local:10.91.33.1						
™_05	🍏 Alarm Virtual machine memory usage' on VM_01 changed from Gray to Green	•	info				
₩_06	🍏 🛛 Alarm 'Virtual machine cpu usage' on VM_01 changed from Gray to Green	0	info				
	Of Changed resource allocation for VM_01	0	info				
	👹 Changed resource allocation for VM_01	0	info				
	🖑 Virtual machine VM 01 is connected	0	info				
	vSphere HA restarted virtual machine VM_01		warning				
	Warning message on VM_01: Insufficient video RAM. The maximum resolution of the virtual machine will be		warning				
	limited to 1672x1254. To use the configured maximum resolution of 2560x1600, increase the amount of video						
	RAM allocated to this virtual machine by setting svga.vramSize="16384000" in the virtual machine's						
	configuration file.						
	Virtual machine VM_04 is vSphere HA Protected and HA will attempt to restart it after a failure.	0	info				
	Virtual machine VM_03 is vSphere HA Protected and HA will attempt to restart it after a failure.	0	info				
	🥶 vSphere HA agent on this host is enabled	0	info				

Figure 26. Viewing Log Messages After Restart Attempt

You can also examine the events for a host to see the log messages denoting that VMware HA has attempted to restart the virtual machine.

🔗 tm-pod01-vc01 - vSphere Client						
File Edit View Inventory Admini	stration Plug-ins Help					
🖸 🔝 🏠 Home 🕨 🚮 Inventory 🕨 🗊 Hosts and Clusters						
e e 58						
tm-pod01-vc01 DemoDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm. tm-pod01-esx02.tm tm-pod01-esx03.tm VM_01 VM_01 VM_01	tm-pod01-esx01.tmsb.local VMv Getting Started Summary Virtu Configuration Issues vSphere HA detected a possible he	vare ESXi, 5.0.0, 413596 Ial Machines Performance Con ost failure of this host				
WM_02	General					
₩ VM_04 ₩ VM_05 ₩ VM_06	Manufacturer: Model:	Cisco Systems Inc N20-B6625-1				
	Processor Type:	8 CPUs x 2,393 GHz Intel(R) Xeon(R) CPU E5620 @ 2,40GHz				
	License:	VMware vSphere 5 Enterprise Plus - Licensed for 2 physic				
	Processor Sockets:	2				
	Cores per Socket:	4				
	Logical Processors:	16				
	Hyperthreading:	Active				
	Number of NICs:	4				
	State:	Not responding				
	Virtual Machines and Templates:	U Vec				
	VMotion Enabled:	N/A (not responding)				
	This ceremote.	N/A (not responding)				
	vSphere HA State	🚯 Host Failed 🛛 🖓				
	Host Configured for F1:	Yes				
	Active Tasks:					
	Host Profile:					
< <u> </u>	Image Profile:	N/A				

Figure 27. Summary of a Failed Host

By selecting the Summary tab for the failed host, you will notice that the issue is displayed in multiple places. The first is located at the top of the screen and second location is the vSphere HA State.

At this point, you will reapply power to the failed host and allow it to boot. Once it completes this process, you will see that it rejoins the cluster and continues to function as before.

Host Isolation

Host isolation occurs when a host loses the ability to communicate to other hosts within the cluster through the management network, and also loses the ability to ping the default isolation address. The following will demonstrate how to create this situation and induce the default actions that will be taken by VMware HA.



Figure 28. Identifying a Host to Be Isolated

First, you want to identify a host that will be isolated. For this example, host tm-pod01-esx03.tmsb.local has been chosen. You can verify that it is currently acting as a slave within the cluster.

💋 tm-pod01-vc01 - vSphere Client								
File Edit View Inventory Administration Plug-ins Help								
F	Home D 🛃 Inventory D 🛐 Hosts and Clusters							
	51 6	88						
		1-vc01 oDatacenter-01 pemoCluster-01 tm-pod01-esx01.tm tm-pod01-esx02.tm	DemoCluster-01 Getting Started Summary Vir	tual Machines Hosts	DRS Resource Allocatio	on Performance Tasks & Events		
		tm-pod01-esx03.tm 4 VM_01 4 VM_02 4 VM_03 4 VM_04 4 VM_05 4 VM_06 4 VM_07	Name Image: VM_01 Image: VM_02 Image: VM_03 Image: VM_04 Image: VM_05 Image: VM_06 Image: VM_07	State Powered On Powered On	Status Normal Normal Normal Normal Normal Normal Normal	Host tm-pod01-esx02.tmsblocal tm-pod01-esx02.tmsblocal tm-pod01-esx02.tmsblocal tm-pod01-esx02.tmsblocal tm-pod01-esx03.tmsblocal tm-pod01-esx03.tmsblocal tm-pod01-esx03.tmsblocal		

Figure 29. Identifying Virtual Machines on tm-pod01-esx03.tmsb.local

Now identify the virtual machines that are currently online on this host. These are the virtual machines that will be affected by the isolation response performed after the fault is inserted.



Figure 30. Obtaining Console Access to the Target Host

To insert a fault within the environment, you need to obtain console access to the target host. This will allow you to continue to access the host after the fault has been inserted, allowing you to recover gracefully afterwards. It is important to note that this procedure requires two networks – one for console access and another for those affected by the test. Refer to the "System Requirements" section for more information on the network configuration used.



Figure 31. Authenticating to the Host

At the console, hit F2 to access the console menu. You will need to authenticate to the host first before it will allow access to the console menu.

TM-POD01-ESX03 (Chassis 3 Server 8) File View Macros Tools Help Boot Server & Shutdown Server Reset						
KVM Console Properties						
l	System Customization	Troubleshooting Options				
	Configure Password Configure Lockdown Mode Configure Management Network Restart Management Network Test Management Network Restore Network Settings Restore Standard Switch	To view various troubleshooting mode options like Enable ESXi Shell, Enable SSH and Restart Agents.				
	Configure Keyboard Troubleshooting Options					
	View System Logs View Support Information					
	Reset System Configuration					

Figure 32. Selecting Troubleshooting Options

Once you're logged in, select the **Troubleshooting Options** menu item.
TM-POD01-ESX03 (Chassis 3 Server 8)	
ad Boot Server ↓ Shutdown Server ♀ Reset	
KVM Console Properties	
Troubleshooting Mode Options	ESXi Shell
Disable ESXI Shell Enable SSH Modify ESXi Shell tineout Restart Management Agents	ESXi Shell is Enabled Change current state of the ESXi Shell

Figure 33. Enabling ESXi Shell

From here, select the **Enable ESXi Shell** option to enable the ESXi Shell. This shell will enable you to remove the network connections to the host.

🕗 tm-pod01-vc01 - vSphere Client										
File Edit View Inventory Administration Plug-ins Help										
The second secon										
5 © 38										
	tm-pod01-esx03.tmsb.local VMwa Getting Started Summary Configuration Issues ESXi Shell for the host has been ena General Manufacturer: Model:	Interent ESXI, 5.0.0, 413596 Machines Performance Configue bled Cisco Systems Inc N20-B6625-1								

Figure 34. vSphere Client Warning Message

Once you do this, you will notice that the vSphere Client displays a warning message.



Figure 35. Accessing the ESXi Shell

At the ESXi console for the host, hit Alt-F1 to access the ESXi Shell. Log in to the shell using the user name and password specified for the host.

A TM-POD01-ESX03 (Chassis 3 Server 8)	
File View Macros Tools Help	
📣 Boot Server 🔩 Shutdown Server 🤐 Reset	
KVM Console Properties	
ESXi 5.0.0 http://www.vnware.con Copyright (c) 2007-2011 VMware, Inc.	<u>^</u>
tm-pod01-esx03.tmsb.local login: root Password: The time and date of this login have been sont to the surtem logs	
VMware offers supported, powerful system administration tools. Ple see ими.vmware.com/go/sysadmintools for details.	ase
The ESXi Shell can be disabled by an administrative user. See the <u>vSobece Security documentation for more information</u> .	
r # esxcfg-vswitch -1 Switch Rame Rum Ports Used Ports Configured Ports MTU vSwitch0 128 11 128 1500	Արlinks vanic0,vanic1
PortGroup Name VLAN ID Used Ports Uplinks Production82 3801 3 vmnic8.vmnic1	
Management Network 2912 1 vmnic0,vmnic1	
vMotion01 3002 1 vmnic0,vmnic1 ET01 3003 1 vmnic0,vmnic1	
iSCSI01 3004 1 vmric0,vmric1	
HBR01 3005 1 vmnic0,vmnic1	
r # esxcfg-vswitch -U vnnic1 vSwitch0 r # esxcfg-vswitch -U vnnic0 vSwitch0 # esxcfg-vswitch -U vnnic0 vSwitch0	
Suffice values of the second s	Up1 inks
PortGroup Name VLAN ID Used Ports Uplinks	
Management Network 2912 1	
vMotion01 3002 1	
FT01 3003 1	
HBR01 3005 1	
·· + _	
	-
•	•

Figure 36. Using the esxcfg-vswitch Command

In order to disrupt the network connection to the host, you can use the esxcfg-vswitch command. Using esxcfg-vswitch –I, obtain a list of the uplinks that are present on the host. In this example, there are two – vmnicO and vmnic1 – that can be identified on vSwitchO.

Use the command esxcfg-vswitch –U <uplink> <switch>, where uplink is an identified uplink and switch is the name of the switch the uplink is connected to, in order to remove the uplinks from the virtual switch. Ensure that you do this for all of the uplinks previously identified. Once completed, verify that all of the uplinks have been removed by using the esxcfg-vswitch –I command again.

💋 tr	🕜 tm-pod01-vc01 - vSphere Client							
File	Edit View	Inventory Admini	stration Plug-ins Help					
	E	Home 🕨 🚮 Inve	entory 👂 🗊 Hosts and Clusters					
	et art							
	 tm-pod01-vc01 DemoDatacenter-01 DemoCluster-01 tm-pod01-esx03.tmsb.local VMware ESXi, 5.0.0, 413596 Getting Started Summary Virtual Machines Performance Configura tm-pod01-esx03.tm tm-pod0							
		/M_03	General		Reso			
		(M_04 (M_05 (M_06 (M_07	Manufacturer: Model: CPU Cores: Processor Type: License: Processor Sockets: Cores per Sockets: Logical Processors: Hyperthreading: Number of NICs: State: Virtual Machines and Templates: vMotion Enabled: VMware EVC Mode:	Cisco Systems Inc N20-B6625-1 8 CPUs x 2.393 GHz Intel(R) Xeon(R) CPU E5620 @ 2.40GHz VMware vSphere 5 Enterprise Plus - Licensed for 2 physic 2 4 16 Active 4 Connected 3 Yes Disabled C	CPU Mem Stor			
			vSphere HA State	🔶 Network Isolated 🛛 🖵	Fault			
			Active Tasks:		Fault			

Figure 37. Identifying Host Isolation

Using the vSphere Client, select the host from the left-hand navigation pane and select the Summary tab. The host will be identified as being isolated both at the top of the screen and in the vSphere HA State notification.

2	🥬 tm-pod01-vc01 - vSphere Client									
File	Edit	View	Inventory	Admini	istration	Plug-ins Help				
-	🖸 🛃 home 🕨 🚓 Inventory 👂 👘 Hosts and Clusters									
đ	6		•							
	🗗 🚛	-pod01	-vc01		tm-p	od01-esx03.tmsb.local VMware ESXi, 5.0.0, 413596				
		Demo Ella Dr	Datacenter-0	1	Getti	ng Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permis	sions	Maps Stor		
			tm-pod01-	esx01.tm	View:	Tasks Events				
		2	tm-pod01-	esx02.tm	<u> </u>					
			tm-pod01-	esx03.tm	Show	v all entries 🔻				
			VM 02		Desc	ription	Туре			
		- 6	VM_03		07	Alarm 'Host service console swap rates' on tm-pod01-esx03.tmsb.local changed from Green to Gray	0	info		
		- 6	VM_04		0	Alarm 'Host memory usage' on tm-pod01-esx03.tmsb.local changed from Green to Gray	0	info		
		- <u>a</u>	VM_05 (dis	sconnecti	i	Alarm 'Host cpu usage' on tm-pod01-esx03.tmsb.local changed from Green to Gray	0	info		
			VM_06 (dis	sconnecti	i	Alarm 'Host connection and power state' on tm-pod01-esx03.tmsb.local changed from Green to Red	0	info		
			VM_U7 (dis	sconnecti	I	VM_07 is disconnected	0	info		
					0	VM_06 is disconnected	0	info		
					9	VM_05 is disconnected	0	info		
					ď	Host is not responding	•	error		
					0	vSphere HA detected that this host is network isolated from the duster	•	error		
					O,	The vSphere HA availability state of this host has changed to Network Isolated	0	info		
					0	Alarm 'vSphere HA host status' on tm-pod01-esx03.tmsb.local changed from Green to Red	0	info		
					0	vSphere HA detected that this host is in a different network partition than the master to which vCenter Server	Δ	warning		
						is connected				
					9	The vSphere HA availability state of this host has changed to Partitioned from Master	0	info		
					9	The vSphere HA availability state of this host has changed to Unreachable	0	info		

Figure 38. Log Messages About Host Isolation

Moving to the Tasks & Events tab, you will also see the log messages that were generated when VMware HA detected the host isolation.

🖉 tn	🕗 tm-pod01-vc01 - vSphere Client										
File	File Edit View Inventory Administration Plug-ins Help										
	-	🖸 🕼 Home 🕨 👸 Inventory 🔹 👹 Hosts and Clusters									
∎*	r 🗗	€ #									
	Der □ 🏦	moDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm tm-pod01-esx02.tm	Getting Started Su	immary Virtual Ma	achines Hosts	DRS Re	source Allocatio	on Performance Tasks & Events			
		tm-pod01-esx03.tm	Name	A 5	State	Statu	JS	Host			
		VM_01 VM_02 VM_03 VM_04 VM_05 (disconnection VM_06 (disconnection VM_06 (disconnection VM_07 (disconnection V	W_01 W_02 W_03 W_05 W_06 W_06 W_07	F F 7 7 7 7	Powered On Powered On Powered On Powered On Powered On Powered On	8 8 8 8 8 8 8 8	Normal Normal Normal Unknown Unknown Unknown	tm-pod01-esx02.tmsblocal tm-pod01-esx01.tmsblocal tm-pod01-esx02.tmsblocal tm-pod01-esx02 tmcblocal tm-pod01-esx03.tmsblocal tm-pod01-esx03.tmsblocal tm-pod01-esx03.tmsblocal			

Figure 39. Observing the Virtual Machines on the Isolated Host

Examine the output of the Virtual Machines tab of the cluster. Observe that the virtual machines on the isolated host are now shown in gray. You'll also observe that the virtual machines did not get restarted on another host. This is due to the fact that the default setting for the isolation response is **Leave Powered On**. With this as the setting for the isolation response, the virtual machines will continue to run on the isolated host. In this scenario, setting the isolation response to **Shutdown** would cause the virtual machines to gracefully shut down, then restart.

File View Macros Tools Help		
Boot Server Shutdown Server Ress	+	
	A	
* # esycfa-uswitch =1		
Switch Name Num Ports vSwitch0 128	Used Ports Configured Ports MTU Uplinks 11 128 1500 vnnic0,vnnic1	
PortGroup Name VLAM Production02 3001 Management Network 2912 vMotion01 3002 FT01 3003 iSCSI01 3004 HBR01 3005 ~ # esxcfg-vswitch -U vmnic1	ID Used Ports Uplinks 3 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 vnnic0,vnnic1 vSwitch0	
<pre>~ # esxcfg-vswitch -U vmnic0 ~ # esycfg-uswitch -1</pre>	vSwitch0	
Switch Name Num Ports vSwitch0 128	Used Ports Configured Ports MTU Uplinks 9 128 1500	
PortGroup Name VLAN Production02 3001 Management Network 2912 vMotion01 3002 F101 3003 iSCS101 3004 HBR01 3005	ID Used Ports Uplinks 3 1 1 1 1 1 1 1	E
/ # esxcfg-vswitch -L vmnic0 / # esxcfg-vswitch -L vmnic1 / # esxcfg-vswitch -l	vSwitch0 vSwitch0	
Switch Name Now Ports vSwitch0 128	used rords Configured Ports MTU Uplinks 11 128 1500 vmnic0,vmnic1	
PortGroup Name VLAN Production02 3001 Management Network 2912 vMotion01 3002 FT01 3003 iSCS101 3004 HBR01 3005	ID Used Ports Uplinks 3 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1 1 vnnic0,vnnic1	

If you would like to see the effects of the various isolation response settings in this situation, simply change the isolation response to the desired setting and perform this test again.

Figure 40. Restoring Uplinks for the Host with the esxcfg-vswitch -I Command

To restore normal operation, utilize the ESXi Shell to execute the esxcfg-vswitch -I command for each of the uplinks that were previously removed. Use the esxcfg-vswitch -I command to verify that the uplinks have been restored.

Log out of the ESXi Shell by typing **exit** at the prompt. Use Alt-F1 to return to the console screen.

🖉 tr	🥬 tm-pod01-vc01 - vSphere Client						
File	Edit	View	/ Inve	entoŋ	y Admini	istration	Plug-ins Help
E	-	1	👌 Но	ome	🕨 🚮 Inv	entory	▶ 🗊 Hosts and Clusters
đ	đ	88	ŀ				
□ 🕹	tm-p	od01	-vc01			tm-po	od01-esx03.tmsb.local VMware E5Xi, 5.0.0, 413596
-		Demo Ba D	emoCli	enter- uster-	01	Getti	ng Started Summary Virtual Machines Performance Configuration Tasks & Events Alarms Permis
		Ĩ	tm-p	od01	-esx01.tm	View:	Tasks Events
		4	tm-p	pod01	-esx02.tm -esx03.tm	Shov	v all entries 👻
			VM_	02		Desc	ription
		Ē	VM_	03		്	Established a connection
			VM_	.04		0	Network connectivity restored on virtual switch "vSwitch0", portgroups: "Production02", "Management
			VM_	05			Network", "vMotion01", "FT01", "ISCSI01", "HBR01", "Management Network". Physical NIC vmnic0 is up.
			VM_	06		0	Alarm 'vSphere HA host status' on tm-pod01-esx03.tmsb.local changed from Red to Green
			\$ VM_	07		0	vSphere HA agentis healthy
						0	The vSphereHA availability state of this host has changed to Slave
						01	Alarm Host connection failure : an Sivier trap for entity tm-podul-esxu3.tmsp.iocal was sent
						0	Alarm 'Host connection failure' on tm-pod01-esx03.tmsb.local triggered an action
						0	Alarm 'Host connection failure' on tm-pod01-esx03.tmsb.local changed from Gray to Gray
						0	Alarm 'Host service console swap rates' on tm-pod01-esx03.tmsb.local changed from Green to Gray
						0	Alarm 'Host memory usage' on tm-pod01-esx03.tmsb.local changed from Green to Gray
						0	Alarm 'Host cpu usage' on tm-pod01-esx03.tmsb.local changed from Green to Gray
						0	Alarm 'Host connection and power state' on tm-pod01-esx03.tmsb.local changed from Green to Red
						0	VM_07 is disconnected
						0	VM_06 is disconnected

Figure 41. Examining Events for the Host

Once you restore the uplinks for the host, you can utilize the vSphere Client to examine the events for the host. This will show you that communication with the other hosts in the cluster has been re-established.

Even after you have re-established the network connections, you'll notice that the host still displays a warning. This warning is due to the fact that the ESXi Shell is still enabled.

	TM-POD01-ESX03 (Chassis 3 Server 8) File View Macros Tools Help Boot Server Shutdown Server Reset KVM Console Properties	
	Troubleshooting Mode Options	ESXi She11
r	Enable ESXi Shell Enable SSH Modify ESXi Shell tincout Restart Management Agents	ESXi Shell is Disabled Change current state of the ESXi Shell

Figure 42. Disabling ESXi Shell Access

Using the console, select **Disable ESXi Shell** under the Troubleshooting Mode Options screen to disable ESXi Shell access.

🤣 tm-pod01-vc01 - vSphere Client									
File Edit View Inventory Administration Plug-ins Help									
🕒 🔝 🏠 Home 🕨 🚮 Inv	entory 👂 🗊 Hosts and Clusters								
I & ø %									
tm-pod01-vc01 DemoDatacenter-01 DemoCluster-01 tm-pod01-esx01.tm tm-pod01-esx02.tm	DRS Resource Allocation Perfor	mance \ Tasks & Ever							
tm-pod01-esx03.tm	Name	State	vSphere HA State	Status					
₩_01	tm-pod01-esx02.tmsb.local	Connected	Connected (Slave)	📀 Normal					
M_02	tm-pod01-esx03.tmsb.local	Connected	📀 Connected (Slave)	📀 Normal					
WM_03	tm-pod01-esx01.tmsb.local	Connected	😨 Running (Master)	🤣 Normal					
K VM 05									

Figure 43. Verifying That Host is Operating Normally

Use the vSphere Client to show all of the hosts within the cluster and verify that the previously isolated host is now operating normally and has reconnected to the cluster.

Disabling VMware HA

As with the enabling of HA, disabling HA is a simple, straightforward process. This section will walk you through the required steps before continuing on to the next topic.

Connect to a Virtual Server

🖉 VMware vSphere Client	
vmware [.] VMware vSphere Client	
To directly manage a single To manage multiple hosts, vCenter Server.	e host, enter the IP address or host name. enter the IP address or name of a
IP address / Name:	tm-pod01-vc01
User name:	root
Password:	******
	Use Windows session credentials
😧 Connecting	Login Cancel Help

Figure 44. Connecting to a Virtual Server Instance

Using the vSphere Client, connect to your virtual server instance.

Im-pod01-vc01 - vSphere Client										
File Edit View Inventory Admin	File Edit View Inventory Administration Plug-ins Help									
💽 🔂 Anne 🕨 🛃 Inventory 👂 🎒 Hosts and Clusters										
E C tm-pod01-vc01	DemoCluster-01									
E E DemoCluster-01	Getting Started Summary Vir	tual Machines Hosts Resource Al	location Performance Tasks & Event	s Alarms Peri						
tm-pod01-esx01.tm	Conoral		vEnhoro HA							
tm-pod01-esx02.tm	General		Vopilere na							
WM 01	vSphere DRS:	Off	Admission Control:	Enabled						
M 02	vSphere HA:	On	Current Failover Capacity:	2 hosts						
₩_03	VMware EVC Mode:	Disabled	Configured Failover Capacity:	1 nost						
👘 VM_04	Total CPU Resources:	57 GHz	Host Monitoring:	Enabled						
👘 VM_05	Total Memory:	143.80 GB	VM Monitoring:	Enabled						
W06	Total Storage:	1.41 TB	Application Monitoring:	Disabled						
₩_07			Advanced Runtime Info							
	Number of Hosts:	3	Cluster Status							
	Total Processors:	24	Configuration Issues							
	Number of Datastore Clusters:	1	Storage							
	Total Datastores:	7	Storage resources 🛛 🖂 Status	Drive						
	Virtual Machines and Templateeu	7	TM-Gobal-Interch 📀 N	Normal Non-						
	Total Migrations using vMotion:	13	TM-POD01-ESX01 📀 N	Normal Non-						
		10	TM-POD01-ESX02 📀 N	Normal Non-						
			TM-POD01-ESX03 🧭 N	Normal Non-						
	Commands		👔 tm-pod01-sas300 🥏 N	Normal Non-						
	The second second		🗊 tm-pod01-sas600 🥏 N	Normal Non-						
	New Virtual Machine	P New Datastore Cluster	🗊 tm-pod01-sas600 🤗 N	Normal Non-						
	Add Host	🚮 Edit Settings	•							

Go to the Cluster Summary

Figure 45. Cluster Summary Screen

Once connected to your virtual server instance, select your cluster by clicking its name on the left-hand panel. Select the **Summary** tab to bring up the cluster summary screen.

🖉 DemoCluster-01 Settings		×
Cluster Features vSphere HA Virtual Machine Options VM Monitoring Datastore Heartbeating VMware EVC Swapfile Location	Name DemoCluster-01 ✓ Turn On vSphere HA vSphere HA detects failures and provides rapid recovery for the virtual machines running within a duster. Core functionality includes host and virtual machine monitoring to minimize downtime when hear tbeats cannot be detected. vSphere HA must be turned on to use Fault Tolerance.	
	 Turn On vSphere DRS vSphere DRS enables vCenter Server to manage hosts as an aggregate pool of resources. Cluster resources can be divided into smaller resource pools for users, groups, and virtual machines. vSphere DRS also enables vCenter Server to manage the assignment of virtual machines to hosts automatically, suggesting placement when virtual machines are powered on, and migrating running virtual machines to balance load and enforce resource allocation policies. vSphere DRS and VMware EVC should be enabled in the duster in order to permit placing and migrating VMs with Fault Tolerance turned on, during load balancing. 	
Help	OK Can	cel

Edit Cluster Settings

Figure 46. Cluster Settings Wizard

In the cluster summary screen, select the **Edit Settings** option. This will bring up a wizard that you can use to modify the settings of the cluster. Click the check box next to **Turn On vSphere HA** to deselect it and select OK. This will close the wizard and the system will unconfigure VMware HA.

Recent Tasks		
Name	Target	Status
Unconfiguring vSphere HA	tm-pod01-esx02.tmsb.local	In Progress
Unconfiguring vSphere HA	tm-pod01-esx03.tmsb.local	In Progress
🛛 🖗 Unconfiguring vSphere HA	tm-pod01-esx01.tmsb.local	In Progress

Figure 47. Viewing the Progress of the Unconfigure Task of VMware HA

Under the Recent Tasks pane of the vSphere Client, you can observe the progress of the unconfigure task of HA on the systems within the cluster.

Wait for Task to Complete

Recent Tasks		
Name	Target	Status
Unconfiguring vSphere HA	tm-pod01-esx02.tmsb.local	Completed
Unconfiguring vSphere HA	tm-pod01-esx03.tmsb.local	Completed
🖉 Unconfiguring vSphere HA	tm-pod01-esx01.tmsb.local	Completed

Figure 48. Unconfigure Tasks Completed

Wait until all the unconfigure tasks show a Completed status.

Getting Familiar with the New Command-Line Interface

Introduction

vSphere supports several command-line interfaces for managing your virtual infrastructure, including the VMware vSphere® Command-Line Interface (vCLI), a set of ESXi Shell commands, and VMware vSphere® PowerCLI. You can choose the CLI set best suited to your needs. The following table provides a summary of the command-line tools available in vSphere 5.0.

COMMANDS	STATE IN 5.0	AVAILABILITY	
esxcli commands	New in vSphere 5.0	 Available from the ESXi Shell and the vCLI Used for local and remote administration Used to manage most aspects of vSphere 	
vicfg- commands Minor changes in vSphere 5.0		 Available from the vCLI only Used for remote administration only Augments the esxcli commands to manage aspects not yet covered by esxcli 	
Other commands (vmware-cmd, vifs)	Minor changes in vSphere 5.0	 Available from the vCLI only Used for remote administration only Additional Perl commands used to manage aspects not covered with esxcli or vicfg- 	
vSphere PowerCLI	Minor changes and updates in vSphere 5.0	 vSphere PowerCLI Used for remote administration only Used to administer ESXi hosts from Windows systems 	

 Table 1. Summary of vSphere 5.0 Command-Line Tools

This section of the *VMware vSphere 5.0 Evaluation Guide, Volume One*, covers the new esxcli command-line interface. The esxcli command allows you to manage many aspects of an ESXi host. You can run esxcli commands remotely from the vCLI or locally from the ESXi Shell.

NOTE: The ESXi Shell is intended for advanced users, because even minor mistakes in the shell can result in serious problems. Users should use the vCLI for routine CLI administration and only fall back on the ESXi Shell when necessary. It is recommended that use of the ESXi Shell be limited to situations when you are working under the direction of the VMware Technical Support staff.

The New esxcli Command

For the first time, the new esxcli command is unified for both local and remote command-line administration. In addition, the esxcli command has been enhanced to perform many tasks previously only performed with the **vicfg-** commands. However, it does not yet perform all the tasks. When performing configuration tasks from the command line, the esxcli command is the preferred command. Only fall back to the **vicfg-** and other vCLI commands when there is no esxcli command available. Moving forward, all the vCLI commands are scheduled to be replaced by esxcli commands.

NOTE: In vSphere 5.0, the esxcli command does not yet provide a full set of command capabilities. Continue to use the esxcli command in conjunction with the vicfg- and other vCLI commands (that is, vmware-cmd, vmkfstools, and vifs). The esxcli command in vSphere 5.0 is not backward compatible with earlier versions of the command, because it introduces a new syntax that is different from earlier vSphere releases.

esxcli Command-Line Syntax

The esxcli command is made up of a hierarchy of namespaces. At each level of the hierarchy there are additional namespaces and commands. This provides for a user-friendly CLI interface that allows for the easy discovery of the command syntax.



Figure 49. esxcli Namespace Hierarchy

The preceding figure provides a graphic illustration of the command to query the ESXi firewall. The user invokes the **esxcli** command with the **network** namespace, the **firewall** sub-namespace, and the get command. The following is an example of this command:



Figure 50. esxcli network firewall get Command

At any time, you can use the **--help** option to discover information about the available namespaces and commands relative to your current namespace. In the following example, the **--help** parameter is used to get more information about the available namespaces and commands under the **network** namespace:

00	Terminal — ssh — 80×24	
~ # esxcli network ip Usage: esxcli network	help ip {cmd} [cmd options]	
Available Namespaces:		
dns	Operations pertaining to Domain Name Server configuration.	
interface	Operations having to do with the creation, management and deletion of VMkernel network interfaces (vmknic).	
connection	List active tcpip connections	
neighbor	Operations that can be performed on arp tables	
Available Commands:		
get	Get global IP settings	
set	Update global IP settings	
~ #		

Figure 51. Using the --help Parameter to Get Information About Namespaces and Commands

Every **esxcli** command is comprised of the esxcli command followed, if needed, by one or more **options**, followed by one or more **namespaces**, followed by the **command** to be executed along with any **command options**. The following screen shot shows the esxcli usage screen:

~ # esxclihelp Usage: esxcli [options]	<pre>{namespace}+ {cmd} [cmd options]</pre>	ñ
Options:		
formatter=FORMATTER		
	Override the formatter to use for a given command. Available	
debug	Enable debug or internal use ontions	
version	Display version information for the script	
-?,help	Display usage information for the script	
Available Namespaces:		
esxcli	Commands that operate on the esculi system itself allowing	
fcoo	VM-uses ECOE commande	
hardware	Vriware FLUE commanus.	
naruware	hardware.	
iscsi	VMware iSCSI commands.	
network	Operations that pertain to the maintenance of networking on an ESX host. This includes a wide variety of commands to manipulate virtual networking components (vswitch, portgroup, etc) as well as local host IP, DNS and general host networking settings.	
software	Manage the ESXi software image and packages	
storage	VMware storage commands.	
system	VMKernel system properties and commands for configuring	
	properties of the kernel core system.	
Vm	A small number of operations that allow a user to Control Virtual Machine operations.	ļ
~ #		Ţ

Figure 52. esxcli -help Example

Although the esxcli command is unified for both local and remote administration, the syntax does vary slightly, depending upon if you are running commands locally from the ESXi Shell or remotely through the vCLI.

- When running esxcli commands locally from the ESXi Shell, the target host is always the local host on which the command is run. In addition, the login credentials are always assumed to be those of the logged-in user.
- When running the esxcli commands remotely, you must specify the target ESXi host (or VMware vCenter Server™), along with the user credentials used to execute the command.

Remote esxcli Command Authentication

When running esxcli commands remotely, you must specify a target ESXi host or vCenter server and provide the user credentials for the command. The following are methods available to perform user authentication:

- Using command-line options
- Using a session file
- Using environment variables
- Using a configuration file
- Using Microsoft Windows --passthroughauth
- Using VMware vSphere® Management Assistant (vMA) vi-fastpass

Details for each method are documented in the Getting Started with vSphere Command-Line Interfaces guide.

The following examples illustrate the different syntax required when running the **esxcli hardware platform get** command from the local ESXi Shell, compared to running it remotely from the vCLI. You must add the **--server** and --**user** options when running the command remotely, in addition to being prompted to enter the password.



Figure 53. Sample esxcli Command Run from ESXi Shell



Figure 54. Sample esxcli Command Run Remotely from vMA

Enabling Access to the ESXi Shell

Before you can run esxcli commands on the host, you must enable the ESXi Shell. Complete the steps in this section to enable the ESXi Shell on each ESXi host.

Enabling the ESXi Shell from the DCUI

Perform the following steps in order to enable the ESXi Shell while logged into the DCUI:

- Log in to the ESXi host DCUI.
- Select Troubleshooting Mode Options.
- Select Enable ESXi Shell and press return.
- Press Alt-F1 to access the ESXi Shell.

Troubleshooting Mode Options	ESXi Shell	
Disable ESXi Shell Disable SSH Modify ESXi Shell timeout Restart Management Agents	ESXi Shell is Enabled Change current state of the ESXi Shell	

Figure 55. Enable ESXi Shell from DCUI

Enabling the ESXi Shell from the vSphere Client

Perform the following steps to enable the ESXi Shell while logged into the vSphere Client:

- Log in to the vSphere Client.
- Select the ESXi host and choose Configuration -> Security Profile.
- From the Services section, select Properties.
- Select the ESXi Shell option and choose Options.
- Select **Start** to start the ESXi Shell, enabling local access to the ESXi Shell.

Remote Access By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.	
By default, remote clients are prevented from accessing services on this host, and local clients are prevented from accessing services on remote hosts.	
Unless configured otherwise, daemons will start automatically.	
Label Daemon	
I/O Redirector (Active Directory Sec. Stopped	
Network Login Server (Active Directory Schned	
Ibtd Pupping	
vSobere High Availability Agent Stopped	
ESXi Shell Running	
Local Security Authentication Serv Stopped	
NTP Daemon Stopped	
ESXi Shell (TSM) Options	
Status	
Running	
-Startup Policy	
Start automatically if any ports are open, and stop when all ports are closed	
Start and stop with host	
Start and stop manually	
Service Commands	
Start Stop Destart	
Kestart	
Ontions	
OK Cancel Help	
OK Cancel Help	

Figure 56. Enable ESXi Shell from vSphere Client

Enabling SSH Access to the ESXi Shell

In addition to running commands directly from the ESXi console, you can also enable SSH services to allow remote access to the ESXi Shell. The following section shows how to enable SSH access to the ESXi Shell.

Enabling SSH from the DCUI

Perform the following steps to enable the ESXi Shell from the DCUI:

- Log in to the ESXi host DCUI.
- Select Troubleshooting Options.
- Select Enable ESXi Shell and press return.
- Press Alt-F1 to access the ESXi Shell.

Troubleshooting Mode Options	SSH Support
Disable ESXi Shell Disable SSH Modify ESXi Shell timeout Restart Management Agents	SSH is Enabled Change current state of SSH

Figure 57. Enable SSH from DCUI

Enabling the SSH from the vSphere Client

Perform the following steps to enable the ESXi Shell from the vSphere Client:

- Log in to the vSphere Client.
- Select the ESXi host and choose Configuration -> Security Profile.
- From the Services section, select Properties.
- Select the SSH option and choose Options.
- Select **Start** to start SSH on the host.

Services Properties		
Remote Access By default, remote clients are prevente accessing services on remote hosts. Unless configured otherwise, daemons w	d from accessing services on this host, and local clients are prevented from will start automatically.	
Label	Daemon	-
I/O Redirector (Active Directory Se	Stopped	
Network Login Server (Active Direc	Stopped	
	Running	
v5phere High Availability Agent	Stopped	
vpxa	Running	
ESXI Shell	Running	
Local Security Authentication Serv	Stopped	
NTP Daemon	Stopped	
SSH	Running	
SSH (TSM-SSH) Options	X	
Status		
Running		
-Startup Policy		
Start automatically if any ports a	are open, and stop when all ports are closed	
Start and stop with host		
C Start and stop manually		
Service Commands Start Stop	Restart Options	
	OK Cancel Help Cancel	Help

Figure 58. Enable SSH from vSphere Client

vSphere Client Notification When the ESXi Shell and SSH Are Enabled

Any time the ESXi Shell or SSH is enabled on a host, the vSphere Client will show a warning on the host summary page serving as a reminder to disable the access when it is no longer needed.



Figure 59. Notification That the ESXi Shell Has Been Enabled

Installing the vCLI

The vCLI is available on Microsoft Windows, Linux, and with the vMA virtual appliance.

Installing the vCLI on Windows

The vCLI installation package for Windows includes the ActivePerl runtime environment, along with the required Perl modules and libraries. The vCLI is supported on the following Windows platforms:

- Microsoft Windows Vista Enterprise SP1 32-bit and 64-bit
- Microsoft Windows 2008 64-bit
- Microsoft Windows 7 32-bit and 64-bit

To install the vCLI on Windows, download the vCLI installer package for Windows on a supported Windows server and launch the installer. Refer to Chapter 2 of the *Getting Started with vSphere Command-Line Interfaces* guide for information on how to install the vCLI on a Windows server.

Installing the vCLI on Linux

The vCLI installation package for Linux includes the vCLI scripts and the VMware vSphere 5.0 SDK for Perl. In can be installed on the Red Hat Enterprise Linux 5.5 server, SUSE Linux Enterprise 10 and 11 servers, and the Ubunto 10.04 server. Download the vCLI package for your Linux distribution and run the installation script. Refer to Chapter 2 of the *Getting Started with vSphere Command-Line Interfaces* guide for information on how to install the vCLI on a Linux server.

Installing the vCLI with the vMA

The vMA includes a Linux environment, the vCLI, and other prepackaged software. To install the vCLI with the vMA, simply deploy the vMA and log in to the console to configure the appliance. Refer to Chapter 2 of the *Getting Started with vSphere Command-Line Interfaces* guide for information on how to install and configure the vMA.

Sample esxcli Commands Run Locally from the ESXi Shell

The following examples show esxcli commands executed from the local ESXi Shell. Because they are being run from the ESXi Shell, it is not necessary to provide the server information or user credentials with the command.

Use the **esxcli system hostname set --host tm-pod01-esx01 --domain tmsb.local** command to set the host name and domain name of the ESXi host. Then use the **esxcli system hostname get** command to display the host name and domain name and verify the change.



Figure 60. Set ESXi Host Name and Domain Name from the ESXi Shell

Use the **esxcli system syslog config get** command to display the ESXi host syslog configuration, as follows:



Figure 61. Display Host Syslog Settings from the ESXi Shell

Use the **esxcli storage core device list** command to list all the storage devices on the ESXi host, as follows:

00	Terminal — ssh — 88×31	
~ # esxcli storage core device	list	
naa.50060160c4603f9550060160c46	03f95	
Display Name: DGC Fibre Chan	nel Disk (naa.50060160c4603f9550060160c4603f95)	
Has Settable Display Name: t	rue	
Size: 0		
Device Type: Direct-Access		
Multipath Plugin: NMP		
Devfs Path: /vmfs/devices/di	lsks/naa.50060160c4603f9550060160c4603f95	
Vendor: DGC		
Model: LUNZ		
Revision: 0430		
SCSI Level: 4		
Is Pseudo: true		
Status: on		
Is RDM Capable: true		
Is Local: false		
Is Removable: false		
Is SSD: false		
Is Offline: false		
Is Perennially Reserved: fal	se	
Thin Provisioning Status: un	Iknown	
Attached Filters:		
VAAI Status: unsupported		
Other UIDs: vml.020000000050	060160c4603f9550060160c4603f954c554e5a2020	
naa 6006016001612800a4cd447e445	46011	
Display Name: DGC Fibre Chan	unel Disk (naa 6006016091612800a4cd447e4454e011)	<u> </u>
Has Settable Display Name: t	rue	
Size: 102400		
Device Type: Direct-Access		4
Multinath Plugin: NMP		<u> </u>
naccipacit i cagini ini		1

Figure 62. Display Storage Devices from the ESXi Shell

Use the **esxcli network ip interface ipv4 get** command to list all the configured IPv4 addresses on the ESXi host, as follows:

00	0		${\sf Terminal-ssh-}$	88×31		
~ # e Name	sxcli network IPv4 Address	ip interface ip IPv4 Netmask	v4 get IPv4 Broadcast	Address Type	DHCP DNS	, I
vmk0 vmk1 vmk2	10.91.33.1 10.91.36.1 10.91.38.1	255.255.254.0 255.255.254.0 255.255.254.0	10.91.33.255 10.91.37.255 10.91.39.255	STATIC STATIC STATIC	false false false	
vmk3 vmk4 ~ #	10.91.40.1 10.91.42.1	255.255.254.0 255.255.254.0	10.91.41.255 10.91.43.255	STATIC	false false	

Figure 63. Display Configured IPs from the ESXi Shell

Sample esxcli Commands Run Remotely from the vCLI

The following examples show methods for using esxcli from the vCLI. For these examples, we will use the vMA. Because these commands are being run remotely, it is necessary to provide the **--server** and **--username** credentials as part of the esxcli command.

Use the **esxcli** --server tm-pod01-esx01 hardware memory get command to display the amount of memory on the ESXi hosts. Here we provide the --server option, but let it prompt for the user name and password, as follows:

000	Terminal — ssh — 88×31	
vi-admin@vma50:~> esxc Enter username: root Enter password: Physical Memory: 514 NUMA Node Count: 2 vi-admin@vma50:~>	liserver tm-pod01-esx01 hardware memory get 469144064 Bytes	

Figure 64. esxcli hardware memory get Command from vMA

Use the **esxcli** --server tm-pod01-esx01 --user root storage core adapter list command to list the available storage adapters on your host. Here we provide the --server and --user options, but let it prompt for the password, as follows:

000			Terminal — ssh — 88×31	i de la companya de l
vi-admin@ Enter pas	vma50:~> esxc sword:	li —server	tm-pod01-esx01user root storage core	e adapter list 🚪
HBA Name	Driver	Link State	UID	Description
			·	
vmhba0 ogic / Sv	mptsas mbios Logic L	link-n/a SI1064E	sas.51cdf0ffa0ac4000	(0:1:0.0) LSI L
vmhba1 o Svstems	fnic Inc Cisco VI	link-up C FCoE HBA	fc.20000025b500000d:20010025b500003d	(0:12:0.0) Cisc
vmhba2 o Systems	fnic Inc Cisco VI	link-up C FCoE HBA	fc.20000025b500000d:20010025b500002d	(0:13:0.0) Cisc
vmhba32	usb-storage	link-n/a	usb.vmhba32	() USB
vmhba33 Adapter vi-admin@	iscsi_vmk vma50:~> [online	iscsi.vmhba33	iSCSI Software

Figure 65. esxcli storage core adapter list Command from vMA

In this example, we use the vMA -vi-fastpass authentication, making it possible to run esxcli commands without providing the -server, -username, or -password options on the command line.

Start by setting up the vMA fastpass access, as follows:

000	Terminal — ssh — 88×31	
<pre>vi-admin@vma50:~> vi-admin@vma50:~></pre>	<pre>vifp addserver tm-pod01-esx01username rootpassword vmware1! vifptargetset_tm-pod01-esx01</pre>	
vi-admin@vma50:~[t	m-pod01-esx01]>	

Figure 66. Setting up vMA Fast Pass

With the fast pass target set to our ESXi host, we can now run the commands without specifying the options for the ESXi host, user name, or password. In the following example, we use the **esxcli system coredump partition list** command to show the configured core dump partition:

00	Terminal — ssh — 88×31			
vi—admin@vma50:~[tm—pod Name	01-esx01]> esxcli system coredump partition Path	list Active	Configured	
naa.500000e1160febb0:7 vi—admin@vma50:~[tm—pod	/vmfs/devices/disks/naa.500000e1160febb0:7 01-esx01]>	true	true	

Figure 67. Display core dump partition list from vMA

In the following example, we will connect to the vCenter Server rather than connecting directly to the ESXi host. We will set the ESXi Shell timeout value to 300 seconds.

0 0	Terminal — ssh — 80×24
<pre>vi-admin@vma50:~> esxcli alusername rootpasswo serVars/ESXiShellTimeOut vi-admin@vma50:~></pre>	-server tm-pod01-vc01vihost tm-pod01-esx01.tmsb.loc ord vmware1! system settings advanced set -i 300 -o /U

Figure 68. Set ESXiShellTimeOut

We can verify the change by displaying the new value of the ESXiShellTimeout, as follows:



Figure 69. Display ESXiShellTimeOut

Formatting esxcli Output

It is common to use the output of the esxcli command as input to another program or for inclusion in a report. To facilitate this, the esxcli command enables you to format and filter the command output in one of three formats: comma-separated values (CSV), key-value pair, or XML. In addition, you can specify which fields to include in the output.

In the following example, we need to generate a report showing all the configured interfaces on a host along with the vSwitch and port group to which they are assigned. We start by running the **esxclinetwork ip interface list** command, as follows:



Figure 70. esxcli network ip interface list Command from the ESXi Shell

The output gives us the information we need, but it is very verbose, requiring the user to use the scroll bar to see the data for all the interfaces. Because we need only a summary showing the interface name, vSwitch, and port group, we can refine our command using the **--formatter** and **--format-param** options, as follows:



Figure 71. esxcli Command with -formatter Option from the ESXi Shell

Now we have a short list giving us just the information we need.

The localcli Command

The **esxcli** command talks to the ESXi hosts through the **hostd** service. In rare circumstances, when the **hostd** service might not be responding, the **localcli** command can be used. The **localcli** command is equivalent to **esxcli** with the exception that it bypasses **hostd**. The **localcli** command is only intended for situations when **hostd** is unavailable and cannot be restarted. After you run the **localcli** command, you must restart **hostd**. Run **esxcli** commands after the restart.

NOTE: Use the **localcli** command only under the direction of VMware technical support, because improper use can result in an inconsistent system state and potential failure of the ESXi host.

The following example shows the use of the localcli command to display all network adaptors on a host:

00	Termir	nal — ssh	- 80×24			
<pre>~ # localcli network nic list Name PCI Device Driver cription</pre>	Link	Speed	Duplex	MAC Address	MTU	Des
vmnic0 0000:008:00.0 enic co Systems Inc Cisco VIC Ethe	Up rnet NI	10000 C	Full	00:25:b5:00:00:0d	1500	Cis
<pre>vmnic1 0000:009:00.0 enic co Systems Inc Cisco VIC Ethe</pre>	Up rnet NI	10000 C	Full	00:25:b5:00:01:0d	1500	Cis
<pre>vmnic2 0000:00a:00.0 enic co Systems Inc Cisco VIC Ethe</pre>	Up rnet NI	10000 C	Full	00:25:b5:00:02:0d	1500	Cis
<pre>vmnic3 0000:00b:00.0 enic co Systems Inc Cisco VIC Ethe ~ #</pre>	Up rnet NI	10000 C	Full	00:25:b5:00:03:0d	1500	Cis

Figure 72. localcli Command Example

Bringing It All Together

The following example shows how to generate a list of the VMFS file systems on an ESXi host that have not been upgraded to VMFS-5. In this example, we will demonstrate the syntax discovery feature of esxcli.

Start by looking at the namespaces available under the storage namespace by running the **esxcli** storage **--help** command, as follows:

0 0	Terminal — ssh — 88×31	1000
~ # esxcli storageh	elp	
Usage: esxcli storage	<pre>{cmd} [cmd options]</pre>	
Available Namespaces:		
core	VMware core storage commands.	
nmp	VMware Native Multipath Plugin (NMP). This is the VMware default implementation of the Pluggable Storage Architecture.	
vmfs	VMFS operations.	
filesystem	Operations pertaining to filesystems, also known as datastores, on the ESX host.	
nfs	Operations to create, manage and remove Network Attached Storage filesystems.	
~ #		

Figure 73. esxcli Namespaces Under Storage from ESXi Shell

We see here that there is a **filesystem** name space. Next, we look to see what namespaces and commands are available under the **esxcli storage filesystem** namespace by running the **esxcli storage filesystem** --help command, as follows:

00	Terminal — ssh — 88×31	10-10-
~ # esxcli storage Usage: esxcli stora	filesystem ——help age filesystem {cmd} [cmd options]	
Available Commands:		
automount	Request mounting of known datastores not explicitly unmounted.	
list	List the volumes available to the host. This includes VMFS,	
	NAS and VFAT partitions.	
mount	Connect to and mount an unmounted volume on the ESX host.	
rescan	Issue a rescan operation to the VMkernel to have is scan storage devices for new mountable filesystems.	
unmount	Disconnect and unmount and existing VMFS or NAS volume. This will not delete the configuration for the volume, but will remove the volume from the list of mounted volumes.	
~ #		

Figure 74. esxcli Namespaces Under Storage Filesystem from ESXi Shell

We see that there is a **list** command under the **filesystem** namespace that will list all the volumes on the host along with the VMFS information. We now run the final command, **esxcli storage filesystem list**, as follows:

00		Termin	nal — ssh — 88×	31	
~ # esxcli storage file Mount Point	esystem li	ist	Vo	lume Name	UUID
	Mounted	Туре	Size	Free	
					40fb32b0-1023
d55c-7f6b-0025b500010d	true	VMFS-5	141733920768	140707364864	49103209-1923
/vmfs/volumes/4d677880- 0564-edd7-0025b500020f	-9b5a0564- true	-edd7-002 VMFS-3	25b500020f TM 805037932544	-Gobal-Interchange01 576271155200	4d677880-9b5a
/vmfs/volumes/4d884a01- 9478-2e69-0025b500020d	-73289478- true	-2e69-002 VMFS-5	25b500020d tm 107105746944	-pod01-sas600-sp-01 48990519296	4d884a01-7328
/vmfs/volumes/4de87ff2- 50ea-c40d-0025b500021d	-e1c750ea- true	-c40d-002 VMFS-5	25b500021d tm 107105746944	-pod01-sas300-sp 28653387776	4de87ff2-e1c7
/vmfs/volumes/4de8d49f- 5bbe-8329-0025b500020d	-1c585bbe- true	-8329-002 VMFS-5	25b500020d tm 107105746944	-pod01-sas600-sp-02 62974328832	4de8d49f-1c58
/vmfs/volumes/4dd49b84- e216-30f7-0025b500010d	-eb00e216- true	-30f7-002 vfat	25b500010d 4293591040	4286251008	4dd49b84-eb00
/vmfs/volumes/28e8cd74- d7o1-062d-d422f191b670	-297ed7e1-	-962d-d43	3f181b670	11/620656	28e8cd74-297e
/vmfs/volumes/d52f4476-	-aa477643-	-f71b-3cf	8c9741af8	114030030	d52f4476-aa47
7643-171b-3cf8c9741af8 /vmfs/volumes/4d827f69-	true- d75bd996-	vfat -4b5d-002	261853184 25b500010d	128200704	4d827f69-d75b
d996-4b5d-0025b500010d ~ #	true	vfat	299712512	115064832	

Figure 75. esxcli storage filesystem list Command from ESXi Shell

This command gives us what we need. However, there is a lot of extra information in the output, making it hard to extrapolate the VMFS version information needed for our report. We can use the **--formatter** option with the **--format-param** filter to show only the information we need, as follows:

● ○ ○ Terminal — ssh — 88×31
🖌 # esxcli ——formatter=csv ——format—param=fields="MountPoint,Type,VolumeName" storage fi 💻
lesystem list
ountPoint,Type,VolumeName,
<pre>/vmfs/volumes/49fb32b9-1923d55c-7f6b-0025b500010d,VMFS-5,TM-POD01-ESX01-Local,</pre>
<pre>/vmfs/volumes/4d677880-9b5a0564-edd7-0025b500020f,VMFS-3,TM-Gobal-Interchange01,</pre>
<pre>/vmfs/volumes/4d884a01-73289478-2e69-0025b500020d,VMFS-5,tm-pod01-sas600-sp-01,</pre>
<pre>/vmfs/volumes/4de87ff2-e1c750ea-c40d-0025b500021d,VMFS-5,tm-pod01-sas300-sp,</pre>
<pre>/vmfs/volumes/4de8d49f-1c585bbe-8329-0025b500020d,VMFS-5,tm-pod01-sas600-sp-02,</pre>
/vmfs/volumes/4dd49b84-eb00e216-30f7-0025b500010d,vfat,,
vmfs/volumes/28e8cd74-297ed7e1-962d-d433f181b670,vfat,,
vmfs/volumes/d52f4476-aa477643-f71b-3cf8c9741af8,vfat,,
<pre>/vmfs/volumes/4d827f69-d75bd996-4b5d-0025b500010d,vfat,,</pre>
• #

Figure 76. esxcli storage filesystem list with Formatting Command from ESXi Shell

We now have a list showing all the file systems on the ESXi host, along with the corresponding VMFS versions. From this we can easily identify those file systems that have not been upgraded to VMFS-5.

vSphere PowerCLI by Example

Introduction

vSphere PowerCLI is a snap-in (add-on) to Microsoft Windows PowerShell, a command-line scripting environment designed for Windows. It leverages the .NET object model, and was designed as an administrative language with system administrators in mind, because it provides administrators with easy-to-learn management and automation capabilities. vSphere PowerCLI adds over 200 cmdlets (commands) to native PowerShell commands, enabling the management of the vSphere environment.

Prerequisites

vSphere PowerCLI is typically installed on a vSphere administrator's Microsoft Windows-based desktop system. In order to support the installation of vSphere PowerCLI to a desktop system, the following prerequisite software packages must be present:

- Windows .NET Framework 3.5
- Windows PowerShell (V2 recommended)

Windows PowerShell V2 is integrated with Windows 7 and Windows 2008 R2. Previous operating systems, such as Windows XP, Windows Vista, Windows 2008 (not R2), and Windows 2003, are compatible with Windows PowerShell. This must be first downloaded and installed from the following Web site: http://support.microsoft. com/kb/968929

Install vSphere PowerCLI

After checking that all prerequisites are installed, you must set the execution policy of PowerShell to enable it to run scripts. By default, PowerShell is installed in secure mode, which will disable the running of scripts within PowerShell. To change the execution policy, start a PowerShell session with administrator privileges, as follows:

Programs (5) Windows PowerShell Windows PowerShell (x86)		Open
Windows PowerShell ISE Windows PowerShell ISE (x86)	۲	Run as administrator
🛃 Windows PowerShell Modules	۵	Scan for threats Pin to Taskbar Pin to Start Menu
	U	Open with Scan for threats
		Restore previous versions
		Cut Copy
♀ See more results		Delete Properties
PowerShell ×		Shut down 🔸
👌 🙆 👸 🔕		

Figure 77. Starting PowerShell Session

From the Windows start menu, type **PowerShell**. Once the PowerShell program is displayed on the start menu, **right-click Windows PowerShell** and select **Run as administrator**.

A PowerShell prompt will be started, as follows:



Figure 78. Setting Execution Policy

It is recommended that you read more about PowerShell's different execution policies to find out more information about these, and ensure that you change this to the correct setting for your organization. Enter **get-help about_Execution_Policies** at the PowerShell prompt.

In this guide, we will change the execution policy to RemoteSigned.

From the PowerShell prompt, enter Set-ExecutionPolicy RemoteSigned.



Figure 79. Information About Execution Policies

You will then receive information about execution policies and a prompt asking you to confirm your action before changing the execution policy. Enter **Y** at the prompt and **press Enter**.

You will then be returned to the PowerShell prompt with the change being completed. Type **Exit** and **press Enter** to leave the PowerShell prompt.

You are now ready to install vSphere PowerCLI.



Figure 80. vSphere PowerCLI Download Screen

Download the vSphere PowerCLI software to your workstation from the following URL: http://vmware.com/go/ PowerCLI

Once the software has been downloaded, start the installation by double-clicking the vSphere PowerCLI .exe file.



Figure 81. Notification of VMware VIX Installation

The installer will first notify you that an additional component, VMware VIX, will be installed as part of the vSphere PowerCLI installation. Click **OK**.

😸 VMwar	re vSphere PowerCLI
1	The PowerShell execution policy of this computer is not set to "RemoteSigned". This prevents execution of PowerShell scripts on your computer. This will result in non-problematic errors when VMware vSphere PowerCLI is invoked. It is recommended that you set the execution policy to "RemoteSigned" in order to be able to execute scripts and to hide the errors in VMware vSphere PowerCLI Console. This can be done by invoking the command 'Set-ExecutionPolicy RemoteSigned' from a PowerShell prompt.
	Press Continue to skip and continue install or Cancel to exit the installation.
InstallShield	Continue Cancel

Figure 82. Recommendation to Set Execution Policy Correctly

If you have not yet set your execution policy correctly, an information box will appear advising you that this will need to be set to RemoteSigned before vSphere PowerCLI will execute correctly. Click the **Continue** button.

If the execution policy is set correctly this box will not appear.

This will bring you to the following **welcome screen:**

😸 VMware vSphere PowerCLI	×		
	Welcome to the InstallShield Wizard for VMware vSphere PowerCLI		
	The InstallShield(R) Wizard will install VMware vSphere PowerCLI on your computer. To continue, click Next.		
vSphere PowerCLI	WARNING: This program is protected by copyright law and international treaties.		
Build version: 5.0.0.3444	< Back Next > Cancel		

Figure 83. Welcome Screen

The welcome screen will now be shown, welcoming you to the install wizard for vSphere PowerCLI. Click **Next** to continue.

This will bring you to the following VMware Patents screen:

授 VMware vSphere PowerCLI	×
VMware Patents This product is covered by one or more of the patents listed below.	
	_
Copyright © 1998-2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one o more U.S. Patent Numbers	r 🗉
D617,808, D617,809, D617,810, D617,811, 6,075,938, 6,397,242, 6,496,84 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,9 6,880,022, 6,883,095, 6,940,980, 6,944,699, 6,961,806, 6,961,941, 6,970,9 7,017,041, 7,055,032, 7,065,642, 7,069,413, 7,069,435, 7,082,598, 7,089,3 7,111,086, 7,111,145, 7,117,481, 7,149,310, 7,149,843, 7,155,558, 7,222,2 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,0 7,281,102, 7,290,253, 7,343,599, 7,356,679, 7,386,720, 7,409,487, 7,412,4 7,412,702, 7,424,710, 7,428,636, 7,433,951, 7,434,002, 7,447,854, 7,447,9	7, 666, 662, 777, 221, 300, 92, 903, •
InstallShield Car	ncel

Figure 84. VMware Patents Screen

Click Next to continue. This will bring you to the following License Agreement screen:

1	VMware vSphere PowerCLI	×				
	License Agreement	ר				
	Please read the following license agreement carefully.	5				
	VMware® End User License Agreement	<u>_</u>				
	VMware, Inc. ("VMware") provides the VMware vSphere					
	PowerCLI (the "Software") to you subject to the following terms and					
	conditions. If you disagree with any of the following terms, then do					
	not use the Software.					
	 The Software contains a variety of materials, interface definitions, documentation, and sample utility applications and sample code regarding 					
	Inrogramming interfaces to one or more VMware products as referenced in	È.				
	I accept the terms in the license agreement Print					
	I do not accept the terms in the license agreement					
I	nstallShield					
	< Back Next > Cancel					

Figure 85. License Agreement Screen

Select the option, I accept the terms in the license agreement and then click Next to continue.

This will bring you to the following **Destination Folder screen:**

😸 VMware vSp	here PowerCLI				×	
Destination Click Next to	Folder o install to this folder	, or click Change to in	istall to a different	folder.		
The wizard will install the files for VMware vSphere PowerCLI in the folder specified below. To install to a different folder, dick the Change button.						
Destination Fo	lder					
C:\Program I	iles (x86)\VMwaı	re\Infrastructure\	vSphere Power(.11/		
Volume	Disk Size	Available	Required	Differences	•	
D:	2046MB	1664MB	68KB	1664MB		
⊜ E:	4093MB	1888MB	0KB	1888MB	•	
InstallShield						
		< Back	Next >	Cancel		

Figure 86. Destination Folder Screen

Select the drive you would like to install vSphere PowerCLI onto and the folder name, or leave this set as the recommended path and click **Next**.

This will bring you to the following **Ready to Install screen:**

😸 VMware vSphere PowerCLI	×
Ready to Install the Program	ר
The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, dick Back. Click Cancel to exit the wizard.	
InstallShield < Back Install Cancel	

Figure 87. Ready to Install Screen

Click Install to begin the **Installation** of PowerCLI.

This will bring you to the Installing VMware vSphere PowerCLI screen.

븅 VMware v	/Sphere PowerCLI	
Installing The prog	VMware vSphere PowerCLI ram features you selected are being installed.	
12	Please wait while the InstallShield Wizard installs VMware vSphere PowerCLI. This may take several minutes.	
	Progress:	
	Details	
InstallShield —	< Back Next >	Cancel

Figure 88. Installing vSphere PowerCLI

Wait while the installation is completed.

📸 VMware vSphere PowerCLI		×
	InstallShield Wizard Completed	
	The InstallShield Wizard has successfully installed VMware vSphere PowerCLI. Click Finish to exit the wizard.	
vSphere PowerCLI		
vm ware [.]		
Build version: 5.0.0.3444	< Back Finish Cance	1

Figure 89. Installation Finish Screen

When the installation is successful, the **finish screen** will be displayed. To complete the installation, click **Finish.**

The vSphere PowerCLI installation will now be completed, and on your desktop you will now have two icons, which allow you to launch vSphere PowerCLI, a 64-bit version and a 32-bit version.

Getting Started with vSphere PowerCLI

On your start menu in the VMware -> VMware vSphere PowerCLI folder, you will now have access to the following items:

- vSphere PowerCLI (32-Bit)
- vSphere PowerCLI
- vSphere PowerCLI Administration Guide
- vSphere PowerCLI Cmdlets Reference
- vSphere SDK for .NET API Reference
- vSphere SDK for .NET Dev Guide

It is highly recommended that you read the *vSphere PowerCLI Administration Guide*, because this will provide the fundamentals of both vSphere PowerCLI and PowerShell, and will aid in the learning process when starting out with vSphere PowerCLI. This guide will show examples of vSphere PowerCLI and PowerShell code, but will not provide all knowledge to learn these languages in full. For further help and support, visit the vSphere PowerCLI community site at http://vmware.com/go/PowerCLI.

Connecting to a vSphere Host or vCenter

With vSphere PowerCLI, you have the ability, as with the vSphere Client, to connect to both vSphere hosts and vCenter servers. This document will show how to manage a vCenter Server and all connected entities, but it should be noted that the same cmdlets could be used to manage a single vSphere host.



Figure 90. Launching PowerShell Session

From the start menu, select VMware -> VMware vSphere PowerCLI -> VMware vSphere PowerCLI.

This will launch a new PowerShell session and automatically import the VMware snap-in used to manage the VMware environment, as follows:

🕼 [vSphere PowerCLI] Not Connected	- • ×
Welcome to the VMware vSphere PowerCLI!	
Log in to a vCenter Server or ESX host: Connect-VIServe To find out what commands are available, type: Get-VICommand	•
To show searchable help for all PowerCLI commands: Get-PowerCLIHel Once you've connected, display all virtual machines: Get-VM If you need more help, visit the PowerCLI community: Get-PowerCLICom	p munity
Copyright (C) 1998-2011 UMware, Inc. All rights reserved.	
PowerCLI C:\> Connect-VIServer tm-pod01-vc01 -User root -Password "P	essword!"
	Ŧ

Figure 91. Connecting to vCenter Server

Use the **Connect-VIServer** cmdlet to connect to your vCenter Server. A user and password parameter can be used with this cmdlet to specify the connection credentials. If no user and password parameter is used, the cmdlet will try to log in with your current logged-on Windows credentials. If a connection cannot be made from the current credentials, you will be prompted for a user name and password.

Once connected, you will be returned to the vSphere PowerCLI prompt. You are then ready for your next cmdlet to be executed, as follows:

[vSphere PowerCLI] Connected to tm-pod01	-vc01 a	s root		- • •
Log in to a vCenter Server or ES To find out what commands are av To show searchable help for all Once you've connected, display a If you need more help, visit the	nity			
Copyright (C) 1998-2011 V	Mware	e, Inc. All right	ts reserved.	
PowerCLI C:\> Connect-VIServer tm-pod01-vc01 WARNING: There were one or more problems with the server certificate: * A certification chain processed correctly, but terminated in a root certificate which isn't trusted by the trust provider.				
* The certificate's CN name does not match the passed value.				
Nane F	ort	User		
 tm-pod01-vc01 4	43	root		
PowerCLI C:>>				~

Figure 92. Certificate Warning

During this "vSphere PowerCLI by Example" section, the certificate warning can be ignored.

Once you are connected, the Name, Port and User properties used to make the connection will be returned to show a successful connection.

Using vSphere PowerCLI

🧐 [vSphere PowerCLI] Conne	cted to tm-pod01	-vc01 as root		- • •
PowerCLI C:\> Get-VM				A
Name	PowerState	Num CPUs	Memory (MB)	E
UM_01 UM_07 UM_02 UM_03 UM_04 UM_05 UM_06 PowerCLI C:\> _	PoweredOn PoweredOn PoweredOn PoweredOn PoweredOn PoweredOn	2 1 2 2 1 1 1	4096 4096 4096 4096 1024 1024 1024	

Figure 93.

To retrieve a list of virtual machines attached to the connected vCenter server, type **Get-VM**. This will return the Name, PowerState, Num CPUs and Memory (MB). These are all called properties of the virtual machine. vSphere PowerCLI returns more information than what is shown on the screen. It actually returns an object to this vSphere PowerCLI session containing more information about the virtual machine.

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root					
PowerCLI C:\> Get-UM	PowerCLI C:\> Get-VM Get-Member				
TypeName: UMware.Vim	Automation.	JiCore.Impl.U1.Inventory.VirtualMachineImpl	=		
Name	MemberType	Definition			
Equals	Method	bool Equals(System.Object obj)			
GetHashCode	Method	int GetHashCode()			
GetType	Method	type GetType()			
ToString	Method	string ToString()			
CDDrives	Property	UMware.UimAutomation.ViCore.Types.V1.Virt			
CustomFields	Property	System.Collections.Generic.IDictionary'2[
DatastoreIdList	Property	System.String[] DatastoreIdList {get;}			
Description	Property	System.String Description (get;)			
DrsAutomationLevel	Property	System.Nullable`1[[VMware.VimAutomation.V			
ExtensionData	Property	System.Object ExtensionData {get;}			
FloppyDrives	Property	VMware.VimAutomation.ViCore.Types.V1.Virt			
Folder	Property	VMware.VimAutomation.ViCore.Types.V1.Inve			
FolderId	Property	System.String FolderId {get;}			
Guest	Property	VMware.VinAutomation.ViCore.Types.V1.VM.G			
HAIsolationResponse	Property	System.Nullable`1[[VMware.VimAutomation.V			
HardDisks	Property	VMware.VinAutomation.ViCore.Types.V1.Virt			
HARestartPriority	Property	System.Nullable`1[[VMware.VimAutomation.V			
Host	Property	VMware.VimAutomation.ViCore.Types.V1.Inve			
HostId	Property	System.String HostId {get;}			
Id	Property	System.String Id {get;}			
MemoryMB	Property	System.Int32 MemoryMB {get;}	Ŧ		

Figure 94.

To find out more information about the object being returned by vSphere PowerCLI, use the **Get-Member** cmdlet to retrieve a list of all properties, and also methods attached to this virtual machine object.

To do this we will take the **Get-VM** cmdlet and "pipe" it through the **Get-Member** cmdlet. This will take the results of the **Get-VM** cmdlet and push them as an input into the **Get-Member** cmdlet.

Type Get-VM | Get-Member

As you can see from the preceding screenshot, the virtual machine object contains more properties than were shown from our initial **Get-VM** results.
🥙 [vSphere PowerCLI] Connec	cted to tm-pod0	1-vc01 as root		
PowerCLI C:\> Get-VM t-Table	Select N	ame, PowerState,	VMHost, NumCPU,	MemoryMB Forma _
Name	PowerState	VMHost	NumCpu	MemoryMB
UM_01 UM_07 UM_02 UM_03 UM_04 UM_05 UM_06 PowerCLI C:\>	PoweredOn PoweredOn PoweredOn PoweredOn PoweredOn PoweredOn PoweredOn	tm-pod01-esx tm-pod01-esx tm-pod01-esx tm-pod01-esx tm-pod01-esx tm-pod01-esx tm-pod01-esx	2 1 2 2 1 1 1 1	4096 4096 4096 1024 1024 1024

Figure 95.

To select properties that we would like to see, we can use the **Select-Object** cmdlet to choose the properties of the virtual machine we would like returned.

Type: Get-VM | Select Name, PowerState, VMHost, NumCPU, MemoryMB | Format-Table

This will retrieve the selected properties and show them in a table view in our console.

🕼 [vSphere	Power	CLI] Conne	cte	d to tm-pod01-vc01 as root	×
PowerCLI		Get-VM	ł	Export-CSU -NoTypeInformation C:\Export\AllUMs.csv	*
PowerCLI		Get-VM	ł	ConvertTo-Html Out-File C:\Export\AllUMs.htm	Ξ
PowerCLI PowerCLI PowerCLI	C:\> C:\> C:\>	Get-VM	:	Out-File C:\Export\AllUMs.txt	
					-

Figure 96.

This information can easily be exported from vSphere PowerCLI into many formats using some of the cmdlets built into the default PowerShell console.

To export the information into a comma-separated values file, type **Get-VM | Export-CSV -NoTypeInformation** C:\Export\AllVMs.csv

To export the information into a html file, type Get-VM | ConvertTo-Html | Out-File C:\Export\AllVMs.htm

To export the information into a plain text file, type Get-VM | Out-File C:\Export\AllVMs.txt

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root						
PowerCLI C:\> New-UM -Name UM_08 -ResourcePool (Get-UMHost tm-pod01-esx03*) -Dat astore (Get-DatastoreCluster "Datastore Cluster 01") -NumCPU 2 -MemoryMB 4096 -D iskMB 40000 -NetworkName Production02 -Floppy -CD -DiskStorageFormat Thin						
Name	PowerState Num CPUs	Memory (MB)				
VM_08	PoweredOff 2	4096				
PowerCLI C:\> _						
			-			

Figure 97.

To create a new virtual machine, the **New-VM** cmdlet can be used. This has many parameters that can be used to specify the exact configuration of the virtual machine. To view these parameters, use the **Get-Help** cmdlet.

We will create a virtual machine with the following configuration:

Name: VM_08 Host: tm-pod01-esx03 Datastore: Datastore Cluster 01 CPUs: 2 Memory: 4GB Disk: 40GB DiskType: Thin Network: Production02 Floppy Drive: Yes CD-Rom: Yes To do this, type the following:

New-VM -Name VM_08 -ResourcePool (Get-VMHost tm-pod01-esx03*) -Datastore (Get-DatastoreCluster "Datastore Cluster 01") -NumCPU 2 -MemoryMB 4096 -DiskMB 40000 -NetworkName Production02 -Floppy -CD -DiskStorageFormat Thin

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root					
PowerCLI C:\> 1020 -pod01-esx03*) -Data 2 -MemoryMB 4096 -Di eFormat Thin >	Foreach { New- store {Get-Datast skMB 40000 -Netwo	VM -Name U oreCluster orkName Pro	IM_\$ResourcePool ⟨Ge ^ "Datastore Cluster Øf oductionØ2 -Floppy -CD	t-VMHost tm "> -NumCPU -DiskStorag	
Name	PowerState Num C	PUs Memory	/ (MB)		
VM_10 VM_11 VM_12 VM_13 VM_15 VM_15 VM_16 VM_16 VM_17 VM_18 VM_19 VM_20 PowerCLI C:\>	PoweredOff 2 PoweredOff 2	4096 4096 4096 4096 4096 4096 4096 4096			

Figure 98.

The New-VM cmdlet can also be used to create any number of virtual machines with the same configuration.

The following example shows how to create 10 new virtual machines with the same configuration. In the following example, \$_ refers to the current number in the pipeline, because they are passed through to the **New-VM** cmdlet:

10..20 | Foreach { New-VM -Name VM_\$_ -ResourcePool (Get-VMHost tm-pod01-esx03*) -Datastore (Get-DatastoreCluster "Datastore Cluster 01") -NumCPU 2 -MemoryMB 4096 -DiskMB 40000 -NetworkName Production02 -Floppy -CD -DiskStorageFormat Thin }

🥙 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root				
PowerCLI C:>> (Get-ViCommand ¥VM	·		
CommandT ype	Name	Definition		
Cmdlet Cmdlet Cmdlet Cmdlet Cmdlet Cmdlet Cmdlet Cmdlet Cmdlet PowerCLI C:>>	Get-UM Move-UM New-UM Remove-UM Setart-UM Start-UM Start-UM Stop-UM Suspend-UM	Get-UM [[-Name] {String[]>] Move-UM [[-UM] {UirtualMachi New-UM [[-UMHost] {UIrtualMac Remove-UM [[-UM] {UirtualMac Restart-UM [[-UM] {UirtualMachin Set-UM [[-UM] {UirtualMachi Start-UM [[-UM] {UirtualMachi Stop-UM [[-UM] {VirtualMachi Suspend-UM [[-UM] {UirtualMa		

Figure 99.

Further virtual machine operations can be performed with vSphere PowerCLI. To see the cmdlets that can be used with virtual machines, type **Get-ViCommand *VM**

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root								
PowerCLI C:\> Get-UMHost								
Name	ConnectionState	PowerState	Id	CpuUsage Mhz	CpuTotal Mhz	Memory UsageMB	Memory Tota1MB	ш
tm-pod01-esx tm-pod01-esx tm-pod01-esx	Connected Connected Connected	PoweredOn PoweredOn PoweredOn	t-19 t-23 st-9	78 71 125	19144 19144 19144	9286 2685 3146	49084 49084 49084	
PowerCLI C:>>								

To find more information on one of these cmdlets, type Get-Help Move-VM -Full

Figure 100.

To list all hosts attached to the current connection, type Get-VMHost

😰 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root 📃 💷 💽				
PowerCLI C:\> Get-VM	Host tm-pod(01-esx02*	l Get-VM	A .
Name	PowerState	Num CPUs	Memory (MB)	=
VM_03 VM_01 VM_04	PoweredOn PoweredOn PoweredOn	2 2 1	4096 4096 1024	
PowerCLI C:>>				

Figure 101.

To list all virtual machines attached to a certain host, type Get-VMHost tm-pod01-esx02* | Get-VM

The preceding example will take the result of the **Get-VMHost** cmdlet and push it through as an input for the **Get-VM** cmdlet, producing a list of virtual machines on that specific host.



Figure 102.

The Get-VMHost cmdlet can be used in conjunction with other cmdlets to retrieve and set information for that host.

To list the NTP servers on each host in the vSphere Client, you would need to go to the host and clusters view, select a host, click the configuration tab and select the time configuration setting to view. You would need to repeat this for each host.

[vSphere PowerCLI] Connected to tm-pod01-vc01 as root					
PowerGLI G:NZ Get	-vn i Get-Snapsno)t		<u>^</u>	
Name	Description		PowerState		
pre tools update			PoweredOn		
PowerCLI C:\> Get ¦ Format-Table	;-VM Get-Snapsho	ot ¦ Select VM, N	ame, Description, (Created, SizeMB	
VM	Name	Description	Created	SizeMB	
VM_02	pre tools update		6/8/2011 9:50	4585.49	
PowerCLI C:\> _					

To do this in vSphere PowerCLI, type Get-VMHost | Get-VMHostNTPServer

Figure 103.

Snapshot information gathering is a time-consuming part of any virtual administrator's job. Snapshots need to be managed correctly or they can quickly cause issues within the virtual infrastructure. Within the vSphere Client, it is hard to get an overview of how many snapshots have been created and how much space they are using, when they were created, and by whom they were created.

vSphere PowerCLI includes multiple cmdlets to allow you to work with snapshots. To view all snapshots on the current connection, type **Get-VM | Get-Snapshot**

To gain more information about all snapshots, type Get-VM | Get-Snapshot | Select VM, Name, Description, Created, SizeMB | Format-Table

In addition to reporting, PowerCLIvSphere PowerCLI also provides cmdlets for the management of snapshots.

🕼 [vSphere PowerCLI] Connect	ted to tm-pod01-vc01 as root				
PowerCLI C:\> Get-UM tch added before appl	UM× ¦ New−Snapshot – ying all Microsoft]	-Name "Patch Tu Patches"	uesday" -Description '	'A Pa	
Name	Description	Pow	verState		
Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday Patch Tuesday	A Patch added beford A Patch added befor A Patch added befor	e applyi Pow e applyi Pow e applyi Pow e applyi Pow e applyi Pow e applyi Pow e applyi Pow	veredOff veredOff veredOff veredOff veredOff veredOff veredOff veredOff		Tasks & Events Alarms Pern
					ces
					age: 22 MHz
				-	rusage: 1670.00 MB
Recent Tasks					N
Name	Target 🛆	Status D	etails Initiated by vCe	enter Server	Requested Start Time
😵 Create virtual machine snapsł	hot 🗗 VM 01	Completed	root 🛃	tm-pod01	-vc01 6/19/2011 7:40:48 PM

Figure 104.

Snapshots are easily created in large numbers in vSphere PowerCLI. Snapshots in the vSphere Client must be created one at a time. With vSphere PowerCLI, you can specify the criteria for your virtual machines and use the **New-Snapshot** cmdlet to create a snapshot on each virtual machine. The following example shows how to create a snapshot on all virtual machines having names that start with VM:

Get-VM VM* | New-Snapshot -Name "Patch Tuesday" -Description "A Patch added before applying all Microsoft Patches"

You will also see from the preceding screen shot that any task produced by vSphere PowerCLI will be recorded in the normal manner within vCenter and attributed to the user who is connected to this vSphere PowerCLI session.

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root	
PowerCLI C:\> Get-UM Get-Snapshot -Name "Patch Tuesday" Remove-Snapshot	-
Confirm Are you sure you want to perform this action? Performing operation "Removing snapshot." on Target "VirtualMachineSnapshot=spapshot=65".	
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help <default "y"="" is="">:A PowerCLI C:>> _</default>	

Figure 105.

As with the creation of snapshots, it is very easy to remove them in large numbers with the **Remove-Snapshot** cmdlet. The following example will remove all snapshots with a name of "Patch Tuesday":

Get-Snapshot -Name "Patch Tuesday" | Remove-Snapshot

🕼 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root					
PowerCLI C:>>	Get-ViCommand *Snapshot*	·			
CommandT ype	Name	Definition			
Cmdlet Cmdlet Cmdlet Cmdlet PowerCLI C:\>	Get-Snapshot New-Snapshot Remove-Snapshot Set-Snapshot	Get-Snapshot [[-UM] <virtualma New-Snapshot [[-UM] <virtualma Remove-Snapshot [-Snapshot] <s Set-Snapshot [-Snapshot] <snap< th=""></snap<></s </virtualma </virtualma 			

Figure 106.

To list the available cmdlets for working with snapshots, type Get-ViCommand *Snapshot*

😰 [vSphere PowerCLI] Connected to tm-pod01-vc01 as root					
PowerCLI C:\> Get-VMHo lable	ost ¦ Get-VirtualSwit	ch ¦ Select VMHost, Name,	. Nic, NumPortsAvai		
UMUsst	Mama	N	Num Pauta Quadlahla		
	Name	N1C			
tm-pod01-esx02.tms tm-pod01-esx03.tms tm-pod01-esx01.tms	vSwitchØ vSwitchØ vSwitchØ	{vmnic1, vmnic0} {vmnic1, vmnic0} {vmnic1, vmnic0}	117 117 119		
PowerCLI C:>>					

Figure 107.

Networking is also a key area of your virtual infrastructure. vSphere PowerCLI has the ability to report, create, and configure all aspects of your networking configuration.

To list all virtual switches and their information, type Get-VMHost | Get-VirtualSwitch | Select VMHost, Name, Nic, NumPortsAvailable

[vSphere PowerCLI] Connect	ted to tm-pod01-vc01 as root	E	- • •
PowerCLI C:\> Get-UMH VMHost";Expression={\$ VMHost	ost ¦ Get-VirtualSwi VirtualSwitch.VMHo	tch ¦ Get-UirtualPortgroup ¦ Select st>>, VirtualSwitchName, Name, VLan	Q{Name="▲ Id ¦ Sort ≡
VMHost	VirtualSwitchName	Name	VLanId
<pre>tm-pod01-esx01.tms tm-pod01-esx01.tms tm-pod01-esx01.tms tm-pod01-esx01.tms tm-pod01-esx01.tms tm-pod01-esx02.tms tm-pod01-esx02.tms tm-pod01-esx02.tms tm-pod01-esx02.tms tm-pod01-esx02.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms tm-pod01-esx03.tms</pre>	vSwitch0 vSwitch0	Management Network HBR01 FT01 vMotion01 iSCSI01 Production02 FT01 Management Network Production02 iSCSI01 vMotion01 HBR01 Management Network Production02 FT01 iSCSI01 HBR01 vMotion01	2912 3005 3002 3004 3001 3003 2001 3004 3002 3004 3005 2912 3004 3005 3004 3005 3004

Figure 108.

vSphere PowerCLI reporting can also be used to ensure that your virtual configurations are correct. If a port group is missed, or the name is incorrect, or the VLANID has been set incorrectly, this can cause fundamental issues with clusters and the vSphere Distributed Resource Scheduler (DRS).

The preceding example shows how the configuration of each host, vSwitch, and port group can be checked. To perform this, type the following:

Get-VMHost | Get-VirtualSwitch | Get-VirtualPortgroup | Select @{Name="VMHost";Expression={\$_. VirtualSwitch.VMHost}}, VirtualSwitchName, Name, VLanId | Sort VMHost

[vSphere PowerCLI] Connected to a	tm-pod01-vc01 as root	- • •
PowerCLI C:\> Get-Cluster vSwitch0 ¦ New-VirtualPort	DemoCluster-01 Get-UMHost (tGroup "Company X" -VLanId 200	Get-VirtualSwitch -Name 🔽 🗐
Name	Кеу	VLanId PortBinding Num Por ts
Company X Company X Company X	key-vim.host.PortGroup-Comp key-vim.host.PortGroup-Comp key-vim.host.PortGroup-Comp	200 200 200
PowerCLI C:\>		

Figure 109.

It is easy to add port groups in large numbers using vSphere PowerCLI. This can be achieved on each host in a specific cluster to ensure the DRS and HA compatibility of the host. The following example will create a new port

group called "Company X" on vSwitch0 for each host in the cluster "DemoCluster-01":

Get-Cluster DemoCluster-01 | Get-VMHost | Get-VirtualSwitch -Name vSwitch0 | New-VirtualPortGroup "Company X" -VLanId 200

vSphere PowerCLI Summary

In conclusion, you can see that vSphere PowerCLI is a robust command-line tool for automating all aspects of vSphere management, including host, network, storage, virtual machine, and guest OS management. It can be used with other PowerShell snap-ins provided by Microsoft or third-party companies to integrate VMware technologies easily into other products and reach inside the guest OS.

The design of PowerShell and, inherently, vSphere PowerCLI, makes this scripting language easier to learn than many scripting languages before it. Complex configurations and reporting can be achieved with minimal effort from the administrator, safe in the knowledge of a repeatable, error-free solution.

Evaluating the ESXi Firewall

Introduction

The ESXi 5.0 management interface is protected by a service-oriented and stateless firewall, which you can configure using the vSphere Client or at the command line with esxcli interfaces. A new firewall engine eliminates the use of iptables, and rule sets define port rules for each service. For remote hosts, you can specify the IP addresses or range of IP addresses that are allowed to access each service.

Evaluation Overview

In this exercise, you will configure the ESXi firewall to allow or deny SSH service to the host. SSH is a service that can be enabled or stopped on an ESXi host. As part of this exercise, you will stop and start SSH service, and also configure firewall rules. ESXi firewall configuration can be done through the vSphere Client interface and through the vCLI. In this example environment, you will configure the firewall rules through vSphere Client UI.

Prerequisites

The evaluation environment consists of the following components:

- 1. Three ESXi hosts
- 2. Virtual machines running on hosts
- 3. Each virtual machine a software tool installed
 - a. PuTTY

Stopping SSH Service to Prevent Access

The SSH service provides a secure shell to manage the ESXi host. By default, this service is enabled. To stop this service, you have to follow these steps:

- 1. Select the Home > Inventory > Hosts and Clusters view.
- 2. Choose the host tm-pod01-esx01.tmsb.local in the left panel, and select Configuration tab on the right.
- 3. To see the firewall and services setting, select the **Security Profile** under the software section. Figure 110 shows the current Security Profile of the selected ESXi host. You can see that the SSH service is enabled and current firewall settings allow access to the SSH server on TCP port 22.



Figure 110.

4. The warning sign on the host tm-pod01-esx01.tmsb.local is regarding the SSH service. Figure 111 shows the summary screen with the warning displayed. Enabling SSH service could be a security risk, so the platform provides the warning. You have to make sure that firewall rules are configured when SSH service is enabled.



Figure 111.

5. To stop the service, you have to click the Services **Properties** link as shown in Figure 112.

🛃 tm-pod01-vc01 - vSphere Client						_ 🗆 ×
File Edit View Inventory Administration Pl	lug-ins Help					
🖸 🔝 🏠 Home 🕨 🛃 Inventory	Hosts and Clusters			🔊 🗸 Search Inve	ntory	Q
ब क स ल						
🖃 🛃 tm-pod01-vc01	tm-pod01-esx01.tmsb.local ¥Mware ES	iXi, 5.0.0, 413596				
DemoDatacenter-01	Getting Started Summary Virtual Mact	ines Performance Configura	tion Tasks & Events Alarms	Permissions Mans Sto	rage Views Hardware I	Stat 4 N
Impod01-esy01 tmsh local	Hardware	Security Profile		(rombions (ridps (see		
tm-pod01-esx02.tmsb.local		Services			Refresh Propertie	5
tm-pod01-esx03.tmsb.local	Processors	I/O Redirector (Active Dire	rtory Service)			_
👘 VM_01	Memory	Network Login Server (Acti	ve Directory Service)			
VM_02	Storage	lbtd				
WM_03	Networking	vSphere High Availability A	gent			
W1_04	Storage Adapters	vpxa				
M 06	Network Adapters	ESXI Shell	n Course (Astino Directory Course	.)		
👗 VM_07	Advanced Settings	NTP Deemon	SIT Server (Active Directory Service	5)		
~	Power Management	SSH				
	C 0	Direct Console UI				
	Sortware	CIM Server				
	Licensed Features	Firewall			Refresh Propertie	is
	Time Configuration	Incoming Connections				
	DNS and Routing	NFC	902 (TCP)	All		
	Authentication Services	vMotion CTM CLD	8000 (TCP) 437 (UDD TCD)	All		
	Power Management	CIM Server	427 (UDP, TCP)	All		
	Virtual Machine Startup/Shutdown	Eault Tolerance	8100.8200 (TCP, UDP)	All		
	Virtual Machine Swapfile Location	SSH Server	22 (TCP)	All		
	 Security Profile 	DHCP Client	68 (UDP)	All		
	Host Cache Configuration	DNS Client	53 (UDP)	All		
	System Recourse Allocation	vSphere Client	902,443 (TCP)	All		
	Agent VM Settings	vSphere Web Access	80 (TCP)	All		-
, Decent Techs	T Addit Wildettinds	CRIMD Carolar	News Te	nii		
Recent Tasks			Name, La	arget or Status contains: •		.ear 🔨
Name	Target		Status	Details Initiated by	vCenter Server	Requ
1						F
🖅 Tasks 💇 Alarms				License Peri	od: 101 days remaining	root //

Figure 112.

emote Access		
y default, remote clients are prev ccessing services on remote hosts	ented from access ,	ng services on this host, and local clients are prevented from
nless configured otherwise, daem	ons will start autor	natically.
Label	Daemon	
I/O Redirector (Active Directory S	e Stopped	
Network Login Server (Active Dire	Stopped	
NTP Daemon	Running	
vpxa	Running	
ocal Security Authentication Serv	Stopped	
ESXi Shell	Stopped	
btd	Running	
5SH	Running	
Direct Console UI	Running	
CIM Server	Running	
Service Properties		
Service Properties GeneralService:S	5H	
Service Properties General Service: S: Package Information: es	5H sx-base	
Service Properties General Service: S: Package Information: et 1	5H :x-base nis VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: e: Ti	5H sx-base nis VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: ex Ti	5H :x-base lis VIB contains all	of the base functionality of vSphere ESXi.
Service Properties General Service: Si Package Information: e: Ti	5H sx-base iis VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: e: Ti	5H sx-base lis VIB contains all	of the base functionality of vSphere ESXI.
Service Properties	5H sx-base lis VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: e: Ti	5H x-base his VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: ex Ti	5H x-base his VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: ex TI TI	5H x-base his VIB contains all	of the base functionality of vSphere ESXI.
Service Properties General Service: S: Package Information: e: Ti	5H tx-base tis VIB contains all	of the base functionality of vSphere ESXI.

6. This will bring up the panel shown in Figure 113. Select SSH and click **Options.** You can start or stop any services that are listed in this panel.

Figure 113.

🚱 SSH (SSH) Options 🛛 🗶
Status
Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with host Start and stop manually
Service Commands Start Stop Restart
OK Cancel Help

Figure 114.

7. Because this service was already started, you have an option to stop it by clicking Stop in the panel shown in Figure 114.

Testing Access with SSH Service Stopped

After stopping the SSH remote access service, you can test if any client can connect to Host1 (tm-pod01-esx01. tmsb.local) on TCP port 22.

In this example environment, you can use virtual machine VM_02 running on Host3 (tm-pod01-esx03.tmsb. local) to establish a SSH session with Host1. You can launch the PuTTY tool to establish the SSH session, as shown in Figure 115.

🞇 PuTTY Configuration		? ×
Category:		
 Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial 	Basic options for your PuTTY ses Specify the destination you want to connect Host Name (or IP address) [tm-pod01-esx01.tmsb.local Connection type: C Raw C Telnet C Rlogin C SSH Load, save or delete a stored session Saved Sessions Default Settings Close window on exit: C Always C Never C Only on cl	ssion to to Port 22 C Serial Load Save Delete ean exit
About Help	Open	Cancel
		Janoor

Figure 115.

The connection times out with a network error, as shown in Figure 116.



Figure 116.

This demonstrates that by shutting down the SSH service, you can completely deny remote access. Instead of blocking all access by stopping a service, you can selectively restrict remote access through the ESXi firewall. In the following section, you will enable the SSH service, and then use firewall settings to provide selective remote access.

Creating Firewall Rules to Block SSH Access

Before creating the firewall rules to block SSH access, you have to first enable the SSH service as follows:

- 1. Click the Services Properties link, as shown in Figure 112.
- 2. Select SSH service in the Service Properties panel, as shown in Figure 117. You can see that the SSH service is stopped. To enable the service, click **Options.**

temote Access ty default, remote clients are prevent accessing services on remote hosts. Inless configured otherwise, daemone Label I/O Redirector (Active Directory Se Network Login Server (Active Directory Se NTP Daemon NTP Daemon NTA Decal Security Authentication Serv ESXI Shell Ibid	ted from accessing services on this host, and local clients are prevented from s will start automatically. Daemon . Stopped . Running . Stopped . Stopped . Stopped . Stopped . Stopped . Stopped .
y default, remote clients are prevent ccessing services on remote hosts. Inless configured otherwise, daemon: Label L/O Redirector (Active Directory Se VITP Daemon VpXa Local Security Authentication Serv ESXI Shell btd	ted from accessing services on this host, and local clients are prevented from s will start automatically. Daemon
nless configured otherwise, daemon: .abel //O Redirector (Active Directory Se Vetwork Login Server (Active Direc TIP Daemon /pXa .ccal Security Authentication Serv :SXi Shell btd	s will start automatically. Daemon Stopped Running Running Stopped Stopped
Label (/O Redirector (Active Directory Se Network Login Server (Active Direc UTP Daemon rpxa 	Daemon Stopped Running Running Stopped Stopped
Label (/O Redirector (Active Directory Se Network Login Server (Active Direc NTP Daemon vpxa Local Security Authentication Serv ESXI Shell btd	Daemon Stopped Running Running Stopped Stopped
Label (/O Redirector (Active Directory Se Vetwork Login Server (Active Direc VTP Daemon vpxa cal Security Authentication Serv ESXi Shell btd	Daemon Stopped Running Running Stopped Stopped
I/O Redirector (Active Directory Se Network Login Server (Active Direc NTP Daemon vpxa cal Security Authentication Serv ESXi Shell btd	. Stopped . Stopped Running Running Stopped Stopped
Network Login Server (Active Direc NTP Deemon vpxa iocal Security Authentication Serv ESXi Shell btd	. Stopped Running Running Stopped Stopped
NTP Daemon vpxa Local Security Authentication Serv ESXI Shell btd	Running Running Stopped Stopped
vpxa Local Security Authentication Serv ESXi Shell Ibtd	Running Stopped Stopped
Local Security Authentication Serv ESXi Shell Ibtd	Stopped Stopped
ESXi Shell Ibtd	Stopped
lbtd	
ccu	Running
55H	Stopped
Direct Console UI	Running
CIM Server	Running
Service Properties	
Service: SSH	
Package Information: esx-	base
This	VIB contains all of the base functionality of vSphere ESXi.
	Options
	OK Cancel Hel

Figure 117.

🔁 SSH (SSH) Options 🛛 🗙
Status
Startup Policy Start automatically if any ports are open, and stop when all ports are closed Start and stop with bost
Start and stop with host Start and stop manually
Service Commands Start Stop Restart
OK Cancel Help

Figure 118.

- 3. Click **Start** in the SSH Options panel, as shown in Figure 118. This will start the SSH service again. You can now configure the firewall rules for this service.
- 4. Click firewall **Properties** to access the firewall setup panel. Figure 119 shows the firewall Properties.

🛃 tm-pod01-vc01 - vSphere Client							×
File Edit View Inventory Administration P	lug-ins Help						
💽 💽 🏠 Home 🕨 🛃 Inventory	Hosts and Clusters			😴 🗸 Search	Inventory		Q
a @ # Q							
tm-pod01-vc01 DemoDatacenter-01 DemoDatacenter-01 m-pod01-esx01.tmsb.local m-pod01-esx02.tmsb.local m-pod01-esx02.tms	tm-pod01-esx01.tmsb.local VMware E5 Getting Started Summary Virtual Mac Hardware Processors	SXI, S.O.O, 413596 hines Performance Configure Security Profile Security Profile	Tasks & Events Alarms	Permissions Maps	Storage Views	Hardware Stat 4	
Wh_01 Wh_02 Wh_02 Wh_03 Wh_04 Wh_05 Wh_06 W	Memory Storage Networking Storage Adapters Network Adapters Advanced Settings Power Management	I/O Redirector (Active Dir Network Login Server (Ac Ibtd vSphere High Availability, vpxa ESW Shell Local Security Authentical NTP Daemon SSH	ectory service) tive Directory Service) Agent ion Server (Active Directory Servi	ce)			
	Software	Direct Console UI CIM Server			Defrech	Properties	
	Licensed reatures Time Configuration DIS and Routing Authentication Services Power Management Virtual Machine Sarup/Shutdown Virtual Machine Swapfile Location • Security Profile Host Cache Configuration System Resource Allocation Agent VM Settings	Incoming Connections DNS Client vSphere Client vMotion CIM Secure Server DHCP Client CIM SLP SSM Server NFC Fault Tolerance SMP Server vSohara Wah Ancare	53 (UDP) 902,443 (TCP) 8000 (TCP) 5889 (TCP) 68 (UDP) 427 (UDP,TCP) 22 (TCP) 902 (TCP) 8100,8200 (TCP,UDP) 161 (UDP) 80 (TCP)	Al Al Al Al Al Al Al Al Al Al	Refresti	properties	
Recent Tasks			Name, 1	arget or Status contains: 👻		Clear	×
Name Update service activation policy Start service	Target	sx01.tmsb.local sx01.tmsb.local	Status Completed Completed	Details Initiated root root	Period: 101 days n	erver R od01-vc01 6 vod01-vc01 6 emaining root	8 ▲ 5) 5) ▼

Figure 119.

emote A	Access					
/ default, ccessing s	remote clients are pr services on remote ho	revented from accessing service osts.	es on this host, and local clier	nts are prevente	ed from	
elect a ch	eck box to provide ad	ccess to a service or client. Dae	mons will start automatically (when their ports	; are	
pened and	d stop when all of the	air ports are closed, or as config	ured.			
						_
Labe	•	Incoming Ports	Outgoing Ports	Protocols	Daemon	-
lequired le	Services					
jecure S	hell					
SSH	Server	22		TCP	Running .	_
SSH	Client		22	TCP	N/A	
Simple Ne	etwork Manageme	ent Protocol				
Ingroup	ed					
	Client	53	53	UDP	N/A	
YMW	are vCenter Agent		902	UDP	Running	
NTP	Client		123	UDP	Running	
 Fault 	t Tolerance	8100,8200	80,8100,8200	TCP,UDP	N/A	-
<u>را</u>) •	
Service Pi	roperties					
General						
Service	:	SSH Server				
Package	e Information:	esx-base This VIB contains all of the bas	se functionality of vSphere E	SXI.		
Firewall	Settings					
	IP Addresses:	All				
Allowed						
Allowed						
Allowed						
Allowed				Firewall	Options	

Figure 120.

- 5. After clicking the firewall Properties link, you will see the Firewall Properties panel, as shown in Figure 120. Select the SSH Server under the Secure Shell category, and click **Firewall**.
- 6. In this example environment, you have to enable the SSH remote access only from virtual machine VM_02 with IP address 10.91.35.55. SSH connections from all other IP addresses are denied. You can also give a range of IP addresses or subnet class in the "Only allow connections..." field shown in Figure 121.

🛃 Firewall Settings 🛛 🛛 🗙
Allowed IP Addresses
Allow connections from any IP address
Only allow connections from the following networks:
10.91.35.55
Separate each network with a comma. Example: 192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64
OK Cancel Help

Figure 121.

After configuring the firewall rule to allow remote access for only virtual machine VM_02, you can test this firewall setting by establishing PuTTY sessions from different virtual machines.

Testing SSH Firewall Rules

In this example environment, you will try to establish SSH sessions from the following two virtual machines that are running from Host3 (tm-pod01-esx03.tmsb.local):

- 1. VM_02 : With IP address 10.91.35.55
- 2. VM_04 : With IP address 10.91.35.67

First, you can try creating a SSH session using the PuTTY tool on VM_02. This virtual machine IP address is one of the allowed IP addresses in the firewall configuration. Therefore, you can expect the SSH connection to be established.

RuTTY Configuration		? ×
Category:		
Session Logging Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Colours Connection Data Proxy Telnet Rlogin SSH	Basic options for your PuTTY s Specify the destination you want to conn Host Name (or IP address) Im-pod01-esx01.tmsb.local Connection type: C Raw C Telnet C Rlogin S Load, save or delete a stored session Saved Sessions Default Settings	ession ect to Port 22 GH C Serial Load Save Delete
Serial	Close window on exit: C Always C Never • Only on	clean exit
About Help	Open	Cancel

Figure 122.

Figure 123 shows the login screen of Host1. You can log in to the host with root credentials.



Figure 123.

When you repeat the step of establishing the SSH connection from VM_04 (10.91.35.67), you will get the "Network error: Connection timed out" message as shown in Figure 124. This is because the ESXi firewall blocks access on TCP port 22 from any IP address other than 10.91.35.55.



Figure 124.

Image Builder

Introduction

In this section, you will learn how to use vSphere 5.0 Image Builder to create and maintain custom ESXi images used to deploy hosts in your vSphere 5.0 environment. A past challenge with ESXi has been the static nature of the vSphere installation image. As customers adopt new hardware and as vendors release updates to CIM providers and software drivers, it was difficult to incorporate these updates into the ESXi installation. Image Builder enables users to update and maintain their ESXi images in order to keep up with the latest software drivers and updates.



Figure 125. Image Builder Overview

Image Builder can be used in conjunction with VWmare vSphere® Auto Deploy to dynamically provision hosts in a diskless environment.

Image Builder Prerequisites

The following components are required to use vSphere 5.0 Image Builder:

- Windows VM with 2GB of free disk space (used to host vSphere PowerCLI and store Image Builder software depots)
- vSphere PowerCLI 5.0
- ESXi Offline Bundle
- vCenter Server 5.0

Preparation Tasks

Complete the following steps prior to beginning your evaluation of Image Builder 5.0:

Install vSphere PowerCLI

Download and install vSphere 5.0 PowerCLI from www.vmware.com. The download file is a self-extracting executable file. Simply double-click on the .exe file to invoke the vSphere PowerCLI installer and follow the prompts. Refer to the vSphere PowerCLI User's Guide and the "vSphere PowerCLI by Example" section of this guide for more information on installing vSphere PowerCLI.

Download the ESXi Offline Bundle

Download the ESXi Offline Bundle ZIP file from www.vmware.com. The offline bundle is shipped in a ZIP format. Download the file on the same server where vSphere PowerCLI was installed.

Extract the ESXi Offline Bundle

Create the C:\ImageBuilder directory and extract the contents of the offline bundle into this directory.

Start an Image Builder vSphere PowerCLI Session

The following steps show how to start a vSphere PowerCLI session and how to connect to a vCenter Server.

Start vSphere PowerCLI by either double-clicking the vSphere PowerCLI icon on the desktop or selecting:

"Start -> Program -> VMware vSphere PowerCLI -> VMware vSphere PowerCLI"

From the vSphere PowerCLI prompt, run the "Connect-VIServer" cmdlet to connect your vSphere PowerCLI session to vCenter Server:

PowerCLI C:\> Connect-VIServer <vCenter IP address>

같 [,] [vSphere PowerCLI] Not Connected	_ 🗆 ×
Welcome to the UMware vSphere PowerCLI!	_
Log in to a vCenter Server or ESX host: To find out what commands are available, type: To show searchable help for all PowerCLI commands: Once you've connected, display all virtual machines: If you need more help, visit the PowerCLI community: Get-PowerCLICommunity	
Copyright (C) 1998-2011 UMware, Inc. All rights reserved.	
PowerCLI C:\Program Files (x86)\UMware\Infrastructure\vSphere PowerCLI> cd ` PowerCLI C:\> Connect-UIServer 10.91.243.185_	

Figure 126. Connect-VIServer

🚱 [vSphere PowerCLI] Not Co	nnected				_ 🗆 🗙
Welcome to t	the UMware vSpl	here PowerCLI!			_
Log in to a vCenter So To find out what comm To show searchable he Once you've connected If you need more help Copyright (C)	specify Credential			JIServer nmand •CLIHelp •CLICommunity •d.	
PowerCLI C:\Program F	Please specify server	credential		PowerCLI> cd >	
	User name: Password:		V <u>pr</u>		
		ОК	Cancel		-

Depending on your login credentials, you might be prompted to enter the vCenter user name and password, as follows:

Figure 127. Connect-VIServer Login Prompt

vSphere PowerCLI will show the vCenter Server name/IP and the port and user. During the Image Builder evaluation, the certificate error can be ignored.

🖉 [vSphere PowerCLI] Connected to 10.91.	.243.185	as root		_ 🗆 🗡
Log in to a vCenter Server or H To find out what commands are a To show searchable help for all Once you've connected, display If you need more help, visit th Copyright (C) 1998-2011	ESX hos availa) l Power all vi ne Powe VMware	st: ble, type: *CLI commands: irtual machines: erCLI community: e, Inc. All right	Connect-UIServer Get-UICommand Get-PowerCLIHelp Get-UM Get-PowerCLICommunity ts reserved.	
PowerCLI C:\Program Files (x86) PowerCLI C:\> Connect-VIServer WARNING: There were one or more	VMwai 10.91. probl	re\Infrastructure .243.185 lems with the se	exuSphere PowerCLI> cd ' rver certificate:	
* A certification chain process certificate which isn't trusted	ed com l by tl	rrectly, but terr he trust provider	ninated in a root *-	
* The certificate's CN name doe	es not	match the passed	l value.	
Name	Port	User		
10.91.243.185	443	root		
PowerCLI C:\>				

Figure 128. Connect-VIServer Results

Import the ESXi Offline Bundle

This section shows how to import an ESXi software depot using the ESXi offline depot staged in the C:\ ImageBuilder directory during the preparation tasks.

PowerCLI C:\> Add-EsxSoftwareDepot C:\ImageBuilder

🚰 [vSphere PowerCLI]	Connected t	to 10.91	.243.18	5 as root		_ 🗆 🗵
PowerCLI C:\> cd PowerCLI C:\]mag Directory: C	.∖ImageB eBuilder> :\ImageBu	uilden dir ilder	•			
Mode	LastW	riteT	ime	Length	Name	
d 5/3 -a 3/3 -a 3/3 -a 3/3	 31/2011 18/2011 18/2011 18/2011	5:15 5:32 5:32 5:32	PM PM PM PM	319 416 75172	 vib20 index.xml vendor-index.xml vmw-ESXi-5.0.0-metadata.zip	
PowerCLI C:\Image	eBuilder>	Add-I	EsxSo	ftwareDepo	ot C:\ImageBuilder	
Depot Url						
file:///C:/Image PowerCLI C:\Image	Builder∕i eBuilder≻	ndex.>	(ml			•

Figure 129. Add Software Depot

The software depot is a collection of vSphere packages used to create and maintain ESXi images. The following steps show how to view information about the software depots added to your vSphere PowerCLI session.

Display Software Depots

Software depots are added using the **Add-ESXSoftwareDepot** cmdlet and removed using the **Remove-SoftwareDepot** cmdlet. Use the **\$DefaultSoftwareDepots** variable to view the list of software depots available in your current vSphere PowerCLI session.

To view available software depots, type the following:

PowerCLI C: > \$DefautSoftwareDepots



Figure 130. Display Software Depot

Display VIBs

A vSphere Installation Bundle (VIB) is a packaging format used in vSphere. VMware and its partners package solutions, drivers, CIM providers and applications as VIBs. VIBs are then grouped together to create ESXi image profiles. To view the available VIBs from the software depots added to your vSphere PowerCLI session, use the **Get-EsxSoftwarePackage** cmdlet.

PowerCLI C:\> Get-EsxSoftwarePackage

🖉 [vSphere PowerCLI] Coni	nected to 10.91.243.185 as root		
PowerCLI C:∖ImageBui	▲		
Name	Version	Vendor	Release Date
 net-s2io ata-pata-atiixp tools-light sata-sata-svw scsi-gla4xxx net-r8168 scsi-aic79xx ata-pata-sil680 esy-thoot	2.1.4.13427-3umw.0.0.381646 0.4.6-3umw.0.0.381646 5.0.0-0.0.381646 5.01.03.2-2umw.0.0.381646 8.013.00-3umw.0.0.381646 3.1-4umw.0.0.381646 0.4.8-3umw.0.0.381646 5.0.0-0.381646	UMware UMware UMware UMware UMware UMware UMware UMware UMware	3/19/2011 3/19/2011 3/19/2011 3/19/2011 3/19/2011 3/19/2011 3/19/2011 3/19/2011 3/19/2011

Figure 131. Get-EsxSoftwarePackage

Display Image Profiles

An image profile is a compilation of VIBs that make up an ESXi image that can be used to install an ESXi host. At a minimum, an image profile is comprised of a base ESXi VIB and a bootable kernel module VIB, but can also include additional VIBs from the pool of available software depots. To list the configured image profiles, use the **Get-EsxImageProfile** cmdlet.

PowerCLI C:\> Get-EsxImageProfile

🖉 [vSphere PowerCLI] Connected to 10.91	.243.185 as root		_ 🗆 🗙
PowerCLI C:\ImageBuilder> Get-	EsxImageProfile		▲
Name	Vendor	Last Modified	Acceptance Level
ESXi-5.0.0-381646-no-tools ESXi-5.0.0-381646-standard	UMware, Inc. UMware, Inc.	3/19/2011 12 3/19/2011 12	PartnerSupported PartnerSupported
PowerCLI C:\ImageBuilder> _			

Figure 132. Get-EsxImageProfile

To list the VIBs that comprise an image profile, use the **Get-EsxImageProfile** cmdlet and expand the properties of the **VibList** property.

PowerCLI C:\> Get-EsxImageProfile MyProfile | Select -ExpandProperty VibList

🚰 [vSphere PowerCLI] Connected to vs-vcenter18 as VMWORLD\administrator 📃 🗖 🗙					
PowerCLI C:\> Get-EsxImageProfile MyProfile Select -ExpandProperty VibList 🗾 🔺					
Name	Version	Vendor	Release Date		
net-cnic	1.10.2j.v50.7-2vmw.500.0.0	VMware	7/3/2011		
net-e1000e	1.1.2-3vmw.500.0.0.441354	UMware	7/3/2011		
scsi-fnic	1.5.0.3-1vmw.500.0.0.441354	VMware	7/3/2011		
net-e1000	8.0.3.1-2vmw.500.0.0.441354	VMware	7/3/2011		
net-bnx2	2.0.15g.v50.11-5vmw.500.0.0	VMware	7/3/2011		
net-enic	1.4.2.15a-1vmw.500.0.0.441354	VMware	7/3/2011		
scsi-adp94xx	1.0.8.12-6vmw.500.0.0.441354	VMware	7/3/2011		
esx-tboot	5.0.0-0.0.441354	VMware	7/3/2011		
scsi-bnx2i	1.9.1d.v50.1-3vmw.500.0.0.4	VMware	7/3/2011		
scsi-qla4xxx	5.01.03.2-3vmw.500.0.0.441354	VMware	7/3/2011		
sata-sata-svw	2.3-3vmw.500.0.0.441354	VMware	7/3/2011		
net-tg3	3.110h.v50.4-4vmw.500.0.0.4	VMware	7/3/2011		
sata-sata-nv	3.5-3vmw.500.0.0.441354	VMware	7/3/2011		
uhci-usb-uhci	1.0-3vmw.500.0.0.441354	VMware	7/3/2011		
ata-pata-sil680	0.4.8-3vmw.500.0.0.441354	VMware	7/3/2011		
ehci-ehci-hcd	1.0-3vmw.500.0.0.441354	VMware	7/3/2011		
ata-pata-pdc2027x	1.0-3vmw.500.0.0.441354	VMware	7/3/2011		
ipmi-ipmi-si-drv	39.1-4vmw.500.0.0.441354	VMware	7/3/2011		
scsi-megaraid2	2.00.4-9vmw.500.0.0.441354	UMware	7/3/2011		
net-forcedeth	0.61-2vmw.500.0.0.441354	VMware	7/3/2011		
net-s2io	2.1.4.13427-3vmw.500.0.0.44	VMware	7/3/2011 💌		

Figure 133. Get-EsxImageProfile VibList

Create a New Image Profile

The following steps show how to create a custom image profile either by manually selecting the individual VIB components or by cloning an existing image profile.

Each image profile must meet the following requirements:

- The image profile must have a unique name.
- The image profile must contain at least one base ESXi VIB and one bootable kernel module.
- The acceptance level for each VIB must match the acceptance level defined for the profile.
- A VIB can only exist once in an image profile.
- All VIB dependencies must be met.

Create a New Image Profile by Manually Selecting Individual VIBs

Create a new image profile named "MyNewProfile" that contains the ESXi base image.

PowerCLI C:\> New-EsxImageProfile -NewProfile "MyNewProfile" -vendor "VMware" -SoftwarePackage esx-base

🖉 [vSphere PowerCLI] Connected t	o 10.91.243.185 a s root	:	
PowerCLI C:\ImageBuilder≻ "VMware" -SoftwarePackage	New-EsxImageProf e esx-base	file -NewProfile "MyNo	ewProfile" -vendor
Name	Vendor	Last Modified	Acceptance Level
MyNewProfile	VMware	6/13/2011 1:	VMwareCertified
PowerCLI C:\ImageBuilder>	-		

Figure 134. New-EsxImageProfile

Next, add the VIB "esx-tboot" to "MyNewProfile" as follows:

PowerCLI C:\> Add-EsxSoftwarePackage -ImageProfile "MyNewProfile" -SoftwarePackage "esx-tboot"

🖉 [vSphere PowerCLI] Connect	ted to 10.91.243.185 as root		_ 🗆 🗙
PowerCLI C:\ImageBuild oftwarePackage "esx-tb	er> Add-EsxSoftwareP oot"	ackage -ImageProfile	"MyNewProfile" -S
Name	Vendor	Last Modified	Acceptance Level
MyNewProfile	UMware	6/13/2011 1:	UM wareCertified

Figure 135. Add-EsxSoftwarePackage esx-tboot

Next, add the VIB "net-e1000e" to "MyNewProfile" as follows:

PowerCLI C:\> Add-EsxSoftwarePackage -ImageProfile "MyNewProfile" -SoftwarePackage "net-e1000e"

🚰 [vSphere PowerCLI] Connect	ed to 10.91.243.185 as root		
PowerCLI C:\ImageBuilde oftwarePackage "net-e10	er> Add-EsxSoftwareP 100e''	ackage -ImageProfile	"MyNewProfile" -S▲
Name	Vendor	Last Modified	Acceptance Level
MyNewProfile	VMware	6/13/2011 1:	VMwareCertified
PowerCLI C:\ImageBuilde	_ <49		

Figure 136. Add-EsxSoftwarePackage net-e1000e

Next, display the available image profiles and confirm that the new image profile "**MyNewProfile**" has been created:

🚰 [vSphere PowerCLI] Connected to 10.	91.243.185 as root		_ 🗆 ×
PowerCLI C:\ImageBuilder> Get	-EsxImageProfile		
Name	Vendor	Last Modified	Acceptance Level
 ESXi-5.0.0-381646-no-tools MyNewProfile ESXi-5.0.0-381646-standard	UMware, Inc. UMware UMware, Inc.	3/19/2011 12 6/13/2011 8: 3/19/2011 12	PartnerSupported UMwareCertified PartnerSupported
PowerCLI C:\ImageBuilder> _			

Figure 137. Get-EsxImageProfile with MyNewProfile

Next, display the list of VIBs in the image profiles to confirm that only the VIBs identified are included:

🖉 [vSphere PowerCl	I] Connected to vs-vcenter18 as VMWORLD\administra	tor	
PowerCLI C:>> G	et-EsxImageProfile MyNewProfile Selec	t -ExpandP	roperty VibList 🔼
Name	Version	Vendor	Release Date
esx-base net-e1000e esx-tboot misc-drivers	5.0.0-0.0.441354 1.1.2-3vmw.500.0.0.441354 5.0.0-0.0.441354 5.0.0-0.0.441354	UMware UMware UMware UMware	7/3/2011 7/3/2011 7/3/2011 7/3/2011 7/3/2011
PowerCLI C:>>			

Figure 138. Get-EsxImageProfile MyNewProfile VibList

Create a New Image Profile by Cloning an Existing Image Profile

Create a new ESXi image named "**MyClonedProfile**" by cloning the **ESXi-5.0.0-381646-standard Image** included with the offline bundle.

PowerCLI C:\> New-EsxImageProfile -CloneProfile ESXi-5.0.0-381646-standard -Name
"MyClonedProfile"

🔄 🛛 🗢								
PowerCLI C:\ImageBuilder> Ne andard -Name "MyClonedProfil	w-EsxImageProfile e''	-CloneProfile ES	Xi-5.0.0-381646-st					
Name	Vendor	Last Modified	Acceptance Level					
MyClonedProfile	 VMware, Inc.	3/19/2011 12	PartnerSupported					
PowerCLI C:\ImageBuilder> _								

Figure 139. New-EsxImageProfile -CloneProfile

Display the list of available image profiles confirming that the new profile was created:

PowerCLI C:\> Get-EsxImageProfile

🖾 [vSphere PowerCLI] Connected to 10.91.243.185 as root								
PowerCLI C:\ImageBuilder> Get-EsxImageProfile								
Name	Vendor	Last Modified	Acceptance Level					
 ESXi-5.0.0-381646-no-tools MyNewProfile ESXi-5.0.0-381646-standard MyClonedProfile	UMware, Inc. UMware UMware, Inc. UMware, Inc.	3/19/2011 12 6/13/2011 8: 3/19/2011 12 3/19/2011 12	PartnerSupported UMwareCert if ied PartnerSupported PartnerSupported					
PowerCLI C:\ImageBuilder> _								

Figure 140. Get-EsxImageProfile with MyClonedProfile

Removing VIBs from an Image Profile

The cloned image profile "MyCloneProfile" includes the VMware Tools package. We can make the size of this image profile smaller by removing the VMware Tools package.

PowerCLI C:\> Remove-EsxSoftwarePackage -ImageProfile MyClonedProfile -SoftwarePackage tools-light

🚰 [vSphere PowerCLI] Connected to 10.91.243.185 as root 📃 🖂 🗙							
PowerCLI C:\ImageBuilder> Rem e -SoftwarePackage tools-lig}	nove-EsxSoftwareF nt	Package -ImageProf	ile MyClonedProfil				
Name	Vendor	Last Modified	Acceptance Level				
MyClonedProfile	VMware, Inc.	6/13/2011 3:	PartnerSupported				
PowerCLI C:\ImageBuilder> _							

Figure 141. Remove-EsxSoftwarePackage

Compare Image Profiles

This section shows how to compare image profiles to help identify and track differences between custom image profiles.

In the previous section, we created a clone of the default image profile called "MyCloneProfile". We then removed the VMware Tools package from the custom image. We can now use the Compare-**EsxImageProfile** cmdlet to compare the two images and verify the changes that were made.

PowerCLI C:\> Compare-EsxImageProfile -ReferenceProfile Esxi-5.0.0-381646-no-tools -CompareProfile MyClonedProfile

🖉 [vSphere PowerCLI] Connected to 10.91.243.185 as root 📃 🗖 🗙						
PowerCLI C:\ImageBuilder> Compare-EsxImageProfile -ReferenceProfile ESXi-5.0.0-3 81646-standard -ComparisonProfile MyClonedProfile						
Equal PackagesEqual RefAcceptanceLevel CompAcceptanceLevel OnlyInRef OnlyInComp UpgradeFromRef DowngradeFromRef	: False : False : PartnerSupported : PartnerSupported : {UMware_locker_tools-light_5.0.0-0.0.381646} : {} : {} : {}					
PowerCLI C:\ImageBuilder>						

Figure 142. Compare-EsxImageProfile

In the preceding example, we can see that the package **VMware** _ **locker** _ **tools**light 5.0.0.0-0.0.381646 does not exist in the reference profile (-ReferenceProfile) but does exist in the comparison profile (-Comparison Profile).

Export Image Profile

The following steps show how to export image profiles as an offline bundle or as a bootable ISO image.

Export As an Offline Bundle

Each time you exit your vSphere PowerCLI session, all software depots and custom image profiles are lost. To save your custom image profiles, in order to continue to work with them between vSphere PowerCLI sessions, you must save them to disk by exporting to an offline bundle. With an offline bundle, each time you start a new vSphere PowerCLI session, you can continue to work with your custom image profiles by importing the offline bundle as a new software depot using the Add-EsxSoftwareDepot cmdlet.

To export an image profile as an offline bundle, use the **Export-EsxImageProfile** cmdlet with the -ExportToBundle option.

PowerCLI C:\> Export-EsxImageProfile -ImageProfile MyNewProfile -ExportToBundle -FilePath C:\ImageBuilder\MyNewProfile

[vSphere PowerCLI] Connected to 10.91.243.185 as root



Figure 143. Export-EsxImageProfile -ExportToBundle

Export As a Bootable ISO Image

In order to use a custom image profile to install ESXi hosts, you must export the image profile as a bootable ISO. Use the **Export-EsxImageProfile** cmdlet with the **-ExportToIso** option.

PowerCLI C:\> Export-EsxImageProfile -ImageProfile MyNewProfile -ExportToIso - FilePath C:\ImageBuilder\MyNewProfile.iso



Figure 144. Export-EsxImageProfile -ExportTolso

Use Windows Explorer to view the ZIP and .iso files.

🗁 Z:\ImageBuilder							
File Edit View Favorites Iools Help							
🚱 Back 🝷 🕤 👻 🥬 Sea	arch [>> Folders 🛛 🛄 ▾					
Address 🛅 Z:\ImageBuilder						• 🔁 💿	
		Name 🔺	Size	Туре	Date Modified	Attributes	
File and Folder Tasks	*	MyNewProfile.iso	143,254 KB	ISO File	6/13/2011 3:54 PM	A	
💋 Make a new folder 🍓 Publish this folder to the Web		🚹 MyNewProfile.zip	133,640 KB	Compressed (zippe	6/13/2011 3:59 PM	A	
Other Places	*						
 share01 on 'OpenFiler01 (10.91.244.133)'(2:) My Documents My Computer My Network Places 							

Figure 145. Show Image Profile Exports

Product Documentation

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

Using Storage Performance Statistics

Introduction

vSphere 5.0 introduces several new performance views. These views allow for a quick overview of the current health of your datastores. There are two different types of views: performance and space.

This next section will display how easy datastore monitoring is with vSphere 5.0. There are two basic views as part of the **Datastores and Datastore Clusters** view:

Monitoring Space Utilization of a Datastore

1. Go to the Datastores and Datastore Clusters view.

🛃 tm-pod01-vc0	1 - vSphere Client								
File Edit View 1	File Edit View Inventory Administration Plug-ins Help								
🖸 🖸 🛕	Home								
Inventory				_					
Q	P	Ð							
Search	Hosts and Clusters	VMs and Templates	Datastores and Datastore Clusters	Networking					
Administration									
6	×			? >	-		¥,		
Roles	Sessions	Licensing	System Logs	vCenter Server Settings	vCenter Solutions Manager	Storage Providers	vCenter Service Status	Auto Deploy	
Management									
2		1		R	-				
Scheduled Tasks	Events	Maps	Host Profiles	VM Storage Profiles	Customization Specifications				

Figure 146.

2. Select a datastore.

🔁 tm-pod01-vc01 - vSphere Client							
File Edit View Inventory Administration Plug-ins Help							
😧 🔝 🏠 Home 🕨 👸 Inventory 🕨 🤤 Datastores and Datastore Clusters							
tm-pod01-vc01 DemoDatacenter-01 TM-Gobal-Interchange01	tm-pod01-sas600-sp-01 Summary Virtual Machines Hosts Performance Configu	ration Tasks & Events Alarms Permissions Storage Views					
TM-POD01-ESX01-Local	General	Capacity					
TM-PODI-E5X03-Local tm-pod01-sas300-sp tm-pod01-sas300-sp-01 tm-pod01-sas600-sp-02	Location: ds:///vmfs/volumes/4d884a01-73289 Type: VMFS Number of Hosts Connected: 3 Virtual Machines and Templates: 2	Refresh Capacity: 99.75 GB Provisioned Space: 54.06 GB Free Space: 59.70 GB Last updated on: 6/3/2011 11:04:40 AM Storage Capabilities 50.000					
	Commands Commands Refresh Enter SDRS Maintenance Mode Browse Datastore Assign User-Defined Storage Capability	Refresh System Storage Capability: N/A User-defined Storage Capability: N/A					

Figure 147.



3. Click on the **Performance** tab. This will show you the current Space Utilization statistics for this particular datastore by default.

Figure 148.

4. Click on **Time Range** to change the range from 1 Day to **1 Week**. This will show if virtual machines have grown or have been migrated to other datastores, and any other trends over the last seven days.



Figure 149.

Monitoring Performance Statistics of a Datastore

The second part of this exercise shows the performance statistics available on the **Datastores and Datastore Clusters** view. These views are showing the most relevant and important metrics to monitor, like **Average Device Latency** 8**Average Write Latency per Virtual Machine Disk.**

1. Go to the Datastores and Datastore Clusters view.

🛃 tm-pod01-vc01	- vSphere Client								
File Edit View In	nventory Administratio	n Plug-ins Help	0						
🖸 🖸 🛕	Home								
Inventory				_					
Q	F	Ð		<u></u>					
Search	Hosts and Clusters	VMs and Templates	Datastores and Datastore Clusters	Networking					
Administration									
6	2	8		₽			V2		
Roles	Sessions	Licensing	System Logs	vCenter Server Settings	vCenter Solutions Manager	Storage Providers	vCenter Service Status	Auto Deploy	
Management									
Scheduled Tasks	Events	Maps	Host Profiles	VM Storage Profiles	Customization Specifications				
					Manager				

Figure 150.

2. Select a datastore.

🔁 tm-pod01-vc01 - v5phere Client								
File Edit View Inventory Administration Plug-ins Help								
🖸 🖸 🏠 Home 🕨 🛃 In	💽 🔝 🏠 Home 🕨 👸 Inventory 🕨 🏮 Datastores and Datastore Clusters							
tm-pod01-vc01	□ 😰 tm-pod01-vc01 tm-pod01-sas600-sp-01							
DemoDatacenter-01 TM-Gobal-Interchange01	center-01 bal-Interchange01 Summary Virtual Machines Hosts Performance Configuration Tasks & Events Alarms Permissions Storage Views							
TM-POD01-E5X01-Local	Capacity							
Im-pool-sxu2-tocal Im-pool-sxu2-tocal	Location: ds:///vmfs/volumes/4d884a01-73289 Type: VMFS Number of Hosts Connected: 3 Virtual Machines and Templates: 2 Commands 1	Refresh Capacity: 99.75 GB Provisioned Space: 54.06 GB Free Space: 59.70 GB Last updated on: 6/3/2011 11:04:40 AM						
	Refresh Inter SDRS Maintenance Mode Browse Datastore Rowse Datastore Assign User-Defined Storage Capability	Refresh System Storage Capability: N/A User-defined Storage Capability: N/A						

Figure 151.

3. Click on the **Performance** tab and select **Performance** in the **View** drop-down list.



Figure 152.

4. You have now successfully completed the Using Storage Performance Statistics exercise.

Help and Support During the Evaluation

This guide provides an overview of the steps required to ensure a successful evaluation of VMware vSphere. It is not meant to be a substitute for product documentation. Refer to the online vSphere product documentation for more detailed information (see the following links). You can also consult the online VMware knowledge base if you have any additional questions. If you require further assistance, 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® 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 additional information or to purchase VMware vSphere, the VMware 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, include the state, country and company name from which you are inquiring. You can also visit http://www.vmware.com/vmwarestore/.

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?

Send your feedback to the following address: tmdocfeedback@vmware.com, with "VMware vSphere 5.0 Evaluation Guide" in the subject line. Thank you for your help in making this guide a valuable resource.

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

Copyright © 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-WP-vSPHR-EVAL-GUIDE-VOL1-USLET-101-WEB