

# VMware vSphere™ 4.1

## Security Hardening Guide

April 2011

---

VMware

# VMware vSphere 4.1 Security Hardening Guide

## Table of Contents

### VMware

<b>VMware vSphere Hardening Guide Introduction</b> .....	<b>4</b>
<b>Scope</b> .....	<b>4</b>
<b>Recommendation Level</b> .....	<b>4</b>
<b>Testing for Configurations</b> .....	<b>5</b>
<b>Guideline Organization</b> .....	<b>5</b>
Virtual Machine .....	5
ESX/ESXi Host .....	5
vNetwork (Virtual Networking) .....	5
vCenter .....	6
Console Operating System (COS).....	6
<b>Guideline Templates</b> .....	<b>6</b>
Type A: Parameter Setting .....	6
Type B: Component Configuration .....	8
Type C: Operational Patterns .....	10
<b>Virtual Machines</b> .....	<b>12</b>
<b>Unprivileged User Actions</b> .....	<b>12</b>
<b>Virtual Devices</b> .....	<b>14</b>
<b>Virtual Machine Information Flow</b> .....	<b>16</b>
<b>Virtual Machine Management APIs</b> .....	<b>20</b>
<b>VMsafe</b> .....	<b>22</b>
VMsafe CPU/Memory API .....	23
VMsafe Network API.....	24
<b>General Virtual Machine Protection</b> .....	<b>26</b>
<b>ESX/ESXi Host</b> .....	<b>31</b>
<b>Installation</b> .....	<b>31</b>
<b>Storage</b> .....	<b>32</b>
<b>Host Communications</b> .....	<b>34</b>
<b>Logging</b> .....	<b>39</b>
<b>Management</b> .....	<b>41</b>
<b>Host Console</b> .....	<b>48</b>
<b>vNetwork (Virtual Networking)</b> .....	<b>54</b>
<b>Network Architecture</b> .....	<b>54</b>
<b>vNetwork Configuration</b> .....	<b>60</b>
<b>Physical Network</b> .....	<b>69</b>
<b>vCenter</b> .....	<b>72</b>
<b>vCenter Server Host</b> .....	<b>72</b>
<b>vCenter Server Communication</b> .....	<b>78</b>
<b>vCenter Server Database</b> .....	<b>85</b>
<b>vSphere Client Components</b> .....	<b>85</b>
<b>vCenter Update Manager</b> .....	<b>88</b>
<b>Console Operating System (COS)</b> .....	<b>94</b>
<b>Console Network Protection</b> .....	<b>94</b>
<b>Console Management</b> .....	<b>96</b>
<b>Console Password Policies</b> .....	<b>99</b>

## VMware vSphere 4.1 Security Hardening Guide

<b>Console Logging .....</b>	<b>103</b>
<b>Console Hardening.....</b>	<b>106</b>
<b>Console Access.....</b>	<b>109</b>

## VMware vSphere Hardening Guide Introduction

### Scope

This set of documents provides guidance on how to securely deploy VMware® vSphere™ 4.1 (“vSphere”) in a production environment. The focus is on *initial configuration of the virtualization infrastructure layer*, which covers the following:

- The virtualization hosts (both VMware ESX® 4 and VMware ESXi™ 4)
- Configuration of the virtual machine container (NOT hardening of the guest operating system (OS) or any applications running within)
- Configuration of the virtual networking infrastructure, including the management and storage networks as well as the virtual switch (but NOT security of the virtual machine’s network)
- VMware vCenter™ Server, its database and client components
- VMware Update Manager (included because the regular update and patching of the ESX/ESXi hosts and the virtual machine containers are essential to maintaining the security of the environment)

The following are specifically out of scope and are NOT covered:

- Security of the software running inside the virtual machine, such as OS and applications, and the traffic traveling through the virtual machine networks
- Security of any other add-on products, such as SRM
- Detailed operational procedures related to maintaining security, such as event monitoring, auditing and privilege management. Guidance is provided on general areas in which to perform these important tasks, but details on exactly how to perform them are out of scope.

### Recommendation Level

The recommendation level for a guideline consists of a rating that corresponds to the operational environment in which it is to be applied:

- **Enterprise:** This includes most enterprise production environments. The recommendations are meant to protect against most security attacks and provide protection of confidential information to the level required by all major security and compliance standards.
- **DMZ:** This includes environments that are particularly susceptible to targeted attacks. Examples include: Internet-facing hosts, internal systems with highly confidential or regulated data, systems subject to security standards such as the PCI-DSS, and so on.

NOTE: Despite the name, this level should not be restricted to only DMZ hosts. Each organization should make its own determination as to the applicability of this level.

## VMware vSphere 4.1 Security Hardening Guide

- **Specialized Security Limited Functionality (SSLF):** This represents specialized environments that have some unique aspect that makes them especially vulnerable to sophisticated attacks. Recommendations at this level might result in loss of functionality or inability to use certain features. Careful consideration must be given to determining the applicability of these recommendations, including the possibility of using alternate compensating controls.

Unless otherwise specified, higher security levels include all recommendations from lower levels. For example, a DMZ environment should implement all level Enterprise and DMZ recommendations, except when otherwise specified (e.g., a parameter that should be set to one value at level Enterprise but a different value at level DMZ).

### Testing for Configurations

Most configuration parameters can be viewed using the vSphere Client as well as being probed using an API client such as VMware vSphere 4 PowerCLI or vSphere Command-Line Interface (vCLI). These methods are all equivalent and nothing in this guide should be viewed as requiring a certain test method unless otherwise indicated.

### Guideline Organization

All recommendations are annotated using a code that consists of three letters followed by a two-digit number (starting with 01). The three-letter codes are as follows.

#### Virtual Machine

- VMX: VM (vmx) parameters
- VMP: General VM protection

#### ESX/ESXi Host

Unless otherwise specified, all guidelines apply to both ESX 4 and ESXi 4.

- HIN: Installation
- HST: Storage
- HCM: Host Communication
- HLG: Logging
- HMT: Management
- HCN: Host Console

#### vNetwork (Virtual Networking)

- NAR: Network Architecture
- NCN: vNetwork Configuration
- NPN: Physical Network

## vCenter

- VSH: vCenter Server Host
- VSC: vCenter Server Communication
- VSD: vCenter Server Database
- VCL: vSphere Client Components
- VUM: VMware Update Manager

## Console Operating System (COS)

NOTE: These guidelines apply only to ESX 4, not to ESXi 4.

- CON: Console OS Networks
- COM: Console OS Management
- COP: Console OS Password Policies
- COL: Console OS Logging
- COH: Console OS Hardening
- COA: Console OS Access

## Guideline Templates

The following templates are used to define the guidelines.

Because a particular security issue might require different recommendations for different operating environments, it is possible that one guideline might have multiple recommendations. The following templates use shading to indicate which parts are common to all recommendations and which parts are unique.

### Type A: Parameter Setting

Use this template type when the recommendation specifies a configuration parameter to set (or not set) in specific products.

Examples:

- VMX parameters
- ESX parameters
- vCenter parameters
- COS parameters

Parameter Element	Description
Code	Code String
Name	Short name of guideline.
Description	Description of the interface or feature that the parameter governs.

## VMware vSphere 4.1 Security Hardening Guide

<b>Threat</b>	Description of the specific threat exposed by this feature. Include characterization of vulnerability.
<b>Recommendation Level</b>	<See recommendation-level descriptions>.
<b>Parameter Setting</b>	Where the parameter is defined, and what the recommended or not recommended values are. Also indicated if there are preferred ways of setting the value (e.g., for a COS parameter, using the API instead of directly editing a configuration file).
<b>Effect on Functionality</b>	If this setting is adopted, what possible effects does it have on functionality? Does some feature stop working? Is there some information missing from a UI? (and so on)

Example:

<b>Parameter Element</b>	<b>Description</b>
<b>Code</b>	VMX01
<b>Name</b>	Prevent virtual disk shrinking.
<b>Description</b>	Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature by setting the parameters listed in Table 9.
<b>Threat</b>	Repeated disk shrinking can make virtual disk unavailable. Capability is available to nonadministrative users in the guest.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	isolation.tools.diskWiper.disable=TRUE isolation.tools.diskShrink.disable=TRUE

<b>Effect on Functionality</b>	
--------------------------------	--

### Type B: Component Configuration

Use this template type when the guideline recommends a certain configuration of components, either to reduce risk or to provide a compensating control. Typically, these involve setting some parameter to a site-specific value or installing some components in a manner that satisfies some constraint, so there is no definitive value to be checked against.

Examples include:

- Configure an NTP server.
- Isolate management networks.
- Install Update Manager on a separate server.

Configuration Element	Description
<b>Code</b>	Code String
<b>Name</b>	Short name of guideline.
<b>Description</b>	Description of the component being addressed and the configuration being recommended.
<b>Risk or Control</b>	Description of the risk being mitigated, including characterization of vulnerability if applicable.
<b>Recommendation Level</b>	<See recommendation-level descriptions>.
<b>Parameters or Objects Configuration</b>	All the parameters or objects involved, and how they should be configured.
<b>Test</b>	Any procedure or way to show evidence that the guideline is being followed, if this is possible.

Example:

Configuration Element	Description
-----------------------	-------------



## VMware vSphere 4.1 Security Hardening Guide

<b>Code</b>	NAR02	
<b>Name</b>	Ensure that vMotion™ traffic is isolated.	
<b>Description</b>	The security issue with vMotion migrations is that information is transmitted in plain text. Anyone with access to the network over which this information flows might view it. Ensure that vMotion traffic is separate from production traffic on an isolated network. This network should be a nonroutable (no layer 3 router spanning this and other networks), which will prevent any outside access to the network.	
<b>Risk or Control</b>	Attackers can sniff vMotion traffic to obtain memory contents of a virtual machine. They might also potentially stage a man-in-the-middle (MiTM) attack in which the contents are modified during migration.	
<b>Recommendation Level</b>	Enterprise.	SSLF
<b>Parameters or Objects Configuration</b>	vMotion port group should be in a dedicated VLAN on a common virtual switch (vSwitch). The vSwitch can be shared with production (VM) traffic, as long as the vMotion port group's VLAN is not used by production VMs.	vMotion port group should be on a management-only vSwitch.
<b>Effect on Functionality</b>		At least one additional physical network adaptor must be dedicated to management (more if network adaptor teaming used). This can greatly increase the cost of the physical networking infrastructure required; in resource-constrained environments (such as blades), this might not be possible to achieve.
<b>Test</b>	<ul style="list-style-type: none"> <li>• Check for usage of VLAN ID on non-vMotion port groups.</li> <li>• Check that VLAN is</li> </ul>	In addition to Enterprise tests: <ul style="list-style-type: none"> <li>• Check that vMotion port group vSwitch does not contain any nonmanagement port groups.</li> <li>• Check that the physical network is not accessed by any other nonmanagement</li> </ul>

## VMware vSphere 4.1 Security Hardening Guide

	isolated and not routed in the physical network.	entity.
--	--	---------

### Type C: Operational Patterns

This type of template should be used to describe recommendations on how to operate or interact with the administrative components of the system.

Examples include:

- Use vSphere Client and vCenter instead of COS.
- Avoid Linux-based clients unless on secure network.
- Use certificates signed by an authority.

Operational Element	Description
<b>Code</b>	Code String
<b>Name</b>	Short name of guideline.
<b>Description</b>	Description of the operational pattern or condition.
<b>Risk or Control</b>	Description of the risk being mitigated.
<b>Recommendation Level</b>	<See recommendation level descriptions>.
<b>Condition or Steps</b>	Concise description of the specific conditions to meet or avoid, and/or the steps needed to achieve this.
<b>Test</b>	Any procedure or way to show evidence that the guideline is being followed, if this is possible.

Here is an example:

Configuration Element	Description
<b>Code</b>	HCM01
<b>Name</b>	Do not use default self-signed certificates for ESX/ESXi

## VMware vSphere 4.1 Security Hardening Guide

	communication.
<b>Description</b>	Replace default self-signed certificates with those from a trusted certification authority (CA), either a commercial CA or an organizational CA.
<b>Risk or Control</b>	The use of default certificates leaves the SSL connection open to MiTM attacks. Changing the default certificates to trusted CA-signed certificates mitigates the potential for MiTM attacks.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or objects configuration</b>	<p>Information on how to replace default self-signed certificates can be found in both the <i>ESXi Configuration Guide</i> and the <i>ESX Configuration Guide</i>, “Security” chapter, “Authentication and User Management” sections, “Encryption and Security Certificates for ESX/ESXi” subsection. This section covers the following advanced customization options:</p> <ul style="list-style-type: none"> <li>• Configuring SSL timeouts</li> <li>• Configuration for certificates in nondefault locations</li> </ul> <p>The two guides can be found at these URLs:</p> <ul style="list-style-type: none"> <li>• <a href="http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf">http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf</a></li> <li>• <a href="http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf">http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf</a></li> </ul>
<b>Test</b>	Ensure that any certificates presented by the host can be verified by a trusted certification authority.

## Virtual Machines

Virtual machines are encapsulated in a small number of files. One of the important files is the configuration file (.vmx), which governs the behavior of the virtual hardware and other settings. You can see and modify the configuration settings by viewing the .vmx file directly in a text editor or by checking the settings in the vSphere Client, using the following procedure:

1. Choose the virtual machine in the inventory panel.
2. Click **Edit Settings**. Click **Options > Advanced/General**.
3. Click **Configuration Parameters** to open the configuration parameters dialog box.

You can also use any vSphere API-based tool such as PowerCLI to view and modify VMX parameters. In many instances, a VMX parameter has two versions: XXX.disable and XXX.enable. In nearly all cases, it is better to use the form XXX.disable=TRUE to disable a feature, because these are all parsed centrally in the VMX code.

Whether you change a virtual machine's settings in the vSphere Client, a vSphere API-based tool, or using a text editor, you must restart the virtual machine for most changes to take effect.

The following sections provide guidelines you should observe when dealing with these and other virtual machine files.

### Unprivileged User Actions

Parameter Element	Description
<b>Code</b>	VMX01
<b>Name</b>	Prevent virtual disk shrinking.
<b>Description</b>	Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature by setting the parameters listed in Table 9.
<b>Threat</b>	Repeated disk shrinking can make a virtual disk unavailable.

## VMware vSphere 4.1 Security Hardening Guide

	Capability is available to nonadministrative users in the guest.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	isolation.tools.diskWiper.disable=TRUE isolation.tools.diskShrink.disable=TRUE
<b>Effect on Functionality</b>	

Parameter Element	Description
<b>Code</b>	VMX02
<b>Name</b>	Prevent other users from spying on administrator remote consoles.
<b>Description</b>	By default, remote console sessions can be connected to by more than one user at a time. When multiple sessions are activated, each terminal window gets a notification about the new session.
<b>Threat</b>	If an administrator in the VM logs in using a VMware remote console during their session, a nonadministrator in the VM might connect to the console and observe the administrator's actions. Also, this could result in an administrator losing console access to a virtual machine. For example if a jump box is being used for an open console session, and the admin loses connection to that box, then the console session remains open.
<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	RemoteDisplay.maxConnections=1
<b>Effect on Functionality</b>	Only one remote console connection to the VM will be permitted. Other attempts will be rejected until the first session disconnects.

Copy and paste to and from the VM Console is disabled by default on vSphere 4.1. Please see this KB for details: <http://kb.vmware.com/kb/1026437>.

## Virtual Devices

Parameter Element	Description
<b>Code</b>	VMX10
<b>Name</b>	Ensure that unauthorized devices are not connected.
<b>Description</b>	<p>Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation.</p> <p>For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.</p> <p>NOTE: The parameters listed are not sufficient to ensure that a device is usable; other parameters are required to indicate specifically how each device is instantiated.</p>
<b>Threat</b>	Any enabled or connected device represents another potential attack channel.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<p>The following parameters should either NOT be present or should be set to FALSE, unless the device is required:</p> <ol style="list-style-type: none"> <li>1. Floppy drives: floppyX.present</li> <li>2. Serial ports: serialX.present</li> <li>3. Parallel ports: parallelX.present</li> <li>4. USB controller: usb.present</li> <li>5. CD-ROM: ideX:Y.present</li> </ol>
<b>Effect on Functionality</b>	

Parameter Element	Description
<b>Code</b>	VMX11
<b>Name</b>	Prevent unauthorized removal, connection and modification of devices.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	<p>Normal users and processes—that is, users and processes without root or administrator privileges—within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings.</p> <p>In general, you should use the virtual machine settings editor or configuration editor to remove any unneeded or unused hardware devices. However, you might want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system, as well as modifying devices, by adding the following parameters.</p>
<b>Threat</b>	<p>By default, a rogue user with nonadministrator privileges in a virtual machine can:</p> <ul style="list-style-type: none"><li>• Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive</li><li>• Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service</li><li>• Modify settings on a device</li></ul>
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<code>isolation.device.connectable.disable=TRUE</code> <code>isolation.device.edit.disable=TRUE</code>
<b>Effect on Functionality</b>	

Virtual machine communications interface (VMCI) is a new type of interface designed to provide efficient and controlled communication between VMs and trusted endpoints on the host, such as the VMKernel, and from VM to VM.

The main objective of VMCI is to provide a socket-based framework for a new generation of applications that will exist only on virtual machines. More information on how to use this interface is detailed here:

<http://www.vmware.com/support/developer/vmci-sdk>.

This interface is implemented as a virtual PCI device, present by default in all VMs created with virtual hardware version 7, common in vSphere 4, VMware Fusion and VMware Workstation 6 and above. A device driver is included and is installed by default with the VMware Tools software package in supported guest operating systems.

## VMware vSphere 4.1 Security Hardening Guide

The interface currently has only two settings: enabled and restricted. In the enabled setting, a VM can be detected and potentially interact with all other VMs that also have the enabled setting. The default is restricted. The formal recommendation is to keep it restricted unless there is a reason to enable it — in this case, an application that is specifically created to leverage this feature.

Parameter Element	Description
<b>Code</b>	VMX12
<b>Name</b>	Disable VM-to-VM communication through VMCI.
<b>Description</b>	<p>If the interface is not restricted, a VM can detect and be detected by all other VMs with the same option enabled within the same host. This might be the intended behavior, but custom-built software can have unexpected vulnerabilities that might potentially lead to an exploit. Additionally, it is possible for a VM to detect how many other VMs are within the same ESX system by simply registering the VM. This information might also be used for a potentially malicious objective.</p> <p>By default, the setting is FALSE.</p>
<b>Threat</b>	The VM can be exposed to other VMs within the same system as long as there is at least one program connected to the VMCI socket interface.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	vmci0.unrestricted=FALSE
<b>Effect on Functionality</b>	

### Virtual Machine Information Flow

Virtual machines can write troubleshooting information to a virtual machine log file (vmware.log) stored on the VMware vStorage Virtual Machine File System (VMFS) volume used to store other files for the virtual machine. Virtual machine users and processes can be configured to abuse the logging function, either intentionally or inadvertently, so that large amounts of data flood the log file. Over time, the log file can consume so much of the ESX/ESXi host's file system space that it fills the hard disk, causing an effective denial of service as the datastore can no longer accept new writes.



## VMware vSphere 4.1 Security Hardening Guide

In addition to logging, guest operating system processes can send informational messages to the ESX/ESXi host through VMware Tools. These messages, known as setinfo messages, are written to the virtual machine's configuration file (.vmx). They typically contain name-value pairs that define virtual machine characteristics or identifiers that the host stores—for example, `ipaddress=10.17.87.224`. A setinfo message has no predefined format and can be of any length. However, the total size of the VMX file is limited by default to 1MB.

Parameter Element	Description	
<b>Code</b>	VMX20	
<b>Name</b>	Limit VM log file size and number.	
<b>Description</b>	<p>You can use these settings to limit the total size and number of log files. Normally a new log file is created only when a host is rebooted, so the file can grow to be quite large. You can ensure that new log files are created more frequently by limiting the maximum size of the log files. If you want to restrict the total size of logging data, VMware recommends saving 10 log files, each one limited to 1,000KB. Datastores are likely to be formatted with a block size of 2MB or 4MB, so a size limit too far below this size would result in unnecessary storage utilization.</p> <p>Each time an entry is written to the log, the size of the log is checked; if it is over the limit, the next entry is written to a new log. If the maximum number of log files already exists, when a new one is created, the oldest log file is deleted. A denial-of-service attack that avoids these limits might be attempted by writing an enormous log entry. But each log entry is limited to 4KB, so no log files are ever more than 4KB larger than the configured limit.</p> <p>A second option is to disable logging for the virtual machine. Disabling logging for a virtual machine makes troubleshooting challenging and support difficult. You should not consider disabling logging unless the log file rotation approach proves insufficient.</p>	
<b>Threat</b>	Uncontrolled logging can lead to denial of service due to the datastore's being filled.	
<b>Recommendation Level</b>	Enterprise	SSLF
<b>Parameter Setting</b>	<code>log.rotateSize=1000000</code> <code>log.keepOld=10</code>	<code>logging=FALSE</code>
<b>Effect on</b>		VM logs unavailable for

## VMware vSphere 4.1 Security Hardening Guide

<b>Functionality</b>	troubleshooting and support.
----------------------	------------------------------

Parameter Element	Description
<b>Code</b>	VMX21
<b>Name</b>	Limit informational messages from the VM to the VMX file.
<b>Description</b>	The configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value if necessary. You might increase this value if large amounts of custom information are being stored in the configuration file. The default limit is 1MB; this limit is applied even when the sizeLimit parameter is not listed in the .vmx file.
<b>Threat</b>	Uncontrolled size for the VMX file can lead to denial of service if the datastore is filled.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	tools.setInfo.sizeLimit=1048576
<b>Effect on Functionality</b>	

Parameter Element	Description
<b>Code</b>	VMX22
<b>Name</b>	Avoid using independent nonpersistent disks.
<b>Description</b>	<p>The security issue with nonpersistent disk mode is that successful attackers, with a simple shutdown or reboot, might undo or remove any traces that they were ever on the machine.</p> <p>To safeguard against this risk, you should set production virtual machines to use either persistent disk mode or nonpersistent disk mode; additionally, make sure that activity within the VM is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector.</p>

## VMware vSphere 4.1 Security Hardening Guide

<b>Threat</b>	Without a persistent record of activity on a VM, administrators might never know whether they have been attacked or hacked.
<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	If remote logging of events and activity is not configured for the guest, scsiX:Y.mode should be either: <ol style="list-style-type: none"> <li>1. Not present</li> <li>2. Not set to independent nonpersistent</li> </ol>
<b>Effect on Functionality</b>	Won't be able to make use of nonpersistent mode, which allows rollback to a known state when rebooting the VM.

A new feature in vSphere 4.1 is the ability to direct the serial port output of a Virtual Machine to a network destination, instead of just a local destination. This allows the use of so-called Virtual Serial Port Concentrators to interact with multiple VM serial ports from a single interface. Because serial port connections to virtual machines are low-level, they may not have as strong controls over access or monitoring. Therefore the access to virtual serial ports should be tightly controlled.

Operational Element	Description
<b>Code</b>	VMX23
<b>Name</b>	Use secure protocols for virtual serial port access.
<b>Description</b>	Serial ports are interfaces for connecting peripherals to the virtual machine. They are often used on physical systems to provide a direct, low-level connection to the console of a server, and a virtual serial port allows for the same access to a virtual machine.
<b>Risk or Control</b>	Serial ports allow for low-level access, which often does not have strong controls like logging or privileges.
<b>Recommendation Level</b>	Enterprise
<b>Condition or steps</b>	Use a secure protocol like telnets as opposed to telnet to access virtual serial ports.

## VMware vSphere 4.1 Security Hardening Guide

Parameter Element	Description	
<b>Code</b>	VMX24	
<b>Name</b>	Disable certain unexposed features	
<b>Description</b>	<p>Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.</p> <p>Note that setting "isolation.tools.hgfsServerSet.disable = TRUE" disables the registration of the guest's HGFS server with the host. Without this, APIs that use HGFS to transfer files to/from the guest (such as some VIX commands or the VMware Tools auto-upgrader) won't work</p>	
<b>Threat</b>	Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.	
<b>Recommendation Level</b>	DMZ	SSLF
<b>Parameter Setting</b>	isolation.tools.unity.push.update.disable = TRUE isolation.tools.ghi.launchmenu.change = TRUE isolation.tools.memSchedFakeSampleStats.disable = TRUE isolation.tools.getCreds.disable = TRUE	isolation.tools.hgfsServerSet.disable = TRUE
<b>Effect on Functionality</b>	none	APIs that use HGFS to transfer files to/from the guest (such as some VIX commands or the VMware Tools auto-upgrader) won't work

### Virtual Machine Management APIs

## VMware vSphere 4.1 Security Hardening Guide

The VIX API is high level and practical for both script writers and application programmers. It runs on either Windows or Linux and supports management of VMware Workstation, VMware Server and VMware vSphere, including ESX/ESXi and vCenter Server. Additionally, bindings are provided for C, Perl and COM (Visual Basic, VBScript, C#).

Parameter Element	Description
<b>Code</b>	VMX30
<b>Name</b>	Disable remote operations within the guest.
<b>Description</b>	The VIX API enables systems administrators to write programs and scripts that automate virtual machine operations, as well as guest operating systems within the VMs themselves. If enabled, the system administrator can execute scripts or programs that use the VIX API to execute tasks within the guest OS.
<b>Threat</b>	An adversary potentially can execute unauthorized scripts within the guest OS.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	guest.command.enabled=FALSE
<b>Effect on Functionality</b>	

vSphere 4.0 introduces the integration of virtual machine performance counters such as CPU and memory into PerfMon for Microsoft Windows guest operating systems when VMware Tools is installed. With this feature, virtual machine owners can do accurate performance analysis within the guest operating system.

The PerfMon integration in vSphere 4 leverages the guest SDK API to get to the accurate counters from the hypervisor. The programming guide for vSphere guest SDK 4.1 is available at <http://www.vmware.com/support/developer/guest-sdk/>. The list of available performance counters is on page 11 of the PDF (accessor functions for VM data).

There is some information about the host that can optionally be exposed to the VM guests:

- GUESTLIB\_HOST\_CPU\_NUM\_CORES

## VMware vSphere 4.1 Security Hardening Guide

- GUESTLIB\_HOST\_CPU\_USED\_MS
- GUESTLIB\_HOST\_MEM\_SWAPPED\_MB
- GUESTLIB\_HOST\_MEM\_SHARED\_MB
- GUESTLIB\_HOST\_MEM\_USED\_MB
- GUESTLIB\_HOST\_MEM\_PHYS\_MB
- GUESTLIB\_HOST\_MEM\_PHYS\_FREE\_MB
- GUESTLIB\_HOST\_MEM\_KERN\_OVHD\_MB
- GUESTLIB\_HOST\_MEM\_MAPPED\_MB
- GUESTLIB\_HOST\_MEM\_UNMAPPED\_MB

The default is not to expose this information. Ordinarily you wouldn't want the guest to know anything about the host it is running on.

Parameter Element	Description
Code	VMX31
Name	Do not send host performance information to guests.
Description	If enabled, a VM can obtain detailed information about the physical host. The default value for the parameter is FALSE. This setting should not be TRUE unless a particular VM requires this information for performance monitoring.
Threat	An adversary potentially can use this information to inform further attacks on the host.
Recommendation Level	Enterprise
Parameter Setting	tools.guestlib.enableHostInfo=FALSE
Effect on Functionality	

### VMsafe

VMsafe™ provides a security architecture for virtualized environments and an API-sharing program to enable partners to develop security products for virtualized environments. VMsafe consists of three parts:

## VMware vSphere 4.1 Security Hardening Guide

- VMsafe memory and CPU API (VMsafe memory/CPU): Inspections of memory accesses and CPU states
- VMsafe network packet inspection API (VMsafe-Net): The VMsafe-Net enables you to create agents that inspect network packets at a point in the packet stream between the virtual network adaptor (vNic) and a vSwitch that sits in front of a physical network adaptor (pnetwork adaptor). The interface provided is a function call library located in the same security appliance where the control-path agent resides. The data-path and control-path agents communicate using the function calls from the library.
- VMsafe Virtual Disk Development Kit (VDDK): The VDDK is separately published. Using the VDDK, you can create applications that manage virtual disk volumes. This enables you to inspect for and prevent malicious access and modification of data in protected disks.

The VDDK API is built into vSphere, and cannot be disabled. Any entity wishing to make use of this API must present the proper credentials of an authorized user to vSphere. The method of controlling access to this API is to use the vSphere Roles and Permissions system. The user whose credentials are presented must have permission to access and modify the datastore on which the protected VM's virtual disks reside.

NOTE: This does not need to be a virtual machine running on the host; any application that has network access to an ESX/ESXi host connected to the datastore can access the VDDK API.

### VMsafe CPU/Memory API

In order for a VM to view and modify the CPU and memory contents of other VMs on the host, it must have access to the CPU/memory APIs. This access is enabled by attaching the VM to a special VMsafe introspection vSwitch.

Communication with hypervisor extension occurs over an isolated network created specifically for this purpose. A security appliance must be configured on this network before it can access the CPU and memory APIs.

By default, the CPU and memory of a virtual machine **cannot** be inspected or modified. To enable this functionality, the following settings must be present in the .vmx configuration file for each VM that is to be protected:

- vmsafe.enable = TRUE
- vmsafe.agentAddress="www.xxx.yyy.zzz"
- vmsafe.agentPort="nnnn"

where "www.xxx.yyy.zzz" is the IP address and "nnnn" is the port number that the VMsafe CPU/memory security virtual appliance uses to connect to the introspection virtual switch.

Parameter	Description
-----------	-------------

Element	
<b>Code</b>	VMX52
<b>Name</b>	Control access to VMs through VMsafe CPU/memory APIs.
<b>Description</b>	A VM must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for VMs for which you want this to be done.
<b>Threat</b>	An attacker might compromise the VM by making use of this introspection channel.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<p>If a VM is not supposed to be protected by a VMsafe CPU/memory product, ensure that the following is <b>not</b> present in its VMX file:</p> <pre>vmsafe.enable=TRUE vmsafe.agentAddress="www.xxx.yyy.zzz" vmsafe.agentPort="nnnn"</pre> <p>The latter two parameters are based on how the VMsafe security virtual appliance is configured; they should not be present at all if the VM is not to be protected.</p>
<b>Effect on Functionality</b>	

### VMsafe Network API

VMsafe network API protection is enabled by a *data path* kernel module that must be installed on the ESX/ESXi host by an administrator. This data path agent has the ability to inspect, modify and block network traffic going to and from a virtual machine's network adaptor ports. There can be up to 16 data path agents on one virtual machine network adaptor port. In addition, there typically would be a *control path* virtual appliance running on the host. This security virtual appliance must be attached to a special VMsafe introspection vSwitch to communicate with the data path agent.

Communication with the data path kernel module occurs over an isolated network created specifically for this purpose. A security appliance must be configured on this network before it can access the data path kernel module.



## VMware vSphere 4.1 Security Hardening Guide

In order for the security appliance to have access to the network packets of other virtual machines, the vmkernel must be configured to send information to it. This is done by setting a kernel parameter value to the IP address that the security virtual machine is using on the introspection virtual switch:

- /Net/DVFilterBindIpAddress

By default, the network traffic of a virtual machine **cannot** be inspected or modified. To enable this functionality, the following setting must be present in the .vmx configuration file for each VM that is to be protected:

- ethernet0.filter1.name = dv-filter1

where “ethernet0” is the network adaptor interface of the virtual machine that is to be protected, “filter1” is the number of the filter that is being used, and “dv-filter1” is the name of the particular data path kernel module that is protecting the virtual machine. There can be up to 10 network adaptors per virtual machine (ethernet0 through ethernet9) and up to 16 filters per vNIC (filter0 through filter15).

Parameter Element	Description
Code	VMX55
Name	Control access to VMs through VMsafe network APIs.
Description	A VM must be configured explicitly to accept access by the VMsafe network API. This should be done only for VMs for which you want this to be done.
Threat	An attacker might compromise the VM by making use of this introspection channel.
Recommendation Level	Enterprise
Parameter Setting	If a VM is not supposed to be protected by a VMsafe CPU/memory product, ensure that the following is <b>not</b> present in its VMX file:  ethernet0.filter1.name = dv-filter1  where “ethernet0” is the network adaptor interface of the virtual machine that is to be protected, “filter1” is the number of the filter that is being used, and “dv-filter1” is the name of the particular data path kernel module that is protecting the VM. If the VM is supposed to be protected, ensure that the name of the data path kernel is set correctly.
Effect on	

## VMware vSphere 4.1 Security Hardening Guide

Functionality	
<b>Parameter Element</b>	<b>Description</b>
<b>Code</b>	VMX56
<b>Name</b>	Restrict access to VMsafe network APIs.
<b>Description</b>	You should ensure that the only VMs configured on the VMsafe network introspection vSwitch are those that you have specifically installed to perform this task.
<b>Threat</b>	An attacker might compromise all other VMs by making use of this introspection channel.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<p>If a VMsafe Network security appliance has been deployed on a host, then ensure that this (and only this) VM's IP address is configured to use this API. This should be done by ensuring that only this VM's IP address appears in the following kernel parameter:</p> <ul style="list-style-type: none"> <li>• /Net/DVFilterBindIpAddress</li> </ul> <p>This can be done using the vCLI, for example, by issuing the command</p> <pre>vicfg-advcfg -g /Net/DVFilterBindIpAddress</pre>
<b>Effect on Functionality</b>	

### General Virtual Machine Protection

Operational Element	Description
<b>Code</b>	VMP01
<b>Name</b>	Secure virtual machines as you would secure physical machines.
<b>Description</b>	A key to understanding the security requirements of a virtualized environment is the recognition that a

## VMware vSphere 4.1 Security Hardening Guide

	virtual machine is, in most respects, the equivalent of a physical server. Therefore, it is critical that you employ the same security measures in virtual machines that you would for physical servers.
<b>Risk or Control</b>	The guest operating system that runs in the virtual machine is subject to the same security risks as a physical system.
<b>Recommendation Level</b>	Enterprise
<b>Condition or steps</b>	Ensure that antivirus, antispymware, intrusion detection, and other protection are enabled for every virtual machine in your virtual infrastructure. Make sure to keep all security measures up-to-date, including applying appropriate patches. It is especially important to keep track of updates for dormant virtual machines that are powered off, because it can be easy to overlook them.

Operational Element	Description
<b>Code</b>	VMP02
<b>Name</b>	Disable unnecessary or superfluous functions inside VMs.
<b>Description</b>	By disabling unnecessary system components that are not needed to support the application or service running on the system, you reduce the number of parts that can be attacked. VMs often don't require as many services or functions as ordinary physical servers; so when virtualizing, you should evaluate whether a particular service or function is truly needed.
<b>Risk or Control</b>	Any service running in a VM provides a potential avenue of attack.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Some of these steps include: <ul style="list-style-type: none"> <li>■ Disable unused services in the operating system. For example, if the system runs a file server, make sure to turn off any Web services.</li> <li>■ Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adaptors.</li> </ul>

## VMware vSphere 4.1 Security Hardening Guide

	<p>This is described in the “Removing Unnecessary Hardware Devices” section in the <i>ESX Configuration Guide</i>.</p> <ul style="list-style-type: none"> <li>■ Turn off any screen savers. If using a Linux, BSD, or Solaris guest operating system, do not run the X Window system unless it is necessary.</li> </ul>
--	---

Operational Element	Description
<b>Code</b>	VMP03
<b>Name</b>	Use templates to deploy VMs whenever possible.
<b>Description</b>	By capturing a hardened base operating system image (with no applications installed) in a template, you can ensure that all your virtual machines are created with a known baseline level of security. You can then use this template to create other, application-specific templates, or you can use the application template to deploy virtual machines.
<b>Risk or Control</b>	Manual installation of the OS and applications into a VM introduces the risk of misconfiguration due to human or process error.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Provide templates for VM creation that contain hardened, patched, and properly configured OS deployments. If possible, predeploy applications in templates as well, although care should be taken that the application doesn't depend upon VM-specific information to be deployed. In vSphere, you can convert a template to a virtual machine and back again quickly, which makes updating templates quite easy. VMware Update Manager also provides the ability to automatically patch the operating system and certain applications in a template, thereby ensuring that they remain up to date.

Operational Element	Description
<b>Code</b>	VMP04

## VMware vSphere 4.1 Security Hardening Guide

<b>Name</b>	Prevent virtual machines from taking over resources.
<b>Description</b>	By default, all virtual machines on an ESX/ESXi host share the resources equally. By using the resource management capabilities of ESX/ESXi, such as shares and limits, you can control the server resources that a virtual machine consumes.
<b>Risk or Control</b>	You can use this mechanism to prevent a denial of service that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.
<b>Recommendation Level</b>	DMZ
<b>Condition or Steps</b>	Use shares or reservations to guarantee resources to critical VMs. Use limits to constrain resource consumption by virtual machines that have a greater risk of being exploited or attacked, or that run applications that are known to have the potential to greatly consume resources.

<b>Operational Element</b>	<b>Description</b>
<b>Code</b>	VMP05
<b>Name</b>	Minimize use of the VM console.
<b>Description</b>	The VM console enables you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show.
<b>Risk or Control</b>	The VM console also provides power management and removable device connectivity controls, which might potentially allow a malicious user to bring down a virtual machine. In addition, it also has a performance impact on the service console, especially if many VM console sessions are open simultaneously.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Instead of VM console, use native remote management services, such as terminal services

## VMware vSphere 4.1 Security Hardening Guide

and ssh, to interact with virtual machines. Grant VM console access only when necessary.

## ESX/ESXi Host

### Installation

Operational Element	Description
<b>Code</b>	HIN01
<b>Name</b>	Verify integrity of software before installation.
<b>Description</b>	Before installing any software from VMware, its authenticity and integrity should be verified. VMware provides digital signatures for downloaded software, and physical seals for software distributed via physical media.
<b>Risk or Control</b>	Software tampering can be used to break security.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Always check the SHA1 hash after downloading an ISO from <a href="http://download.vmware.com">download.vmware.com</a> to ensure the ISO image's authenticity. If you obtain media from VMware and the security seal is broken, return the software to VMware for a replacement.

Operational Element	Description
<b>Code</b>	HIN02
<b>Name</b>	Keep ESX/ESXi system properly patched.
<b>Description</b>	By staying up to date on ESX/ESXi patches, vulnerabilities in the hypervisor can be mitigated.
<b>Risk or Control</b>	If an attacker can obtain access and elevate privileges on the ESX/ESXi system, they can then take over the VMs on that host.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Employ a system to keep the ESX/ESXi system up to date with patches in accordance with industry-

## VMware vSphere 4.1 Security Hardening Guide

standard guidelines, or internal guidelines where appropriate. VMware Update Manager is an automated tool that can greatly assist with this. VMware also publishes Advisories on security patches, and offers a way to subscribe to email alerts for them.

### Storage

Parameter Element	Description
<b>Code</b>	HST01
<b>Name</b>	Ensure bidirectional CHAP authentication is enabled for iSCSI traffic.
<b>Description</b>	vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. Choosing not to enforce more stringent authentication can make sense if you create a dedicated network or VLAN to service all your iSCSI devices. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.
<b>Threat</b>	By not authenticating both the iSCSI target and host, there is a potential for a MiTM attack in which an attacker might impersonate either side of the connection to steal data. Bidirectional authentication can mitigate this risk.
<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	Configuration → Storage Adaptors → iSCSI Initiator Properties → CHAP → CHAP (Target Authenticates Host) and Mutual CHAP (Host Authenticates Target), both set to “Use CHAP” and each with a “Name” and “Secret” configured.
<b>Effect on Functionality</b>	

Operational Element	Description
<b>Code</b>	HST02



## VMware vSphere 4.1 Security Hardening Guide

<b>Name</b>	Ensure uniqueness of CHAP authentication secrets.	
<b>Description</b>	The mutual authentication secret for each host should be different; if possible, the secret should be different for each client authenticating to the server as well. This ensures that if a single host is compromised, an attacker cannot create another arbitrary host and authenticate to the storage device.	
<b>Risk or Control</b>	With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device.	
<b>Recommendation Level</b>	DMZ	SSLF
<b>Condition or Steps</b>	Configure a different authentication secret for each ESX/ESXi host.	Configure a different secret for each client authenticating to the server.

Zoning provides access control in a SAN topology. It defines which host bus adaptors (HBAs) can connect to which SAN device service processors. When a SAN is configured using zoning, the devices outside a zone are not detectable to the devices inside the zone. In addition, SAN traffic within each zone is isolated from the other zones. Within a complex SAN environment, SAN switches provide zoning, which defines and configures the necessary security and access rights for the entire SAN.

LUN masking is commonly used for permission management. It is also referred to as selective storage presentation, access control, and partitioning, depending on the vendor. It is performed at the storage processor or server level. It makes a LUN invisible when a target is scanned. The administrator configures the disk array so each server or group of servers can detect only certain LUNs. Masking capabilities for each disk array are vendor specific, as are the tools for managing LUN masking.

Operational Element	Description
<b>Code</b>	HST03
<b>Name</b>	Mask and zone SAN resources appropriately.
<b>Description</b>	You should use zoning and LUN masking to segregate SAN activity. For example, you manage

	zones defined for testing independently within the SAN so they do not interfere with activity in the production zones. Similarly, you can set up different zones for different departments. Zoning must take into account any host groups that have been set up on the SAN device.
<b>Risk or Control</b>	
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Zoning and masking capabilities for each SAN switch and disk array are vendor specific, as are the tools for managing LUN masking.

### Host Communications

To ensure the protection of the data transmitted to and from external network connections, ESX uses the 256-bit AES block encryption. ESX Server also uses 1024-bit RSA for key exchange. Client sessions with the ESX/ESXi host can be initiated from any vSphere API client, such as vSphere Client, vCenter Server, and the vCLI.

SSL encryption protects the connection to ESX/ESXi, but the default certificates are not signed by a trusted certificate authority and, therefore, do not provide the authentication security you might need in a production environment. These self-signed certificates are vulnerable to MiTM attacks, and clients receive a warning about them. If you intend to use encrypted remote connections externally, consider purchasing a certificate from a trusted certification authority or use your own security certificate for your SSL connections.

Configuration Element	Description
<b>Code</b>	HCM01
<b>Name</b>	Do not use default self-signed certificates for ESX/ESXi communication.
<b>Description</b>	Replace default self-signed certificates with those from a trusted CA, either commercial or organizational.
<b>Risk or Control</b>	The use of default certificates leaves the SSL connection open to MiTM attacks. Changing the default certificates to trusted CA-signed certificates mitigates the potential for MiTM attacks.
<b>Recommendation Level</b>	Enterprise

## VMware vSphere 4.1 Security Hardening Guide

<b>Parameters or Objects Configuration</b>	<p>Information on how to replace default self-signed certificates can be found in both the <i>ESXi Configuration Guide</i> and the <i>ESX Configuration Guide</i>, “Security” chapter, “Authentication and User Management” section, “Encryption and Security Certificates for ESX/ESXi” subsection. This section covers the following advanced customization options:</p> <ul style="list-style-type: none"><li>• Configuring SSL timeouts</li><li>• Configuration for certificates in nondefault locations</li></ul> <p>The two guides can be found at these URLs:</p> <ul style="list-style-type: none"><li>• <a href="http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf">http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf</a></li><li>• <a href="http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf">http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf</a></li></ul> <p>Additional information may be found in this document:</p> <ul style="list-style-type: none"><li>• <a href="http://www.vmware.com/resources/techresources/10124">http://www.vmware.com/resources/techresources/10124</a></li></ul>
<b>Test</b>	<p>Ensure that any certificates presented by the host can be verified by a trusted certification authority.</p>

The host agent (hostd) acts as a proxy for several services running on the ESX/ESXi host. Most of the services are required for proper functioning of ESX/ESXi, but there are some that can be disabled. This will limit some management and diagnostic functionality on the host.

The list of currently running services may be viewed as follows:

- On ESXi: log into Tech Support Mode and issue the following command:  
`vim-cmd proxysvc/service_list`
- On ESX: log into the Service Console and issue the following command:  
`vmware-vim-cmd proxysvc/service_list`

Services can be modified by following the instructions in the following KB Article: <http://kb.vmware.com/kb/1016039>. Note that the article is written for ESX, but for ESXi the information still applies with the following changes:

The command to use is “vim-cmd” instead of “vmware-vim-cmd”. This command is executed in Tech Support Mode. The command to re-enable the welcome web page is

```
vim-cmd proxysvc/add_tcp_service "/" httpsWithRedirect localhost 8309
```

Changes take effect immediately, and persist across reboots.

## VMware vSphere 4.1 Security Hardening Guide

Parameter Element	Description
<b>Code</b>	HCM02
<b>Name</b>	Disable managed object browser.
<b>Description</b>	The managed object browser provides a way to explore the object model used by the VMkernel to manage the host; it enables configurations to be changed as well. This interface is used primarily for debugging the vSphere SDK.
<b>Threat</b>	This interface might potentially be used to perform malicious configuration changes or actions.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	Instructions for how to disable the Managed Object Browser may be found in KB 1016039.
<b>Effect on Functionality</b>	The managed object browser will no longer be available for diagnostics.

Parameter Element	Description
<b>Code</b>	HCM03
<b>Name</b>	Disable vSphere Web Access (ESX <b>only</b> ).
<b>Description</b>	<p>vSphere Web Access provides a means for users to view virtual machines on a single ESX host and perform simple operations such as power-on and suspend. It also provides a way to obtain console access to virtual machines. All of this is governed by the users permissions on the local ESX host.</p> <p>In most cases, users should manage virtual machines through vCenter Server, using either the vSphere Client or the vCenter vSphere Web Access.</p> <p>NOTE: ESXi does not have vSphere Web Access; this guideline is not relevant for ESXi.</p>
<b>Threat</b>	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.

## VMware vSphere 4.1 Security Hardening Guide

<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	In the vSphere Client, select the host, click on the configuration tab, and select the Security Profile item. Click on Properties; then in the list of services, ensure that the box for “vSphere Web Access” is unchecked.
<b>Effect on Functionality</b>	vSphere Web Access will no longer be available.

Parameter Element	Description
<b>Code</b>	HCM05
<b>Name</b>	Disable Welcome web page
<b>Description</b>	If you point a web browser at the management interface of ESX/ESXi, a static page is presented which contain links to the Managed Object Browser, the host datastore browser, and various downloads. Although the presence of this page doesn’t actually change the security profile of the host, it might be desirable to not have it displayed at all.
<b>Threat</b>	This page might reveal information about the identity of a host to an attacker.
<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	Instructions for how to disable the Welcome web page may be found in KB 1016039, with variations for ESXi as noted above.
<b>Effect on Functionality</b>	The welcome web page will no longer be accessible.

NFC (Network File Copy) is the name of the mechanism used to migrate or clone a VM between two ESX hosts over the network. The initial authentication for this transfer occurs using SSL, but by default, the actual data transfer occurs in plain text, for performance reasons.

Because this file transfer occurs over the management network, which itself should be isolated from all other non-management traffic, the risk of data being leaked is related to the isolation of that management network.

## VMware vSphere 4.1 Security Hardening Guide

If desired, SSL can be enabled on the data transfer part of NFC. If SSL is enabled, the NFC traffic will go through a SSL connection rather than plain TCP connection. You can add the following entry in vpxd.cfg to enable NFC SSL.

```
<config>
  <nfc>
    <useSSL>true</useSSL>
  </nfc>
</config>
```

NOTE: the use of SSL for NFC data transfer has not been extensively tested.

Parameter Element	Description
<b>Code</b>	HCM06
<b>Name</b>	Use SSL for Network File Copy (NFC).
<b>Description</b>	NFC (Network File Copy) is the name of the mechanism used to migrate or clone a VM between two ESX hosts over the network. By default, SSL, is used only for the authentication of the transfer, but If desired, SSL can also be enabled on the data transfer.
<b>Threat</b>	VM contents could potentially be sniffed if the management network is not adequately isolated and secured.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	Add the following entry in vpxd.cfg to enable NFC SSL.  <config> <nfc> <useSSL>true</useSSL> </nfc> </config>

<p><b>Effect on Functionality</b></p>	<p>This setting will likely reduce performance of actions involving NFC, such as VM clone or migration. It has also not been extensively tested and so may cause operations to fail in certain circumstances.</p>
---------------------------------------	---

## Logging

The following sets of recommendations do not pertain to ESX 4.1 (i.e., the “classic” ESX architecture, with the console OS). They apply to only the ESXi architecture. Logging for the ESX architecture is covered separately in the Console Operating System section of this guide.

ESXi 4.1 maintains a log of activity in log files, using a syslog facility. The following logs are available:

- hostd.log
- messages
- vpxa.log (only if the host has been joined to a VirtualCenter instance)

There are several ways to view the contents of these log files.

To view the logs in a VI Client, take the following steps:

1. Log in directly to the ESXi host using VI Client; make sure the host is selected in the inventory.
2. Click **Administration**; then click the **System Logs** tab.
3. Choose the log file you want to view in the drop-down menu in the upper left.

To view the logs in a Web browser, enter the URL `https://<hostname>/host`, where <hostname> is the host name or IP address of the management interface of the ESXi host; then choose from the list of files presented. You can also use the vCLI command `vifs` to download the log files to your local system.

An important point to consider is that the log messages are not encrypted when sent to the remote host, so it is important that the network for the service console be strictly isolated from other networks.

Another point is that, by default, the logs on ESXi are stored only in the in-memory file system. They are lost upon reboot, and only one day’s worth of logs are stored. Persistent logging to a datastore can be configured. It is recommended that this be done so that a dedicated record of server activity is available for that host.

Configuration Element	Description
Code	HLG01

## VMware vSphere 4.1 Security Hardening Guide

<b>Name</b>	Configure remote syslog.
<b>Description</b>	Remote logging to a central host provides a way to greatly increase administration capabilities. By gathering log files onto a central host, you can easily monitor all hosts with a single tool. You can also do aggregate analysis and searching to look for such things as coordinated attacks on multiple hosts.
<b>Risk or Control</b>	Logging to a secure, centralized log server can help prevent log tampering; it also provides a long-term audit record.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	Remote syslog can be configured on an ESXi host, using a remote command line such as vCLI or PowerCLI, or using an API client.
<b>Test</b>	Query the syslog configuration to make sure that a valid syslog server has been configured, including the correct port.

Configuration Element	Description
<b>Code</b>	HLG02
<b>Name</b>	Configure persistent logging.
<b>Description</b>	By default, the logs on ESXi are stored only in the in-memory file system. The logs are lost upon reboot; only one day's worth of logs are stored. Persistent logging to a datastore can be configured; it is recommended that this be done so that a dedicated record of server activity is available for that host.
<b>Risk or Control</b>	In addition to remote syslog, having the log files for a server sent to a datastore provides a dedicated set of log records for that server, making it easier to monitor events and diagnose issues for that specific server.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	Persistent logging to a datastore for an ESXi host can be configured using the vSphere Client, vCLI or other API client. More information on how this can be done can be found in <i>vSphere Basic System Administration Guide</i> in the "Configuring Hosts and vCenter Server" chapter, in the "System Log Files:



## VMware vSphere 4.1 Security Hardening Guide

	Configure Syslog on ESXi Hosts” section.
<b>Test</b>	View the contents of the configured log file on the datastore to make sure that it is being updated with log messages.

Configuration Element	Description
<b>Code</b>	HLG03
<b>Name</b>	Configure NTP time synchronization.
<b>Description</b>	By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC), you can make it simpler to track and correlate an intruder’s actions when reviewing the relevant log files.
<b>Risk or Control</b>	Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects configuration</b>	NTP can be configured on an ESXi host using the vSphere Client or a remote command line such as vCLI or PowerCLI. To avoid potential vulnerabilities in the NTP software, it is recommended to synchronize the ESXi clock with a time server that is located on the management network rather than directly with a time server on a public network. This time server can then synchronize with a public source through a strictly controlled network connection with a firewall.
<b>Test</b>	<ul style="list-style-type: none"> <li>• Query the NTP configuration to make sure that a valid time source has been configured.</li> <li>• Make sure that the NTP service is running on the host.</li> </ul>

## Management

The Common Information Model (CIM) is an open standard that defines a framework for agent-less, standards-based monitoring of hardware resources for

## VMware vSphere 4.1 Security Hardening Guide

ESXi. This framework consists of a CIM object manager, often called a CIM broker, and a set of CIM providers.

CIM providers are used as the mechanism to provide management access to device drivers and underlying hardware. Hardware vendors, including server manufacturers and specific hardware device vendors, can write providers to provide monitoring and management of their particular devices. VMware also writes providers that implement monitoring of server hardware, ESXi storage infrastructure, and virtualization-specific resources. These providers run inside the ESXi system and therefore are designed to be extremely lightweight and focused on specific management tasks. The CIM broker takes information from all CIM providers, and presents it to the outside world via standard APIs, the most common one being WS-MAN.

Parameter Element	Description
<b>Code</b>	HMT01
<b>Name</b>	Control access by CIM-based hardware monitoring tools.
<b>Description</b>	The CIM system provides an interface that enables hardware-level management from remote applications via a set of standard APIs. To ensure that the CIM interface is secure, provide only the minimum access necessary to these applications. Do not provision them with the root account or any other full administrator account; instead, provide an account that has only limited privileges.
<b>Threat</b>	If an application has been provisioned with a root or full administrator account, compromise of that application can lead to full compromise of the virtual environment.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>Do not provide root credentials to remote applications to access the CIM interface. Instead, create a service account specific to these applications. Read-only access to CIM information is granted to any local account defined on the ESX/ESXi system, as well as any role defined in vCenter Server.</p> <p>If the application requires write access to the CIM interface, only two privileges are required. It is recommended that you create a role to apply to the service account with only these privileges:</p> <ul style="list-style-type: none"><li>• Host &gt; Config &gt; SystemManagement</li><li>• Host &gt; CIM &gt; CIMInteraction</li></ul> <p>This role can be either local to the host or centrally defined on</p>

## VMware vSphere 4.1 Security Hardening Guide

	vCenter Server, depending on how the particular monitoring applications work.
<b>Test</b>	Logging into the host with the service account (e.g., using the vSphere Client) should provide only read-only access, or only the two privileges indicated above.

ESXi 4.1 contains a different SNMP agent from that in ESX 4.1, and it supports only versions 1 and 2c. It provides the same notifications as ESX 4.1 and adds notifications for hardware-related sensors. Unlike ESX 4.1, it supports only the SNMPv2-MIB, and only for discovery, inventory and diagnostics of the SNMP agent.

SNMP messages contain a field called the *community string*, which conveys context and usually identifies the sending system for notifications. This field also provides context for the instance of a MIB module on which the host should return information. ESX/ESXi SNMP agents allow multiple community strings per notification target as well as for polling. Keep in mind that community strings are not meant to function as passwords but only as a method for logical separation.

Configuration Element	Description
<b>Code</b>	HMT02
<b>Name</b>	Ensure proper SNMP configuration (ESXi <b>only</b> ).
<b>Description</b>	If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured.
<b>Risk or Control</b>	If SNMP is not properly configured, monitoring information can be sent to a malicious host that can then use this information to plan an attack.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	SNMP can be configured on an ESXi host, using a remote command line such as vCLI or PowerCLI, or using an API client.
<b>Test</b>	If SNMP is not being used, make sure that it is not running.  If SNMP is being used, make sure the parameter settings have the right destination properly configured.

## VMware vSphere 4.1 Security Hardening Guide

As with ESX, ESXi maintains its configuration state in a set of configuration files. However, on ESXi these files can be accessed using only the remote file access API, and there are far fewer files involved. These files normally are not modified directly. Instead, their contents normally change indirectly because of some action invoked on the host. However, the file access API does allow for direct modification of these files, and some modifications might be warranted in special circumstances.

The following is a list of configuration-related files exposed via the vSphere API on ESXi:

- esx.conf
- hostAgentConfig.xml
- hosts
- license.cfg
- motd
- openwsman.conf
- proxy.xml
- snmp.xml
- ssl\_cert
- ssl\_key
- syslog.conf
- vmware\_config
- vmware\_configrules
- vmware.lic
- vpxa.cfg

NOTE: for the most up-to-date list, a live system with the latest patch release of ESXi should be queried. The accessible and relevant configuration files are found by browsing to <https://<hostname>/host>.

Operational Element	Description
<b>Code</b>	HMT03
<b>Name</b>	Establish and maintain configuration file integrity (ESXi <b>only</b> ).
<b>Description</b>	ESXi maintains its configuration state in a set of configuration files. You should monitor all of these files for integrity and unauthorized tampering, either by periodically downloading them and tracking their contents or by using a commercial tool designed to do this. Any changes should be correlated with some approved administrative action, such as a configuration change.

## VMware vSphere 4.1 Security Hardening Guide

<b>Risk or Control</b>	Tampering with these files has the potential to enable unauthorized access to the host configuration and virtual machines.
<b>Recommendation Level</b>	DMZ
<b>Condition or Steps</b>	<p>The accessible and relevant configuration files in ESXi 4.1 are found by browsing to <code>https://&lt;hostname&gt;/host</code>.</p> <p>The files can be viewed or retrieved using this Web interface or with an API client (e.g., vCLI, PowerCLI). This provides a means to keep track of the files and their contents, to ensure that they are not improperly modified.</p> <p>Be sure not to monitor log files and other files whose content is expected to change regularly due to system activity. Also, account for configuration file changes that are due to deliberate administrative activity.</p> <p>NOTE: for file integrity monitoring on ESX 4.1, refer to the section on the Console Operating System.</p>

VMsafe provides a security architecture for virtualized environments and an API-sharing program to enable partners to develop security products for virtualized environments. For more information on VMsafe, see the “Virtual Machine” section of this guide.

VMsafe network API protection is enabled by a *data path* kernel module that must be installed on the ESX/ESXi host by an administrator. This data path agent has the ability to inspect, modify, and block network traffic going to and from a virtual machine’s network adaptor ports. In addition, there typically would be a *control path* virtual appliance running on the host. This security virtual appliance must be configured to communicate with the data path agent. This is done by setting a kernel parameter value to the IP address that the security virtual machine is using on the introspection virtual switch:

- `/Net/DVFilterBindIpAddress`

Configuration Element	Description
<b>Code</b>	HMT12
<b>Name</b>	Prevent unintended use of VMsafe network APIs.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	If you are not using any products that make use of the VMsafe network API, the host should not be configured to send network information to any VM.
<b>Risk or Control</b>	If the API is enabled, an attacker might attempt to connect a VM to it, thereby potentially providing access to the network of other VMs on the host.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>If a VMsafe network security appliance is not being used on the host, ensure that the following kernel parameter has a blank value:</p> <ul style="list-style-type: none"> <li>• /Net/DVFilterBindIpAddress</li> </ul> <p>This can be done using the vCLI, for example, by issuing the command</p> <pre>vicfg-advcfg -g /Net/DVFilterBindIpAddress</pre>

<b>Configuration Element</b>	<b>Description</b>
<b>Code</b>	HMT15
<b>Name</b>	Audit for loading of unauthorized kernel modules (ESXi <b>only</b> ).
<b>Description</b>	VMware provides digital signatures for 3 <sup>rd</sup> party kernel modules that meet certain requirements. By default the ESXi host does not permit loading of kernel modules that lack a valid digital signature. This behavior can be overridden; however, a warning is sent to the system logs alerting the Admin any time an unauthorized module is loaded.
<b>Risk or Control</b>	Malicious kernel modules can be used to take full control of the ESXi host
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>The “messages” kernel log file will show an entry any time an unsigned module is loaded into memory. This log file should be monitored and scanned for this text. The message will be of the form</p> <pre>ALERT: Elf: NNNN: Kernel module XXXXX was loaded, but has no signature attached</pre>

Where “NNNN” is a number and “XXXXX” is the name of the module

In order to control an ESX/ESXi host, vCenter Server creates a special user account called ‘vpxuser’ on each host as it is joined to the inventory. This is a privileged account which acts as a proxy for all actions initiated through vCenter Server. It is created automatically on an ongoing basis. The vpxuser password is 32 characters long and is guaranteed to contain at least one symbol from the following four character classes:

1. Symbols in the set "-./:=@[\\]^\_{}~"
2. Digits 0-9
3. Upper case letters
4. Lower case letters

The vpxuser password is randomly generated with the use of OpenSSL crypto libraries as a source of randomness. The expiration time is 30 days by default and can be changed in the vCenter server advanced options for VirtualCenter.VimPasswordExpirationInDays. The password length is 32 by default but can be changed by modifying vpxd.hostPasswordLength in the vpxd.cfg file.

Configuration Element	Description
<b>Code Number</b>	HMT20
<b>Name</b>	Ensure that vpxuser auto-password change meets policy.
<b>Description</b>	By default, the vpxuser password will be automatically changed by vCenter every 30 days. Ensure that this setting meets your policies; if not, configure to meet password aging policies. NOTE: It is very important that the password aging policy not be shorter than the interval that is set to automatically change the vpxuser password, to preclude the possibility that vCenter might get locked out of an ESX host.
<b>Risk or Control</b>	If an attacker obtains the vpxuser password, the password can be used only for a limited amount of time.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	Configure the following parameter in the vCenter Server advanced settings in the vSphere Client: vCenterVirtualCenter.VimPasswordExpirationInDays

## VMware vSphere 4.1 Security Hardening Guide

	On an ESX host, ensure that the value is set lower than the password aging policy on the COS.
--	---

Configuration Element	Description
Code Number	HMT21
Name	Ensure that vpxuser password meets length policy.
Description	The default length of the vpxuser password is 32 characters. Ensure that this setting meets your policies; if not, configure to meet password length policies
Risk or Control	Longer passwords make brute-force password attacks more difficult.
Recommendation Level	DMZ
Parameters or Objects Configuration	If the password length does not meet your security policies modify the vpxd.hostPasswordLength parameter in the vpxd.cfg file.

### Host Console

The following sets of recommendations do not pertain to ESX 4.1 (i.e., the “classic” ESX architecture, with the console OS). They apply to only the ESXi architecture.

The Direct Console User Interface (DCUI) is the interface available at the console of an ESXi host (e.g., at the terminal connect to the server) or the iLO, DRAC, or other out-of-band management console of the host. It allows for basic host configuration—modifying networking settings and the root password, for example—as well as performing maintenance operations such as restarting agents or rebooting the host.

A username and password must be entered to access the DCUI. By default, only the root account has access to the DCUI. Additional accounts may be given access to the DCUI by granting them the local Administrator role on the ESXi host.

Lockdown mode is available on any ESXi 4.1 host that you have added to a vCenter Server. Enabling lockdown mode disables all remote access to ESXi 4.1 machines. Any subsequent local changes to the host must be made:

- Using the DCUI. Access to the DCUI is not affected by lockdown mode.
- In a vSphere Client session or using vCLI commands to vCenter Server.



## VMware vSphere 4.1 Security Hardening Guide

Note that lockdown mode can be enabled or disabled in two places:

- In the vSphere Client, when connected to the vCenter Server managing the host
- In the DCUI of the host

Parameter Element	Description
<b>Code</b>	HCN02
<b>Name</b>	Enable lockdown mode to restrict remote access.
<b>Description</b>	<p>Lockdown mode can be enabled after an ESXi host is added to vCenter Server. Enabling lockdown mode disables all remote access to ESXi 4.1 machines. Any subsequent local changes to the host must be made:</p> <ul style="list-style-type: none"> <li>• Using the DCUI</li> <li>• In a vSphere Client session or using vCLI commands to vCenter Server</li> </ul> <p>There are some operations, such as backup and troubleshooting, that require direct access to the host. In these cases Lockdown Mode can be disabled on a temporary basis for specific hosts as needed, and then re-enabled when the task is completed.</p>
<b>Threat</b>	Security best practices dictate that administrative tasks be controlled and monitored from a central location. By forcing all interaction to occur through vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	To do this manually, in the vSphere Client, in the configuration tab for a host, in the security profile setting, select Lockdown Mode "Edit" and click the checkbox for "Lockdown Mode." This can also be done using PowerCLI or with an API client, as well as with Host Profiles. Lockdown mode can also be enabled and disabled from the DCUI.
<b>Effect on Functionality</b>	Enabling lockdown prevents all API-based access by the all accounts to the ESXi host. This includes: vSphere Client, vCLI, PowerCLI, and any API-based client.

## VMware vSphere 4.1 Security Hardening Guide

In the extreme case, disabling of all direct access to the host may be desired. For example, you might want to prevent anyone with the root password from disabling lockdown mode and managing the host. In this case, you can take the additional step of disabling the DCUI for the host, through vCenter Server. After this is done, no direct interaction with the host, local or remote, is possible. It can be managed only through vCenter Server. If vCenter Server is down or otherwise unavailable, you cannot revert to direct management, because logging into the DCUI is no longer possible. If the vCenter Server cannot be restored, then the only way to revert to direct management is to reinstall the ESXi software on the host.

The following table presents a summary of lockdown mode and its interaction with the various host access services

Access mode	Normal	Lock down	Lock down + DCUI disabled
vSphere API (e.g., vSphere client, PowerCLI, vCLI, etc)	Any user, based on local roles/privileges	None (except vCenter "vpxuser")	None (except vCenter "vpxuser")
CIM	Any user, based on local role/privilege	None (except via vCenter ticket)	None (except via vCenter ticket)
DCUI	Root and users with admin privileges	Root only	None
Tech Support Mode (local and remote)	Root and users with admin privileges	None	None

Parameter Element	Description
<b>Code</b>	HCN05
<b>Name</b>	Disable DCUI to prevent all local administrative control.
<b>Description</b>	The DCUI allows for simple low-level configuration, such as hostname and root password, as well as diagnostic capabilities such as viewing log files, restarting agents, and resetting configurations. To restrict local administrative activity, it can be disabled.
<b>Threat</b>	A user with local administrator role can perform actions directly in the DCUI, and this won't be tracked by vCenter Server. Even if Lockdown Mode is enabled, someone with the root password can perform administrative tasks in the DCUI. Disabling it prevents local activity and thus forces actions to be performed in vCenter

## VMware vSphere 4.1 Security Hardening Guide

	Server, where they can be centrally audited and monitored.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	To do this manually, in the vSphere Client, in the configuration tab for a host, in the security profile setting, select “Properties” for the Services, highlight DCUI and click “Options”. The pop-up window will let you enable and disable the DCUI service. This can also be done using PowerCLI or with an API client, as well as with Host Profiles. Lockdown mode can also be enabled and disabled from the DCUI.
<b>Effect on Functionality</b>	The DCUI will no longer be accessible. If Lockdown Mode is enabled, then no direct connection to the host will be possible, and all interaction must occur through vCenter Server.

On ESXi, Tech Support Mode is a simple shell for advanced technical support. With situations in which remote command-line tools are not capable of addressing some particular issue, Tech Support Mode provides an alternative. Similar to the way the COS is used to execute diagnostic commands and fix certain low-level problems, Tech Support Mode enables users to view log and configuration files, as well as run certain configuration and utility commands in order to diagnose and fix problems. Note that Tech Support Mode is not based on Linux; rather, it is a limited-capability shell compiled especially for ESXi.

In ESXi 4.1, Tech Support Mode is fully supported for use by end-users, and is enhanced in several ways. In addition to being available on the local console of a host, it can also be accessed remotely through SSH. Access to Tech Support Mode is controlled in the following ways:

- Both local and remote Tech Support Mode can be enabled and disabled separately in both the DCUI and vCenter Server.
- Tech Support Mode may be used by any authorized user, not just root users. Users become authorized when they are granted the administrator role on a host (through Active Directory membership in a privileged group and through other methods).
- All commands issued in Tech Support Mode are logged through syslog, allowing for a full audit trail. If a syslog server is configured, then this audit trail is automatically included in the remote logging.
- A timeout can be configured for Tech Support Mode (both local and remote), so that after being enabled, it will automatically be disabled after the configured time.

## VMware vSphere 4.1 Security Hardening Guide

Tech Support Mode is recommended for use primarily for support, troubleshooting and break-fix situations. It also can be used as part of a scripted installation, as described in the next section. All other uses of Tech Support Mode, including running custom scripts, are not recommended for most cases.

To ensure accurate and reliable system logs, you should configure remote syslog on the server, so log messages are kept on an outside system and cannot be altered from the server.

Parameter Element	Description
<b>Code</b>	HCN06
<b>Name</b>	Disable Tech Support Mode unless needed for diagnostics and break-fix
<b>Description</b>	Tech Support Mode is an interactive command line available only on the console of the server or remotely via SSH. Access to this mode requires the root password of the server. It can be turned on and off for individual hosts, and on a production server should only be turned on if needed to solve a particular troubleshooting issue.
<b>Threat</b>	Anyone logged into Tech Support Mode can assume complete control of the host, including reconfiguring and stealing a virtual machine.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<p>Tech Support Mode can be enabled and disabled in one of several ways:</p> <ul style="list-style-type: none"><li>- On the DCUI of a host, in the Troubleshooting Options menu</li><li>- With the vSphere Client, on the Configuration tab for a host in the Security Profiles section</li><li>- Using Host Profiles, management CLI (e.g. PowerCLI), or vSphere API</li></ul> <p>Local and Remote Tech Support Mode must be enabled and disabled independently of one another.</p>
<b>Effect on Functionality</b>	If Tech Support Mode is disabled, supportability and diagnosability of the host might be limited.

## VMware vSphere 4.1 Security Hardening Guide

Parameter Element	Description
<b>Code</b>	HCN07
<b>Name</b>	Set a timeout for Tech Support Mode
<b>Description</b>	A timeout can be configured for Tech Support Mode (both local and remote), so that after being enabled, it will automatically be disabled after the configured time. A value of ten minutes is recommended, although the exact value depends upon the needs of your particular environment.
<b>Threat</b>	If Tech Support Mode is left enabled by accident, it increases the potential for someone to gain privileged access to the host
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	<p>The timeout for Tech Support Mode can be set in the DCUI, under the menu item for Troubleshooting Options.</p> <p>You can also enable the TSM timeout value in the vSphere client. On the Configuration tab select Advanced Settings in the Software section. Find the <u>UserVars.TSMTimeout</u> parameter and set it to a value between 0 and 86400 seconds. A value of 0 disables TSM timeout.</p>
<b>Effect on Functionality</b>	If Tech Support Mode is disabled, supportability and diagnosability of the host might be limited.

## vNetwork (Virtual Networking)

### Network Architecture

NOTE: Unless otherwise indicated, “vSwitch” refers generically to both VMware vNetwork Standard Switches and VMware vNetwork Distributed Switches (Distributed Switches). In the case of Distributed Switches, it is not restricted to any particular vendor.

Several capabilities of vSphere involve communication among components over a management network.

This includes the following types of communication:

- Between ESX/ESXi and vCenter Server
- Among ESX/ESXi hosts—for example, for VMware HA coordination
- Between ESX/ESXi or vCenter and systems running client software such as the vSphere Client or a vSphere SDK application
- Between ESX/ESXi and ancillary management services, such as DNS, NTP, syslog and the user authentication service
- Between a client system and a privileged VM interface, such as the virtual machine console or the virtual serial port
- Between ESX/ESXi and third-party management tools, such as third-party virtual switch management, hardware monitoring, systems management and backup tools
- Between vCenter Server and supporting services, such as the vCenter Server database and the user authentication service
- Between vCenter Server and optional add-on components such as VMware Update Manager
- VMware Converter Enterprise, if they are installed on separate servers
- vMotion, involving transferring the live running state of a virtual machine from one ESX/ESXi host to another
- Storage, including any network-based storage, such as iSCSI and NFS

All of the networks used for these communications provide direct access to core functionality of vSphere. The management network provides access to the vSphere management interface on each component; any remote attack would most likely begin with gaining entry to this network. vMotion traffic is not encrypted, so the entire state of a virtual machine might potentially be snooped from this network. Finally, access to the storage network potentially allows someone to read the contents of virtual disks residing on shared storage. Therefore, all of these networks should be isolated and strongly secured from all other traffic, especially any traffic going to and from virtual machines. The exception is if one of the components previously listed actually runs in a virtual machine. In that case, this virtual machine naturally has an interface on the management network and therefore should not have an interface on any other network.

## VMware vSphere 4.1 Security Hardening Guide

VMware recommends that you isolate networks using one of these methods:

- Create a separate VLAN for each network.
- Configure network access for each network through its own virtual switch and one or more uplink ports.

In either case, you should consider using network adaptor teaming for the virtual switches to provide redundancy.

If you use VLANs, you need fewer physical network adaptors to provide the isolation, a factor that is especially important in environments with constrained hardware such as blades. VMware virtual switches, by design, are immune to certain types of attacks that have traditionally targeted VLAN functionality. In general, VMware believes that VLAN technology is mature enough that it can be considered a viable option for providing network isolation. The greater risk in using VLANs is that of misconfiguration, in both the virtual network layer and the physical switches.

If you do not use VLANs, either because the VLAN support in your physical network environment is not sufficiently mature or because you do not consider VLANs strong enough for isolation, you can combine the management networks onto one or two virtual switches. However, you should still keep the virtual machine networks separate from the management networks by using separate virtual switches with separate uplinks.

No matter how the management network is restricted, there will always be a need for administrators to access this network to configure vCenter and the ESX/ESXi hosts. Instead of allowing client systems on this network, there are ways to enable access to management functionality in a strictly controlled manner. One way to do this is to configure a controlled gateway or other controlled method to access the management network. For example, require that administrators connect to it via a VPN, and allow access only by trusted administrators.

A more secure way to restrict access to the management network is to Configure jump boxes that run vSphere Client and other management clients (e.g., vMA). There are different industry-accepted ways to configure a jump box, and the particular method should be chosen based upon a local risk assessment. In one implementation, these systems reside on the management network and do not run any other application. In addition to controlling access to the management network, require that administrators use a remote display protocol (such as RDP or PCoIP) to connect to the jump boxes, and that this access goes through a firewall that restricts network traffic only to this display protocol and any other required to support it. Only the management clients running on the jump boxes are able to manage the vSphere deployment.

Note that if the VMs being hosted are only going to be accessed by the same administrators that are accessing the management interfaces then the need to have a separate management network is diminished because the risk is also diminished. For example if the VMs running on an ESX host are all Top Secret in

## VMware vSphere 4.1 Security Hardening Guide

nature and that is the highest level of classification of VM that will be running on the host, then having a separate management network is not necessary. However if there are different security levels of VMs running on the host/cluster (for example, DMZ VMs and Internal VMs, or PCI and non-PCI VMs), then the management network should be protected at the security level of the most secure VM running on a host/cluster.

At no time should a management interface be on a network where the VMs running on that host are publicly accessible as this introduces too much risk that a compromised VM could then allow an attacker to attack the management interfaces.

Configuration Element	Description	
<b>Code</b>	NAR01	
<b>Name</b>	Ensure that vSphere management traffic is on a restricted network.	
<b>Description</b>	<p>The vSphere management network provides access to the vSphere management interface on each component. Any remote attack would most likely begin with gaining entry to this network. The vSphere management interfaces include:</p> <ul style="list-style-type: none"> <li>• Service console interface on ESX</li> <li>• Management VMkernel interface on ESXi</li> </ul>	
<b>Risk or Control</b>	Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems.	
<b>Recommendation Level</b>	Enterprise	SSLF
<b>Parameters or Objects Configuration</b>	The vSphere management port group should be in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (VM) traffic, as long as the vSphere management port group's VLAN is not used by production VMs.	The vSphere management port group should be on a management-only vSwitch,
<b>Effect on Functionality</b>		At least one additional physical network adaptor must be dedicated to management (more if network adaptor teaming is



## VMware vSphere 4.1 Security Hardening Guide

		used). This might greatly increase the cost of the physical networking infrastructure required; in resource-constrained environments (such as blades), this might not be possible to achieve.
<b>Test</b>	<ul style="list-style-type: none"> <li>• Check for usage of VLAN ID on nonmanagement port groups</li> <li>• Check that the network segment is not routed, except possibly to networks where other management-related entities are found. In particular, make sure that production VM traffic cannot be routed to this network.</li> </ul>	<p>In addition to enterprise tests,</p> <ul style="list-style-type: none"> <li>• Check that the management-only vSwitch does not contain any nonmanagement port groups.</li> </ul>

<b>Configuration Element</b>	<b>Description</b>	
<b>Code</b>	NAR02	
<b>Name</b>	Ensure that vMotion traffic is isolated.	
<b>Description</b>	The security issue with vMotion migrations is that information is transmitted in plain text, and anyone with access to the network over which this information flows can view it. Ensure that vMotion traffic is separate from production traffic on an isolated network. This network should be nonroutable (no layer 3 router spanning this and other networks), which will prevent any outside access to the network.	
<b>Risk or Control</b>	Attackers can sniff vMotion traffic to obtain memory contents of a VM. They might also potentially stage a MiTM attack in which the contents are modified during migration.	
<b>Recommendation Level</b>	Enterprise	SSLF
<b>Parameters or Objects</b>	vMotion port group should be	vMotion port group should be on a management-only vSwitch.

## VMware vSphere 4.1 Security Hardening Guide

<b>Configuration</b>	in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (VM) traffic, as long as the vMotion port group's VLAN is not used by production VMs.	
<b>Effect on Functionality</b>		At least one additional physical network adaptor must be dedicated to management (more if network adaptor teaming is used). This might greatly increase the cost of the physical networking infrastructure required, and in resource-constrained environments (such as blades), this might not even be possible to achieve.
<b>Test</b>	<ul style="list-style-type: none"> <li>• Check for usage of VLAN ID on non-vMotion port groups.</li> <li>• Check that VLAN is isolated and not routed in the physical network.</li> </ul>	<p>In addition to enterprise tests:</p> <ul style="list-style-type: none"> <li>• Check that vMotion port group vSwitch does not contain any nonmanagement port groups.</li> <li>• Check that the physical network is not accessed by any other nonmanagement entity.</li> </ul>

Configuration Element	Description
<b>Code</b>	NAR03
<b>Name</b>	Ensure that IP-based storage traffic is isolated.
<b>Description</b>	<p>Virtual machines might share virtual switches and VLANs with the IP-based storage configurations. IP-based storage includes:</p> <ul style="list-style-type: none"> <li>• iSCSI</li> <li>• NFS</li> </ul> <p>This type of configuration might expose IP-based storage traffic to</p>

## VMware vSphere 4.1 Security Hardening Guide

	<p>unauthorized virtual machine users. To restrict unauthorized users from viewing the IP-based storage traffic, the IP-based storage network should be logically separated from the production traffic. Configuring the IP-based storage adaptors on separate VLANs or network segments from the VMkernel management and service console network will limit unauthorized users from viewing the traffic.</p>	
<b>Risk or Control</b>	<p>IP-based storage frequently is not encrypted and therefore can be viewed by anyone with access to this network.</p>	
<b>Recommendation Level</b>	Enterprise	SSLF
<b>Parameters or Objects Configuration</b>	<p>Storage port groups should be in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (VM) traffic, as long as the storage port group's VLAN is not used by production VMs.</p>	<p>Storage port group should be on a management-only vSwitch.</p>
<b>Effect on Functionality</b>		<p>At least one additional physical network adaptor must be dedicated to management (more if network adaptor teaming is used). This might greatly increase the cost of the physical networking infrastructure required; in resource-constrained environments (such as blades), this might not even be possible to achieve.</p>
<b>Test</b>	<ul style="list-style-type: none"> <li>• Check for usage of VLAN ID on non-storage port groups.</li> <li>• Check that VLAN is isolated and not routed in the physical network.</li> </ul>	<p>In addition to enterprise tests,</p> <ul style="list-style-type: none"> <li>• Check that storage port group vSwitch does not contain any nonmanagement port groups.</li> <li>• Check that the physical network is not accessed by any other nonmanagement entity.</li> </ul>

Operational Element	Description
Code	NAR04

## VMware vSphere 4.1 Security Hardening Guide

<b>Name</b>	Strictly control access to management network.	
<b>Description</b>	<p>The management network should be protected at the security level of the most secure VM running on a host/cluster.</p> <p>No matter how the management network is restricted, there will always be a need for administrators to access this network to configure vCenter and the ESX/ESXi hosts. Instead of allowing client systems on this network, there are ways to enable access to management functionality in a strictly controlled manner.</p>	
<b>Risk or Control</b>	If an attacker gains access to the management network, it provides the staging ground for further attack.	
<b>Recommendation Level</b>	Enterprise	DMZ
<b>Condition or Steps</b>	Configure a controlled gateway or other controlled method to access the management network. For example, require that administrators connect to it via a VPN, and allow access only by trusted administrators.	Configure jump boxes that run vSphere Client and other management clients (e.g., vMA). There are different industry-accepted ways to configure a jump box, and the particular method should be chosen based upon a local risk assessment.

### vNetwork Configuration

Port groups define how virtual machine connections are made through the virtual switch. Port groups can be configured with bandwidth limitations and VLAN tagging policies for each member port. Multiple ports can be aggregated under port groups to provide a local point for virtual machines to connect to a network. The maximum number of port groups that can be configured on a virtual switch is 512. A network label and optionally a VLAN ID identify each port group.

Configuration Element	Description
<b>Code</b>	NCN02
<b>Name</b>	Ensure that there are no unused ports on a

## VMware vSphere 4.1 Security Hardening Guide

	distributed vSwitch port group.
<b>Description</b>	The number of ports in a distributed port group can be adjusted to exactly match the number of VMs assigned to that port group.
<b>Risk or Control</b>	Limiting the number of ports in a port group limits the potential for a VM administrator, either accidentally or maliciously, to move a VM to an unauthorized network. This is especially relevant if the management network is on a distributed switch, because it could help prevent someone from putting a rogue VM on this network.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	“Number of Ports” setting in the settings page of a port group.
<b>Test</b>	<p>Can be done manually through the vSphere Client.</p> <ol style="list-style-type: none"> <li>1. While connected to the vCenter Server: Navigate to Home → Inventory → Networking in the vSphere Client and click on the vDS in question.</li> <li>2. Click on the Ports Tab.</li> <li>3. Check if all of the ports in the list have a VM associated with them in the “connected” column.</li> </ol> <p>The equivalent steps can be automated using scripting or the SDK.</p>

Each virtual network adaptor in a virtual machine has an initial MAC address assigned when the virtual adaptor is created. Each virtual adaptor also has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. A virtual adaptor’s effective MAC address and initial MAC address are the same when they are initially created. However, the virtual machine’s operating system might alter the effective MAC address to another value at any time. If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. System administrators can use virtual switch security profiles on ESX Server hosts to protect against this type of attack by setting two options on virtual switches. These options are MAC Address Changes and Forged Transmits.

## VMware vSphere 4.1 Security Hardening Guide

MAC address changes are set to accept by default, meaning that the virtual switch accepts requests to change the effective MAC address. The MAC Address Changes option setting affects traffic received by a virtual machine. To protect against MAC impersonation, this option will be set to reject, ensuring that the virtual switch does not honor requests to change the effective MAC address to anything other than the initial MAC address. Setting this to reject disables the port that the virtual network adaptor used to send the request. Therefore, the virtual network adaptor does not receive any more frames until it configures the effective MAC address to match the initial MAC address. The guest operating system will not detect that the MAC address change has not been honored.

Forged transmissions are set to accept by default. This means the virtual switch does not compare the source and effective MAC addresses. The Forged Transmits option setting affects traffic transmitted from a virtual machine. If this option is set to reject, the virtual switch compares the source MAC address being transmitted by the operating system with the effective MAC address for its virtual network adaptor, to see if they are the same. If the MAC addresses are different, the virtual switch drops the frame. The guest operating system will not detect that its virtual network adaptor cannot send packets using the different MAC address. To protect against MAC address impersonation, all virtual switches should have forged transmissions set to reject.

ESX Server has the ability to run virtual and physical network adaptors in promiscuous mode. Promiscuous mode can be enabled on public and private virtual switches. When it is enabled for a public virtual switch, all virtual machines connected to the public virtual switch have the potential of reading all packets sent across that network, from other virtual machines and any physical machines or other network devices. When it is enabled for a private virtual switch, all virtual machines connected to the private virtual switch have the potential of reading all packets across that network, meaning only the virtual machines connected to that private virtual switch. By default, promiscuous mode is set to reject, meaning that the virtual network adaptor cannot operate in promiscuous mode.

These parameters can be set on a per-vSwitch basis. They can also be overridden on individual port groups, and this is how exceptions should be made for special VMs that require these capabilities, such as inline virtual security devices or clustering software.

Parameter Element	Description
Code	NCN03
Name	Ensure that the "MAC Address Change" policy is set to reject.
Description	To protect against MAC impersonation, this option should be set to reject, ensuring that the virtual switch does not honor requests to change the effective MAC address to anything other than the

## VMware vSphere 4.1 Security Hardening Guide

	initial MAC address.
<b>Threat</b>	If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	MAC address changes set to reject (accept by default) on all vSwitches.
<b>Effect on Functionality</b>	This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. vShield Zones will not operate properly if the “MAC Address Change” is set to reject. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the port groups that these applications are connected to.

Parameter Element	Description
<b>Code</b>	NCN04
<b>Name</b>	Ensure that the “Forged Transmits” policy is set to reject.
<b>Description</b>	Forged transmissions should be set to accept by default. This means the virtual switch does not compare the source and effective MAC addresses. To protect against MAC address impersonation, all virtual switches should have forged transmissions set to reject.
<b>Threat</b>	If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	“Forged Transmits” parameter should be set to “Reject” on all

## VMware vSphere 4.1 Security Hardening Guide

	vSwitches.
<b>Effect on Functionality</b>	This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. vShield Zones will not operate properly if the “Forged Transmits” parameter is set to “Reject.” This will also affect applications that require a specific MAC address for licensing. An exception should be made for the port groups that these applications are connected to.

Parameter Element	Description
<b>Code</b>	NCN05
<b>Name</b>	Ensure that the “Promiscuous Mode” policy is set to reject.
<b>Description</b>	Promiscuous mode is disabled by default on the ESX Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons.
<b>Threat</b>	When promiscuous mode is enabled for a private virtual switch, all virtual machines connected to the private virtual switch have the potential of reading all packets across that network, meaning only the virtual machines connected to that private virtual switch.
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	“Promiscuous Mode” parameter should be set to “Reject” on all vSwitches.
<b>Effect on Functionality</b>	vShield Zones and other security devices that require the ability to see all packets on a vSwitch will not operate properly if the “Promiscuous Mode” parameter is set to “Reject.” An exception should be made for the port groups that these applications are connected to, in order to allow for full-time visibility to the traffic on that virtual switch.

Physical switches use the native VLAN for switch control and management protocol. Native VLAN frames are not tagged with any VLAN ID in many types of switches. The trunk ports implicitly treat all untagged frames as native VLAN



## VMware vSphere 4.1 Security Hardening Guide

frames. VLAN 1 is the default native VLAN ID for many commercial switches. However, in many enterprise networks, the native VLAN might be VLAN 1 or any number depending on the switch type.

Parameter Element	Description
<b>Code</b>	NCN06
<b>Name</b>	Ensure that port groups are not configured to the value of the native VLAN.
<b>Description</b>	<p>ESX does not use the concept of native VLAN. Frames with VLAN specified in the port group will have a tag, but frames with VLAN not specified in the port group are not tagged and therefore will end up as belonging to native VLAN of the physical switch.</p> <p>For example, frames on VLAN 1 from a Cisco physical switch will be untagged, because this is considered as the native VLAN. However, frames from ESX specified as VLAN 1 <i>will</i> be tagged with a "1"; therefore, traffic from ESX that is destined for the native VLAN will not be correctly routed (because it is tagged with a "1" instead of being untagged), and traffic from the physical switch coming from the native VLAN will not be visible (because it is not tagged).</p>
<b>Risk or Control</b>	If the ESX virtual switch port group uses the native VLAN ID, traffic from those VMs will not be visible to the native VLAN on the switch, because the switch is expecting untagged traffic.
<b>Recommendation Level</b>	Enterprise
<b>Parameters Setting</b>	If the default value of 1 for the native VLAN is being used, the ESX Server virtual switch port groups should be configured with any value between 2 and 4094. Otherwise, ensure that the port group is <b>not</b> configured to use whatever value is set for the native VLAN.

Parameter Element	Description
-------------------	-------------

## VMware vSphere 4.1 Security Hardening Guide

<b>Code</b>	NCN07
<b>Name</b>	Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT).
<b>Description</b>	When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest VM without modifying the VLAN tags, leaving it up to the guest to deal with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself.
<b>Risk or Control</b>	If VGT is enabled inappropriately, it might cause denial of service or allow a guest VM to interact with traffic on an unauthorized VLAN.
<b>Recommendation Level</b>	Enterprise
<b>Parameters setting</b>	VLAN ID setting on all port groups should not be set to 4095 unless VGT is required.

<b>Parameter Element</b>	<b>Description</b>
<b>Code</b>	NCN08
<b>Name</b>	Ensure that port groups are not configured to VLAN values reserved by upstream physical switches
<b>Description</b>	Certain physical switches reserve certain VLAN IDs for internal purposes and often disallow traffic configured to these values. For example, Cisco Catalyst switches typically reserve VLANs 1001–1024 and 4094, while Nexus switches typically reserve 3968–4047 and 4094. Check with the documentation for your specific switch.
<b>Risk or Control</b>	Using a reserved VLAN might result in a denial of service on the network.
<b>Recommendation Level</b>	Enterprise
<b>Parameters Setting</b>	VLAN ID setting on all port groups should not be set to reserved values of the physical switch.

## VMware vSphere 4.1 Security Hardening Guide

Operational Element	Description
<b>Code</b>	NCN10
<b>Name</b>	Ensure that port groups are configured with a clear network label.
<b>Description</b>	A network label identifies each port group with a name. These names are important because they serve as a functional descriptor for the port group.
<b>Risk or Control</b>	Without these descriptions, identifying port groups and their functions becomes difficult as the network becomes more complex.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>This can be done through the vSphere client by manually checking the names of the different port groups. To check the port group names in the vSphere client, connect to the vCenter server and navigate to Home → Inventory → Networking. You will be able to view all the different port groups and determine if the port group names are clearly labeled or might be renamed with a meaningful name.</p> <p>Scripted method (vCLI command): vicfg-vswitch -l command.</p>

Operational Element	Description
<b>Code</b>	NCN11
<b>Name</b>	Ensure that all vSwitches have a clear network label.
<b>Description</b>	Virtual switches within the ESX Server require a field for the name of the switch. This label is important because it serves as a functional descriptor for the switch, just as physical switches require a host name.
<b>Risk or Control</b>	Labeling virtual switches will indicate the function or the IP subnet of the virtual switch. For instance, labeling the virtual switch as “internal” or some

## VMware vSphere 4.1 Security Hardening Guide

	variation will indicate that the virtual switch is only for internal networking between a virtual machine's private virtual switch with no physical network adaptors bound to it.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>This can be done through the vSphere Client by manually checking the names of the different vSwitches. To check the port group names in the vSphere Client, connect to the vCenter server and navigate to Home → Inventory → Networking. You will be able to view all the different vSwitches and determine if the port group names are clearly labeled or might be renamed with a meaningful name.</p> <p>Scripted method (vCLI command): vicfg-vswitch -l command.</p>

Operational Element	Description
<b>Code</b>	NCN12
<b>Name</b>	Fully document all VLANs used on vSwitches.
<b>Description</b>	When defining a physical switch port for trunk mode, care must be taken to ensure that only specified VLANs are configured. It is considered best practice to restrict only those VLANs required on the VLAN trunk link.
<b>Risk or Control</b>	The risk with not fully documenting all VLANs on the vSwitch is that it is possible that a physical trunk port might be configured without needed VLANs, or with unneeded VLANs, potentially enabling an administrator to either accidentally or maliciously connect a VM to an unauthorized VLAN.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>Both standard and distributed vSwitch configurations can be viewed in the vSphere Client or by using the vSphere API.</p> <p>For a standard vSwitch, vicfg-vswitch -l will list all port groups and their VLAN association. Compare</p>

	this list with the physical switch configuration.
--	---

Operational Element	Description
<b>Code</b>	NCN13
<b>Name</b>	Ensure that only authorized administrators have access to virtual networking components.
<b>Description</b>	It is important to leverage the role-based access controls within vSphere to ensure that only authorized administrators have access to the different virtual networking components. For example, VM administrators should have access only to port groups in which their VMs reside. Network administrators should have permissions to all virtual networking components but not have access to VMs. These controls will depend very much on the organization's policy on separation of duties, least privilege, and the responsibilities of the administrators within the organization.
<b>Risk or Control</b>	This control mitigates the risk of misconfiguration, whether accidental or malicious, and enforces key security concepts of separation of duties and least privilege.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Ensure that vSphere permissions to specific port groups are granted only to those individuals who need it.

### Physical Network

Operational Element	Description
<b>Code</b>	NPN01
<b>Name</b>	Ensure that physical switch ports are configured with spanning tree disabled.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	EST mode has a one-to-one relationship; the number of VLANs supported on the ESX Server system is limited to the number of physical network adaptor ports assigned to the VMkernel. EST is enabled when the port group's VLAN ID is set to 0 or left blank. Due to the integration of the ESX Server into the physical network, the physical network adaptors must have spanning tree disabled or portfast configured for external switches, because VMware virtual switches do not support STP. Virtual switch uplinks do not create loops within the physical switch network.
<b>Risk or Control</b>	If these are not set, potential performance and connectivity issues might arise.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Log in to the physical switch and ensure that spanning tree protocol is disabled and/or portfast is configured for all physical ports connected to ESX/ESXi hosts.

Operational Element	Description
<b>Code</b>	NPN02
<b>Name</b>	Ensure that the <i>non-negotiate</i> option is configured for trunk links between external physical switches and virtual switches in VST mode.
<b>Description</b>	In order to communicate with virtual switches in VST mode, external switch ports must be configured as trunk ports. VST mode does not support Dynamic Trunking Protocol (DTP), so the trunk must be static and unconditional. The auto or desirable physical switch settings do not work with the ESX Server because the physical switch communicates with the ESX Server using DTP. The <i>non-negotiate</i> and <i>on</i> options unconditionally enable VLAN trunking on the physical switch and create a VLAN trunk link between the ESX Server and the physical switch. The difference between <i>non-negotiate</i> and <i>on</i> options is that <i>on</i> mode still sends out DTP frames, whereas the <i>non-negotiate</i>

## VMware vSphere 4.1 Security Hardening Guide

	option does not.
<b>Risk or Control</b>	The <i>non-negotiate</i> option should be used for all VLAN trunks, to minimize unnecessary network traffic for virtual switches in VST mode.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Log in to the physical switch and ensure that DTP is not enabled on the physical switch ports connected to the ESX/ESXi Host.

Operational Element	Description
<b>Code</b>	NPN03
<b>Name</b>	Ensure that VLAN trunk links are connected only to physical switch ports that function as trunk links.
<b>Description</b>	When connecting a virtual switch to a VLAN trunk port, you must be careful to properly configure both the virtual switch and the physical switch at the uplink port. If the physical switch is not properly configured, frames with the VLAN 802.1q header would be forwarded to a switch not expecting their arrival. The vSphere administrator should always ensure that virtual switch uplinks, acting as VLAN trunk links, are connected only to physical switch ports that function as trunk links.
<b>Risk or Control</b>	Misconfiguration of the physical switch ports might lead to undesirable performance, including frames being dropped or misdirected.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Routinely check physical switch ports to ensure that they are properly configured as trunk ports.

## vCenter

### vCenter Server Host

Because vCenter Server runs on a Windows host, it is especially critical to protect this host against vulnerabilities and attacks. The standard set of recommendations applies, as it would for any host: Install antivirus agents, spyware filters, intrusion detection systems, and any other security measures. Make sure to keep all security measures up to date, including application of patches.

Operational Element	Description
<b>Code</b>	VSH01
<b>Name</b>	Maintain supported operating system, database, and hardware for vCenter.
<b>Description</b>	vCenter Server resides on a Windows-based operating system and therefore requires a supported version of Windows.
<b>Risk or Control</b>	If vCenter is not running on a supported OS, it might not run properly. An attacker might be able to take advantage of this to perform a DoS attack or worse.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>For OS and database compatibility, see the <i>vSphere Compatibility Matrixes</i> white paper:  <a href="http://www.vmware.com/pdf/vsphere4/r40/vsp_compatibility_matrix.pdf">http://www.vmware.com/pdf/vsphere4/r40/vsp_compatibility_matrix.pdf</a></p> <p>For hardware requirements, see the <i>ESX and vCenter Server Installation Guide</i> white paper:  <a href="http://www.vmware.com/pdf/vsphere4/r40/vsp_40_esx_vc_installation_guide.pdf">http://www.vmware.com/pdf/vsphere4/r40/vsp_40_esx_vc_installation_guide.pdf</a></p>



## VMware vSphere 4.1 Security Hardening Guide

Operational Element	Description
<b>Code</b>	VSH02
<b>Name</b>	Keep vCenter Server system properly patched.
<b>Description</b>	By staying up to date on Window patches, vulnerabilities in the OS can be mitigated.
<b>Risk or Control</b>	If an attacker can obtain access and elevate privileges on the vCenter Server system, they can then take over the entire vSphere deployment.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Employ a system to keep the vCenter Server system up to date with patches in accordance with industry-standard guidelines, or internal guidelines where appropriate.

Operational Element	Description
<b>Code</b>	VSH03
<b>Name</b>	Provide Windows system protection on the vCenter Server host.
<b>Description</b>	By providing OS-level protection, vulnerabilities in the OS can be mitigated. This protection includes antivirus, antimalware, and similar measures.
<b>Risk or Control</b>	If an attacker can obtain access and elevate privileges on the vCenter Server system, they can then take over the entire vSphere deployment.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Provide Windows system protection, such as antivirus, in accordance with industry-standard

## VMware vSphere 4.1 Security Hardening Guide

	guidelines, or internal guidelines where appropriate.
--	---

Operational Element	Description
<b>Code</b>	VSH04
<b>Name</b>	Avoid user login to vCenter Server system.
<b>Description</b>	After someone has logged in to the vCenter Server system, it becomes more difficult to prevent what they can do. In general, logging in to the vCenter Server system should be limited to very privileged administrators, and then only for the purpose of administering vCenter Server or the host OS.
<b>Risk or Control</b>	Anyone logged in to the vCenter Server can potentially cause harm, either intentionally or unintentionally, by altering settings and modifying processes. They also have potential access to vCenter credentials, such as the SSL certificate.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Restrict login to the vCenter System only to those personnel who have legitimate tasks to perform in it. Ensure that they log in only when necessary, and audit these events.

Configuration Element	Description
<b>Code</b>	VSH05
<b>Name</b>	Install vCenter Server using a service account instead of a built-in Windows account.
<b>Description</b>	<p>You can use the Microsoft Windows built-in system account or a user account to run vCenter Server. With a user account, you can enable Windows authentication for SQL Server; it also provides more security.</p> <p>The user account must be an administrator on the local machine. In the installation wizard, you specify the account name as DomainName\Username. If</p>

## VMware vSphere 4.1 Security Hardening Guide

	<p>you are using SQL Server for the vCenter database, you must configure the SQL Server database to allow the domain account access to SQL Server.</p> <p>Even if you do not plan to use Microsoft Windows authentication for SQL Server, or if you are using an Oracle database, you might want to set up a local user account for the vCenter Server system. In this case, the only requirement is that the user account is an administrator on the local machine.</p>
<b>Risk or Control</b>	The Microsoft Windows built-in system account has more permissions and rights on the server than the vCenter Server system requires, which can contribute to security problems.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	Before installing vCenter Server, create a special-purpose user account on the Windows host and grant it only to the local administrator role on the host. This account should have "Act as part of the operating system" privilege, and write access to the local file system. Specify this account in the vCenter Server installation process.
<b>Test</b>	<ul style="list-style-type: none"> <li>- Check to see that the vCenter processes are running as the service account.</li> <li>- Check to make sure that the service account has only local administrator role.</li> </ul>

Configuration Element	Description
<b>Code</b>	VSH06
<b>Name</b>	Restrict usage of vSphere administrator privilege.
<b>Description</b>	By default, vCenter Server grants full administrative rights to the local administrator's account, which can be accessed by domain administrators.
<b>Risk or Control</b>	Separation of duties dictates that full vSphere administrative rights should be granted only to those administrators who are required to have it. This privilege should not be granted to any group whose membership is not strictly controlled. Therefore, administrative

## VMware vSphere 4.1 Security Hardening Guide

	rights should be removed from the local Windows administrator account and instead be given to a special-purpose local vSphere administrator account.	
<b>Recommendation Level</b>	Enterprise	DMZ
<b>Condition or Steps</b>	<ol style="list-style-type: none"> <li>1. Create an ordinary user account that will be used to manage vCenter (example vi-admin).</li> <li>2. Make sure the user does not belong to any local groups, such as administrator.</li> <li>3. Log onto vCenter as the Windows administrator; then grant the role of administrator (global vCenter administrator) to the account created in step 1 on the top-level hosts and clusters folder.</li> <li>4. Log out of vCenter and log into vCenter with the account created in step 1; verify that user is able to perform all tasks available to a vCenter administrator.</li> <li>5. Remove the permissions in the vCenter for the local administrator group.</li> </ol>	<p>After performing the steps in the “Enterprise” level, protect the vi-admin account from regular usage and instead rely upon accounts tied to specific individuals. This should be done as follows:</p> <ol style="list-style-type: none"> <li>1. Logged in as vi-admin, grant full administrative rights to the minimum number of individuals required, typically senior IT staff.</li> <li>2. Log out as vi-admin, and then protect the password.</li> </ol> <p>There are numerous ways in which the password can be protected; for example, use a very strong password and then lock the printout in a safe, or employ a system by which two individuals each must type one half of a password, the other half of which is mutually unknown by the other individual.</p>
<b>Test</b>	Observe the assigned permissions in vSphere; make sure that “Administrator” or any other account or group does not have any privileges.	

Operational Element	Description
<b>Code</b>	VSH07
<b>Name</b>	Check for privilege re-assignment after vCenter Server restarts

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	<p>During a restart of vCenter Server, if the user or user group that is assigned Administrator Role on the root folder could not be verified as a valid user/group during the restart, the user/group's permission as Administrator will be removed. In its place, vCenter Server grants the Administrator role to the local Windows administrators group, to act as a new vCenter Server administrator.</p> <p>Since it is not recommended to grant vCenter Server Administrator rights to Windows Administrators, this results in a situation that should be rectified by re-establishing a legitimate administrator account.</p>
<b>Risk or Control</b>	<p>Separation of duties dictates that full vSphere administrative rights should be granted only to those administrators who are required to have it. This privilege should not be granted to any group whose membership is not strictly controlled. Therefore, administrative rights should be removed from the local Windows administrator account and instead be given to a special-purpose local vSphere administrator account.</p>
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>Any time that vCenter Server restarts, the log file should be scanned to ensure that no privileges were re-assigned.</p> <p>For the location of vCenter Server log files, please see this KB: <a href="http://kb.vmware.com/kb/1021804">http://kb.vmware.com/kb/1021804</a>.</p>

Operational Element	Description
<b>Code</b>	VSH10
<b>Name</b>	Clean up log files after failed installations of vCenter Server
<b>Description</b>	<p>In certain cases, if the vCenter installation fails, a log file (with a name of the form "hs_err_pidXXXX") is created that contains the database password in plain text.</p>

## VMware vSphere 4.1 Security Hardening Guide

<b>Risk or Control</b>	An attacker who breaks into the vCenter Server server could potentially steal this password and access the vCenter Database.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	If at any time a vCenter Server installation fails, the log files should be deleted securely before putting the host into production. For the location of vCenter Server log files, please see this KB: <a href="http://kb.vmware.com/kb/1021804">http://kb.vmware.com/kb/1021804</a> .

### vCenter Server Communication

Client sessions with vCenter Server can be initiated from any vSphere API client, such as vSphere Client and PowerCLI. By default, SSL encryption protects this connection, but the default certificates are not signed by a trusted certificate authority and, therefore, do not provide the authentication security you might need in a production environment. These self-signed certificates are vulnerable to MiTM attacks, and clients receive a warning about them. If you intend to use encrypted remote connections externally, consider purchasing a certificate from a trusted certificate authority or use your own security certificate for your SSL connections.

Certificates are currently stored in C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL\. By default, these can be accessed by any user on the server.

Configuration Element	Description
<b>Code</b>	VSC01
<b>Name</b>	Do not use default self-signed certificates.
<b>Description</b>	Self-signed certificates are automatically generated by vCenter Server during the installation process, are not signed by a commercial CA, and might not provide strong security. Replace default self-signed certificates with those from a trusted certification authority, either a commercial CA or an organizational CA.
<b>Risk or Control</b>	The use of default certificates leaves the SSL connection open to MiTM attacks. Changing the default certificates to trusted

## VMware vSphere 4.1 Security Hardening Guide

	CA-signed certificates mitigates the potential for MiTM attacks.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	For instructions on how to change self-signed certificates, see the “ <i>Replacing vCenter Server Certificates</i> ” white paper:  <a href="http://www.vmware.com/resources/techresources/10124">http://www.vmware.com/resources/techresources/10124</a>
<b>Test</b>	Ensure that any certificates presented by the host can be verified by a trusted certification authority.

Operational Element	Description
<b>Code</b>	VSC02
<b>Name</b>	Monitor access to SSL certificates.
<b>Description</b>	The directory that contains the SSL certificates only needs to be accessed by the service account user on a regular basis. Occasionally, the vCenter Server system administrator might need to access it for support purposes.
<b>Risk or Control</b>	The SSL certificate can be used to impersonate vCenter and decrypt the vCenter database password.
<b>Recommendation Level</b>	DMZ
<b>Condition or Steps</b>	Use event log monitoring to alert on nonservice account access to certificates directory.

Parameter Element	Description
<b>Code</b>	VSC03
<b>Name</b>	Restrict access to SSL certificates.
<b>Description</b>	By default, any user on the vCenter Server system can access the directory containing the SSL certificates. The directory that contains the SSL certificates only needs to be accessed by the

## VMware vSphere 4.1 Security Hardening Guide

	service account user on a regular basis. Occasionally, when collecting data for support purposes, the vCenter Server system administrator might need to access it.
<b>Threat</b>	The SSL certificate can be used to impersonate vCenter and decrypt the vCenter database password.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	Change the Windows file permission on the SSL certificate directory so that only the vCenter service account can access it.
<b>Effect on Functionality</b>	Supportability limitations: <ul style="list-style-type: none"> <li>• Will prevent a complete support log from being collected when the vc-support script is issued</li> <li>• Will prevent the administrator from being able to change the vCenter database password</li> </ul>

Operational Element	Description
<b>Code</b>	VSC04
<b>Name</b>	Always verify SSL certificates.
<b>Description</b>	When connecting to vCenter Server using vSphere Client, the client checks to see if the certificate being presented can be verified by a trusted third party. If it cannot be, the user is presented with a warning and the option to ignore this check. This warning should not be ignored; if an administrator is presented with this warning, they should inquire further about it before proceeding.
<b>Risk or Control</b>	Without certificate verification, the user can be subject to a MiTM attack, which potentially might enable compromise through impersonation with the user's credentials to the vCenter Server system.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Instruct any user of vSphere Client to never ignore certificate verification warnings.

The only network connection vCenter Server requires is to the management network described in the vNetwork section. Avoid putting the vCenter Server



## VMware vSphere 4.1 Security Hardening Guide

system on any other network, such as your production or storage network, or on a network with access to the public Internet. Specifically, vCenter Server does not need access to the network on which vMotion operates. By limiting the network connectivity, you cut down on the possible avenues of attack.

In general, vCenter Server needs network connectivity only to the following systems:

- All ESX/ESXi hosts
- The vCenter Server database
- Other vCenter Server systems, if operating in linked mode.
- Systems that are authorized to run management clients. Examples of these include:
  - o vSphere Client
  - o vMA (the vSphere Management Assistant)
  - o A Windows system from which the PowerCLI is to be used
  - o Any other SDK-based client
- Systems running add-on components, such as VMware Update Manager
- IT infrastructure services, such as DNS, AD, NTP, and so on
- Other systems running components essential to any particular functionality of vCenter Server that is needed

Use the following guidelines to limit network connectivity:

Configuration Element	Description
<b>Code</b>	VSC05
<b>Name</b>	Restrict network access to vCenter Server system.
<b>Description</b>	Restrict access to only those essential components required to communicate with vCenter.
<b>Risk or Control</b>	Blocking access by unnecessary systems mitigates against general attacks on the Windows system.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	You should protect the vCenter Server by using a local firewall on the Windows system of vCenter, or by using a network firewall. This protection should include IP-based access restrictions, so that only necessary components can communicate with the vCenter Server system.
<b>Test</b>	

## VMware vSphere 4.1 Security Hardening Guide

Configuration Element	Description
<b>Code</b>	VSC06
<b>Name</b>	Block access to ports not being used by vCenter.
<b>Description</b>	A local firewall on the Windows system of vCenter, or a network firewall, can be used to block access to ports not specifically being used by vCenter.
<b>Risk or Control</b>	Blocking unneeded ports can militate against general attacks on the Windows system.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	<p>A list of ports used by vCenter can be found in this VMware Knowledge Base article: <a href="http://kb.vmware.com/kb/1012382">http://kb.vmware.com/kb/1012382</a></p> <p>Here is a partial list of examples of where ports might be blocked:</p> <ul style="list-style-type: none"> <li>• 636/TCP: If the vCenter will not be part of a linked-mode vCenter group</li> <li>• 1521/TCP: If the VCDB is not Oracle</li> </ul> <p>Make sure not to block any ports for functionality that is actually in use in your environment.</p>
<b>Test</b>	

Parameter Element	Description
<b>Code</b>	VSC07
<b>Name</b>	Disable managed object browser.
<b>Description</b>	The managed object browser provides a way to explore the object model used by the vCenter to manage the vSphere environment; it enables configurations to be changed as well. This interface is used primarily for debugging the vSphere SDK.
<b>Threat</b>	This interface might potentially be used to perform malicious configuration changes or actions.
<b>Recommendation</b>	DMZ

## VMware vSphere 4.1 Security Hardening Guide

<b>Level</b>	
<b>Parameter Setting</b>	To disable the managed object browser, edit the vpxd.cfg file and ensure that the following element is set: <code>&lt;enableDebugBrowse&gt;false&lt;/enableDebugBrowse/&gt;</code> This should be the only occurrence of this element, and it should be within the <code>&lt;vpxd&gt;</code> ... <code>&lt;/vpxd&gt;</code> element in vpxd.cfg
<b>Effect on Functionality</b>	The managed object browser will no longer be available for diagnostics.

<b>Parameter Element</b>	<b>Description</b>
<b>Code</b>	VSC08
<b>Name</b>	Disable vSphere Web Access.
<b>Description</b>	vSphere Web Access provides a means for users to view virtual machines and perform simple operations such as power-on and suspend. It also provides a way to obtain console access to virtual machines. All of this is governed by the users permissions on vCenter Server.  In some cases, you might want to disable vSphere Web Access to eliminate the risk of having an open interface that is not being used.
<b>Threat</b>	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.
<b>Recommendation Level</b>	DMZ
<b>Parameter Setting</b>	To completely delete the vSphere Web Access service from vCenter Server:  <ol style="list-style-type: none"> <li>1. Select <b>Start &gt; Programs &gt; Administrative Tools &gt; Services</b>.</li> <li>2. Stop the VMware VirtualCenter Management Webservices service.</li> <li>3. Use Windows Explorer to open C:\Program Files\VMware\Infrastructure\tomcat\webapps and delete the ui</li> </ol>

## VMware vSphere 4.1 Security Hardening Guide

	<p>directory.</p> <p>4. (Optional) Use Windows Explorer to open C:\Program Files\VMware\Infrastructure\tomcat\work\Catalina\localhost and delete the ui directory.</p> <p>5. Start the VMware VirtualCenter Management Webservices service.</p> <p>See VMware Knowledge Base #1009420 for more details.</p> <p>NOTE: Any upgrade to vCenter Server will recreate this file.</p>
<b>Effect on Functionality</b>	vSphere Web Access will no longer be available.

<b>Parameter Element</b>	<b>Description</b>
<b>Code</b>	VSC09
<b>Name</b>	Disable datastore browser.
<b>Description</b>	<p>The datastore browser enables you to view all the datastores associated with the vSphere deployment, including all folders and files contained in them, such as VM files. This is governed by the users permissions on vCenter Server.</p> <p>In some cases, you might want to disable the datastore browser to eliminate the risk of having an open interface that is not being used.</p>
<b>Threat</b>	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	<p>To disable the datastore browser, edit the vpxd.cfg file and ensure that the following element is set:</p> <pre>&lt;enableHttpDatastoreAccess&gt;false&lt;/enableHttpDatastoreAccess&gt;</pre> <p>This should be the only occurrence of this element, and it should be within the</p> <pre>&lt;vpxd&gt; ... &lt;/vpxd&gt;</pre> <p>element in vpxd.cfg</p>
<b>Effect on</b>	You will no longer be able to browse and view datastore files using

## VMware vSphere 4.1 Security Hardening Guide

<b>Functionality</b>	a Web browser connected to vCenter Server.  NOTE: The datastore browser available on each ESX/ESXi host is unaffected by this setting; it can be disabled separately using a host-level setting.
----------------------	--

### vCenter Server Database

Configuration Element	Description
<b>Code</b>	VSD01
<b>Name</b>	Use least privileges for the vCenter Server database user.
<b>Description</b>	vCenter requires only certain specific privileges on the database. Furthermore, certain privileges are required only for installation and upgrade, and can be removed during normal operation. These privileges should be added again if another upgrade must be performed.
<b>Risk or Control</b>	Least privileges mitigates attacks if the vCenter database account is compromised.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>The privileges needed for vCenter on both Oracle and Microsoft SQL Server are given in the <i>vSphere Upgrade Guide</i>, “Preparing for the Upgrade to vCenter Server” chapter, “Prerequisites for the vCenter Server Upgrade” section, “Database Prerequisites” subsection. This document can be found here: <a href="http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_upgrade_guide.pdf">http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_upgrade_guide.pdf</a></p> <p>NOTE: This section indicates which privileges are needed for installation and upgrade, and which are needed just for ongoing operation.</p>

### vSphere Client Components

Although SSL-based encryption is used to protect communication between client components and vCenter Server or ESX/ESXi, the Linux versions of these components do not perform certificate validation. Therefore, even if you have replaced the self-signed certificates on vCenter and ESX/ESXi with legitimate certificates signed by your local root certificate authority or a third party,

## VMware vSphere 4.1 Security Hardening Guide

communications with Linux clients are still vulnerable to MiTM attacks. The components that are vulnerable when running on Linux include:

- Any vCLI command
- Any vSphere SDK for Perl script
- Virtual machine console access initiated from a Linux-based Web Access browser session
- Any program written using the vSphere SDK

The management interfaces of vCenter Server and ESX should be available only on trusted networks, but providing encryption and certificate validation add extra layers of defense against an attack. If you are able to militate against systems on the management network's interposing themselves on network traffic, or you can trust that such systems will not appear on the network, the use of Linux-based clients would not increase the security risk.

Operational Element	Description
<b>Code</b>	VCL01
<b>Name</b>	Restrict the use of Linux-based clients.
<b>Description</b>	Although SSL-based encryption is used to protect communication between client components and vCenter Server or ESX/ESXi, the Linux versions of these components do not perform certificate validation.
<b>Risk or Control</b>	<p>Even if you have replaced the self-signed certificates on vCenter and ESX/ESXi with legitimate certificates signed by your local root certificate authority or a third party, communications with Linux clients are still vulnerable to MiTM attacks.</p> <p>With proper controls, this restriction can be relaxed if deemed appropriate. These controls include:</p> <ul style="list-style-type: none"><li>- Restriction of management network access only to authorized systems</li><li>- Use of firewalls to restrict access to vCenter only by authorized hosts</li><li>- Use of jump-box systems for exclusive access to vCenter</li></ul>
<b>Recommendation Level</b>	DMZ
<b>Condition or Steps</b>	Options include:

## VMware vSphere 4.1 Security Hardening Guide

- Instruct administrators, especially those who have high levels of privileges, not to use Linux-based clients when connecting to vCenter Server.
- Make use of a jump-box architecture so that the only Linux clients are those behind the jump.

vCenter Server includes a vSphere Client extensibility framework, which provides the ability to extend the vSphere Client with menu selections or toolbar icons that provide access to vCenter add-on components or external, Web-based functionality. With the flexibility, customization and innovation that this entails, there is also the risk of introducing vSphere Client capabilities that were not intended. For example, a plug-in might be surreptitiously installed on an administrator's vSphere Client instance, and then might execute arbitrary commands with the privilege level of that administrator. If a user with low or no privileges were to use such a client, there would be no added risk, because the plug-in can only interact with vCenter or ESX/ESXi with the permissions of the user running the client.

The integrity of client software is a common concern across all client-server platforms in which the client might be running on an insecure host, but the vSphere Client extensibility framework reduces the effort needed to compromise the client software. To protect against such compromises, users of vSphere Client should not install any plug-ins that do not come from a trusted source. You can check to see which plug-ins are actually installed for a given vSphere Client by going to the menu item **Plug-ins > Manage Plug-ins** and clicking the **Installed Plug-ins** tab.

Operational Element	Description
<b>Code</b>	VCL02
<b>Name</b>	Verify the integrity of vSphere Client.
<b>Description</b>	vCenter Server includes a vSphere Client extensibility framework, which provides the ability to extend the vSphere Client with menu selections or toolbar icons that provide access to vCenter Server add-on components or external, Web-based functionality.
<b>Risk or Control</b>	vSphere Client extensions run at the same privilege level as the user logged in. A malicious extension might masquerade as something useful but then do harmful things such as stealing credentials or

	misconfiguring the system.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Make sure that the vSphere Client installation used by administrators includes only authorized extensions from trusted sources. You can check to see which plug-ins are actually installed for a given vSphere Client by going to the menu item <b>Plug-ins &gt; Manage Plug-ins</b> and clicking the <b>Installed Plug-ins</b> tab.

### vCenter Update Manager

vCenter includes a framework that enables you to add components to it that extend its functionality. These components typically run as separate services that are installed on a separate host or in a virtual machine. For the *VMware vSphere 4.1 Security Hardening Guide*, the only such component that is considered in-scope is VMware Update Manager. If you choose to make use of other add-on components, use the recommendations herein as a guide to how they should be deployed securely.

You should consider VMware Update Manager an essential component of any VMware infrastructure deployment. The ability to make sure that critical operating system patches are applied to all virtual machines, especially offline virtual machines and templates, addresses one of the most important aspects of security in a virtualized environment. Furthermore, the ability to automate the patching of ESX/ESXi hosts greatly increases the likelihood that you are protected against any vulnerability that might be discovered for this platform. Although there are numerous other ways to keep the virtual machine up to date with respect to patches, VMware Update Manager is the preferred way to keep the ESX/ESXi hosts patched.

In the default installation, the host where you install VMware Update Manager also needs access to the Internet to download patches and patch information. You can configure it to use a Web proxy, a step you should take if a Web proxy is available. For highest security, you can install the Update Manager Download Service on a separate server; the patches and information that it downloads can be transferred manually to the Update Manager host—for example, using a USB key or scheduled, secure file transfer. This prevents having the Update Manager host itself connected to an external network. For more information on installing Update Manager and the Update Manager Download Service, see the “Working with Update Manager” chapter in the *Update Manager Administration Guide*.

Configuration Element	Description
-----------------------	-------------



## VMware vSphere 4.1 Security Hardening Guide

<b>Code</b>	VUM01
<b>Name</b>	Use least privileges for the Update Manager database user.
<b>Description</b>	<p>Update Manager requires certain privileges on its database user in order to install, and the installer automatically checks for these. These are documented in the <i>VMware Update Manager Administration Guide</i>.</p> <p>However, after installation, only a small number of privileges are required for operation. The privileges on the VUM database user can be reduced during normal operation. These privileges should be added again if an upgrade or uninstall must be performed.</p>
<b>Risk or Control</b>	Least privileges mitigates attacks if the Update Manager database account is compromised.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>For Oracle: After installation, only the following permissions are needed for normal operation: <i>create session, create any table, drop any table</i>.</p> <p>For SQL Server: After installation, the <i>dba_owner</i> role or <i>sysadmin</i> role can be removed from the MSDB database (it is still required, however, for the Update Manager database).</p> <p>Please check the latest <i>VMware Update Manager Administration Guide</i> for any updates to these configurations.</p>

Operational Element	Description
<b>Code</b>	VUM02
<b>Name</b>	Keep Update Manager system properly patched.
<b>Description</b>	By staying up to date on Windows patches, vulnerabilities in the OS can be mitigated.
<b>Risk or Control</b>	If an attacker can obtain access and elevate privileges on the Update Manager system, it can compromise the patching process.

## VMware vSphere 4.1 Security Hardening Guide

<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Employ a system to keep the Update Manager system up to date with patches in accordance with industry-standard guidelines, or internal guidelines where appropriate.

Operational Element	Description
<b>Code</b>	VUM03
<b>Name</b>	Provide Windows system protection on the Update Manager system.
<b>Description</b>	By providing OS-level protection, vulnerabilities in the OS can be mitigated.
<b>Risk or Control</b>	If an attacker can obtain access and elevate privileges on the Update Manager system, it can compromise the patching process.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Provide Windows system protection, such as antivirus, in accordance with industry-standard guidelines, or internal guidelines where appropriate.

Operational Element	Description
<b>Code</b>	VUM04
<b>Name</b>	Avoid user login to Update Manager system.
<b>Description</b>	After someone has logged in to the Update Manager system, it becomes more difficult to prevent what they can do. In general, logging in to the Update Manager system should be limited to very privileged administrators, and then only for the purpose of administering Update Manager or the host OS.
<b>Risk or Control</b>	Anyone logged in to the Update Manager can potentially cause harm, either intentionally or

## VMware vSphere 4.1 Security Hardening Guide

	unintentionally, by altering settings and modifying processes.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Restrict login to the Update Manager to only those personnel who have legitimate tasks to perform in it. Ensure that they log in only when necessary, and audit these events.

Configuration Element	Description
<b>Code</b>	VUM05
<b>Name</b>	Do not configure Update Manager to manage its own VM or the VM of its vCenter Server.
<b>Description</b>	Although you can install both Update Manager and vCenter Server on VMs and place them on the same ESX/ESXi host, you should not configure Update Manager to manage the patches on those VMs.
<b>Risk or Control</b>	Upon scanning and remediation, the virtual machine on which Update Manager and vCenter Server are installed can reboot and the whole deployment system will shut down.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	If installed in virtual machines, ensure that Update Manager does not manage the patching of the VM on which it runs, nor the VM on which the associated vCenter Server runs.

Configuration Element	Description
<b>Code</b>	VUM06
<b>Name</b>	Do not use default self-signed certificates.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	Self-signed certificates are automatically generated by Update Manager during the installation process, are not signed by a commercial CA, and might not provide strong security. Replace default self-signed certificates with those from a trusted certification authority, either a commercial CA or an organizational CA.
<b>Risk or Control</b>	The use of default certificates leaves the SSL connection open to MiTM attacks. Changing the default certificates to trusted CA-signed certificates mitigates the potential for MiTM attacks.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	For instructions on how to change self-signed certificates on Update Manager, please see the following KB article: <a href="http://kb.vmware.com/kb/1023011">http://kb.vmware.com/kb/1023011</a>

Update Manager has three main architectures for obtaining and registering patches:

- 1) Direct download onto the Update Manager system
- 2) Download onto a separate system and then network-based transfer via a Web server – this is referred to as a “semi-air-gap” model
- 3) Download onto a separate system, and then physical transfer via portable media – this is referred to as an “air-gap” model

Both the semi-air-gap and air-gap models make use of the Download Service, which is a component that is installed on a separate, standalone system. It connects to public repositories, and downloads the patches. From that point, how the patches are transferred to the Update Manager system depends on the model being used.

For information on how to set up these alternatives, refer to the *VMware vCenter Update Manager Administration Guide*, in the “Installing, Setting Up, and Using Update Manager Download Service” chapter; as well as in the “Configuring Update Manager” chapter, “Configuring Update Manager Patch Download Sources” section.

Configuration Element	Description
-----------------------	-------------

## VMware vSphere 4.1 Security Hardening Guide

<b>Code</b>	VUM10		
<b>Name</b>	Limit the connectivity between Update Manager and public patch repositories.		
<b>Description</b>	In a typical deployment, Update Manager connects to public patch repositories on the Internet to download patches. This connection should be limited as much as possible to prevent access from the outside to the Update Manager system.		
<b>Risk or Control</b>	Any channel to the Internet represents a threat.		
<b>Recommendation Level</b>	Enterprise	DMZ	SSLF
<b>Parameters or Objects Configuration</b>	Configure a Web proxy for Update Manager, rather than directly connecting to the Internet.	Configure Update Manager to use the Download Service, and configure a Web server to transfer the files to the Update Manager server (semi-air-gap model).	Configure Update Manager to use the Download Service, and use physical media to transfer the files to the Update Manager server (air-gap model).
<b>Test</b>	Check the proxy settings for Update Manager to make sure they are correct. Refer to the guide in the “Configuring Update Manager” chapter in the “Configure Update Manager Proxy Settings” section.	Ensure that the Download Service is functioning and that the Update Manager server does not obtain patches directly from the Internet.	Ensure that the Download Service is functioning and that the Update Manager server does not obtain patches directly from the Internet.

## Console Operating System (COS)

### Console Network Protection

ESX includes a built-in firewall between the service console and the network. To ensure the integrity of the service console, VMware has limited the number of firewall ports that are open by default. At installation time, the service console firewall is configured to block all incoming and outgoing traffic except for ports 902, 443, 80, and 22, which are used for basic communication with ESX. This setting enforces a high level of security for the ESX host. Medium security blocks all incoming traffic except on the default ports (902, 443, 80, and 22) and any ports users specifically open. Outgoing traffic is not blocked. Low security does not block either incoming or outgoing traffic. This setting is equivalent to removing the firewall. Because the ports open by default on the ESX are strictly limited, additional ports might need to be open after installation for third-party applications such as management, storage, NTP, and so on. For instance, a backup agent might use specific ports such as 13720, 13724, 13782, and 13783.

The list of ports used by ESX can be found in this VMware Knowledge Base article: <http://kb.vmware.com/kb/1012382>.

Configuration Element	Description
<b>Code Number</b>	CON01
<b>Name</b>	Ensure that ESX firewall is configured to high security.
<b>Description</b>	ESX Server includes a built-in firewall between the service console and the network. A high-security setting disables all outbound traffic and allows only selected inbound traffic.
<b>Risk or Control</b>	Prevention of network-based exploits.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	The following commands configure high security on the firewall:  <pre>esxcfg-firewall --blockIncoming esxcfg-firewall --blockOutgoing</pre>
<b>Test</b>	Ensure that outbound connections are blocked and only selected inbound connections are allowed.

## VMware vSphere 4.1 Security Hardening Guide

Configuration Element	Description
<b>Code Number</b>	CON02
<b>Name</b>	Limit network access to applications and services
<b>Description</b>	<p>As a security best practice, disabling and removing services and applications that aren't required is advisable. The ESX service console, by default, has a number of available services that should be disabled unless required for business. Also, ensure limited use of external software within the service console. Examples of additional software that might be acceptable to run in the service console are management and backup agents.</p> <p>For more information and recommendations on running third-party software in the service console, see <a href="http://www.vmware.com/vmtn/resources/516">http://www.vmware.com/vmtn/resources/516</a>.</p>
<b>Risk or Control</b>	Prevention of network-based exploits
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	All services not required explicitly for business purposes should be disabled.
<b>Test</b>	Run the "esxcfg-firewall -query" command to determine what services are enabled. To disable a service, execute the "esxcfg-firewall -d <service name>" command.

Parameter Element	Description
<b>Code Number</b>	CON03
<b>Name</b>	Do not run NFS or NIS clients in the service console.
<b>Description</b>	<p>Because of the standards for how NFS and NIS are implemented, enabling the NFS or NIS client service in the service console opens up outbound UDP and TCP ports 0-65535; that is, it unblocks <b>all</b> outbound IPv4 connections.</p> <p>NOTE: Some implementations of NFS allow the server to configure specific ports for communication. These can then be selectively opened on the service console firewall, but not through the built-in services configuration.</p>

<b>Risk or Control</b>	Turning on these services effectively disables the service console firewall for outbound connections.
<b>Recommendation Level</b>	Enterprise
<b>Parameters Setting</b>	Run the “esxcfg-firewall –query” command to determine whether nfsClient or nisClient are enabled. To disable a service, execute the “esxcfg-firewall –d <service name>” command.

## Console Management

Although the ESX service console is derived from Red Hat Linux, it is a unique operating platform that should not be managed as a true Linux host. As such, the service console should be managed according to VMware and other virtualization security best practices, which might differ from many well-known Linux-focused best practices in some ways.

If you follow the best practice of isolating the network for the service console, there is no reason to run any antivirus or other such security agents, and their use is not necessarily recommended. However, if your environment requires that such agents be used, use a version designed to run on Red Hat Enterprise Linux 5.

Operational Element	Description
<b>Code Number</b>	COM01
<b>Name</b>	Do not apply Red Hat patches to the service console.
<b>Description</b>	Although the ESX service console is derived from Red Hat Linux, it is important that you not treat it like a Linux host when it comes to patching. Never apply patches issued by Red Hat or any other third-party vendor.
<b>Risk or Control</b>	The service console is generated from a Red Hat Linux distribution that has been modified to provide exactly the functionality necessary to communicate with and allow management of the VMkernel. Any additional software installed should not depend upon the presence of the standard set of RPM packages. In several cases, the packages that do exist have been modified especially for ESX.
<b>Recommendation Level</b>	Enterprise



## VMware vSphere 4.1 Security Hardening Guide

<b>Condition or Steps</b>	Apply only patches that are published by VMware specifically for the versions of ESX that you have in use. These are published for download periodically, as well as on an as-needed basis for security fixes. You can receive notifications for security-related patches by signing up for email notifications at <a href="http://www.vmware.com/security">http://www.vmware.com/security</a> .
---------------------------	--

Operational Element	Description
<b>Code Number</b>	COM02
<b>Name</b>	Do not rely upon tools that check only for Red Hat patches.
<b>Description</b>	You should never use a scanner to analyze the security of the service console unless the scanner is specifically designed to work with your version of ESX.
<b>Risk or Control</b>	Scanners that assume that the service console is a standard Red Hat Linux distribution routinely yield false positives. These scanners typically look only for strings in the names of software; they therefore do not account for the fact that VMware releases custom versions of packages with special names when providing security fixes. Because these special names are unknown to the scanners, they are flagged as vulnerabilities when in reality they are not.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	You should use only scanners that specifically treat the ESX service console as a unique target. For more information, see the “Security Patches and Security Vulnerability Scanning Software” section in the “Service Console Security” chapter of the <i>ESX Server 4 Configuration Guide</i> .

Operational Element	Description
<b>Code Number</b>	COM03
<b>Name</b>	Do not manage the service console as a Red Hat Linux host.
<b>Description</b>	The usual redhat-config-* commands are not present, nor

## VMware vSphere 4.1 Security Hardening Guide

	are other components such as the X server.
<b>Risk or Control</b>	Attempts to manage the service console as a typical Red Hat Linux host might result in misconfigurations that affect security, including availability.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	Manage the service console using purpose-built commands, such as vmkfstools and the esxcfg-* commands, to the extent possible, and only use other built-in commands as necessary. Do not deploy additional packages for management unless absolutely needed for a specific purpose.

Operational Element	Description
<b>Code Number</b>	COM04
<b>Name</b>	Use vSphere Client and vCenter Server to administer the hosts instead of service console.
<b>Description</b>	The best measure to prevent security incidents in the service console is to avoid accessing it if at all possible. You can perform many of the tasks necessary to configure and maintain the ESX host using the vSphere Client, either connected directly to the host or, better yet, going through vCenter Server. Another alternative is to use a remote scripting interface, such as vCLI or PowerCLI. These interfaces are built on the same API that vSphere Client and vCenter Server use, so any script using them automatically enjoys the same benefits of authentication, authorization and auditing.
<b>Risk or Control</b>	By using alternatives to the service console, the need to access it is reduced, thereby minimizing the risk due to misuse.
<b>Recommendation Level</b>	Enterprise
<b>Condition or Steps</b>	<p>Security policies and processes should be written that require the use of the remote API-based tools wherever possible. Accounts with direct service console access should be limited to the minimum number of administrators possible.</p> <p>Some advanced tasks, such as initial configuration for password policies, cannot be performed via the vSphere</p>

## VMware vSphere 4.1 Security Hardening Guide

Client. For these tasks, you must log in to the service console. Also, if you lose your connection to the host, executing certain of these commands through the command line interface might be your only recourse—for example, if the network connection fails and you are therefore unable to connect using vSphere Client.

### Console Password Policies

Configuration Element	Description
<b>Code Number</b>	COP01
<b>Name</b>	Use a directory service for authentication.
<b>Description</b>	<p>Advanced configuration and troubleshooting of an ESX host might require local privileged access to the service console. For these tasks, you should set up individual host-localized user accounts and groups for the few administrators with overall responsibility for your virtual infrastructure. Ideally, these accounts should correspond to real individuals and not be accounts shared by multiple persons. Although you can create on the service console of each host local accounts that correspond to each global account, this presents the problem of having to manage user names and passwords in multiple places. It is much better to use a directory service, such as NIS or LDAP, to define and authenticate users on the service console, so you do not have to create local user accounts.</p> <p>If an organization does not rely upon the service console for configuration and routine operations, or if the number of individuals who are allowed to access the service console is small, the maintenance of local accounts will not present too large an overhead. In this case, a directory service might not be necessary. This decision should be dictated by local security policies.</p>
<b>Risk or Control</b>	Centralized control of user authentication greatly reduces the chance of misconfiguration or inappropriate access.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	Please see the <i>ESX Configuration Guide</i> , Chapter 13 “Authentication and User Management” for information on how to configure Active Directory for authentication. ( <a href="http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf">http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esx_server_config.pdf</a> )

Configuration Element	Description
<b>Code Number</b>	COP02
<b>Name</b>	Establish a password policy for password complexity.
<b>Description</b>	<p>These controls ensure that users create passwords that are hard for password generators to determine. Instead of using words, a common technique for ensuring password complexity is to use a memorable phrase, then derive a password from it—for example, by using the first letter of each word.</p> <p>The default pam_cracklib.so plug-in provides sufficient password strength enforcement for most environments. However, if the pam_cracklib.so plug-in is not stringent enough for your needs, you can change the parameters used for the pam_cracklib.so plug-in or use the pam_passwdqc.so plug-in instead. You can change the plug-in by using the esxcfg-auth-usepamqc command.</p>
<b>Risk or Control</b>	This recommendation addresses the risk of passwords being guessed or cracked.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	<p><b>esxcfg-auth --usepamqc</b></p> <p>This command requires six parameters in the following order:</p> <ul style="list-style-type: none"> <li>- Minimum length of a single character class password</li> <li>- Minimum length of a password that has characters from two character classes</li> <li>- Minimum number of words in a passphrase</li> <li>- Minimum length of a password that has characters from three character classes</li> <li>- Minimum length of a password that has characters from four character classes</li> <li>- Maximum number of characters reused from the previous password</li> </ul> <p>If you pass a value of -1 for any of the six parameters, it disables that option.</p> <p>For example, the command line</p> <p><b>esxcfg-auth --usepamqc=-1 -1 -1 12 8 -1</b></p> <p>disables the first three parameters, requires a 12-character password using characters from three character classes or an 8-character password that uses characters from four character</p>

## VMware vSphere 4.1 Security Hardening Guide

	classes and disables the final parameter.
<b>Test</b>	<p>Check the following line in the <code>/etc/pam.d/system-auth-generic</code> file:</p> <p><b>“password required /lib/security/\$ISA/pam_passwdqc.so”</b>:          if no text string is displayed, the complexity is not set. If there is a text string at the end of this line, ensure that it meets your policy.</p>

Configuration Element	Description
<b>Code Number</b>	COP03
<b>Name</b>	Establish a password policy for password history.
<b>Description</b>	Keeping a password history mitigates the risk of a user reusing a previously used password too often.
<b>Risk or Control</b>	This recommendation addresses the risk of passwords being guessed or cracked.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	<p>If it does not already exist, create a password history file:</p> <pre>touch /etc/security/opasswd</pre> <pre>chmod 600 /etc/security /opasswd</pre> <p>Set the number of passwords to retain for matching:</p> <p>Edit the <code>/etc/pam.d/system-auth</code> file and add the string “remember=x” to the end of the following line, where x is the number of passwords to retain:</p> <p><b>“password sufficient /lib/security/\$ISA/pam_unix.so”</b></p>
<b>Test</b>	Check for the presence of the string “remember=” and ensure that the value is in compliance with your internal policy.

Configuration Element	Description
<b>Code Number</b>	COP04
<b>Name</b>	Establish a maximum password aging policy.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	These controls govern how long a user password can be active before the user is required to change it.
<b>Risk or Control</b>	They help ensure that passwords change often enough that if an attacker obtains a password through sniffing or social engineering, the attacker cannot continue to access the ESX host indefinitely.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	To set the maximum password age, use the following command:  <b>esxcfg-auth --passmaxdays=n</b>  where n is the maximum number of days for a password to live.
<b>Test</b>	Run the following command to see what the password maximum life setting is set to:  <b>grep -i max_days /etc/login.defs</b>  This number should be compared to your policy.

<b>Configuration Element</b>	<b>Description</b>
<b>Code Number</b>	COP05
<b>Name</b>	Establish a password policy for minimum days before a password is changed.
<b>Description</b>	Because the maximum number of days for a password to live is important, there also must be a minimum number of days as well. This will mitigate the risk of a user's changing a password enough times to enable the reuse of their favorite password, which is outside of the password reuse policy.
<b>Risk or Control</b>	This recommendation addresses the risk of passwords being guessed or cracked.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	<b>esxcfg-auth --passmindays=n</b>
<b>Test</b>	Run the following command to check the setting for password minimum life:  "grep -i min_days /etc/login.defs"

This number should be compared to your policy.

## Console Logging

Proper and thorough logging enables you to keep track of any unusual activity that might be a precursor to an attack. It also allows you to do a postmortem on any compromised systems and learn how to prevent attacks from occurring in the future.

The syslog daemon performs the system logging in ESX. You can access the log files in the service console by going to the `/var/log/` directory. Several types of log files generated by ESX are shown in the following table.

Component	Location	Purpose
VMkernel	<code>/var/log/vmkernel</code>	Records activities related to the virtual machines and ESX
VMkernel warnings	<code>/var/log/vmkwarning</code>	Records activities with the virtual machines
VMkernel summary	<code>/var/log/vmksummary</code>	Used to determine uptime and availability statistics for ESX; comma separated
VMkernel summary human readable	<code>/var/log/vmksummary.txt</code>	Used to determine uptime and availability statistics for ESX; human-readable summary
ESX host agent log	<code>/var/log/vmware/hostd.log</code>	Contains information on the agent that manages and configures the ESX host and its virtual machines
vCenter agent	<code>/var/log/vmware/vpx/vpxa.log</code>	Contains information on the agent that communicates with vCenter
Web access	Log all the files in the directory <code>/var/log/vmware/webAccess</code> /*.log: client.log, proxy.log, unitTest.log, viewhelper.log, objectMonitor.log, timer.log,	Records information on Web-based access to ESX (service <code>vmware-webAccess</code> start on ESX host to enable this)

## VMware vSphere 4.1 Security Hardening Guide

	updateThread.log	
Authentication log	/var/log/secure	Contains records of connections that require authentication, such as VMware daemons and actions initiated by the xinetd.
Service Console	/var/log/messages	Contain all general log messages used to troubleshoot virtual machines or ESX
Virtual machines	The same directory as the affected virtual machine's configuration files; named vmware.log and vmware-*.log, e.g.  /vmfs/volumes/<datastore> /<virtual machine>/vmware.log	Contains Virtual Machine Power Events, system crashes, Tools status and activity, Time Sync, Virtual Hardware changes, vMotion Migrations, Machine Clones, etc.

The log files provide an important tool for diagnosing security breaches as well as other system issues. They also provide key sources of audit information. In addition to storing log information in files on the local file system, you can send this log information to a remote system. The syslog program is typically used for computer system management and security auditing, and it can serve these purposes well for ESX hosts. You can select individual service console components for which you want the logs sent to a remote system.

Configuration Element	Description
Code Number	COL01
Name	Configure syslog logging.
Description	Remote logging to a central host provides a way to greatly increase administration capabilities. By gathering log files onto a central host, you can easily monitor all hosts with a single tool as well as do aggregate analysis and searching to look for such things as coordinated attacks on multiple hosts.
Risk or Control	Logging to a secure, centralized log server can help prevent log tampering and provides a long-term audit record.
Recommendation Level	Enterprise



## VMware vSphere 4.1 Security Hardening Guide

<b>Parameters or Objects Configuration</b>	<p>Syslog behavior is controlled by the configuration file <code>/etc/syslog.conf</code>. For logs you want to send to a remote log host, add a line with <code>@&lt;loghost.company.com&gt;</code> after the message type, where <code>&lt;loghost.company.com&gt;</code> is the name of a host configured to record remote log files. Make sure that this host name can be properly resolved, putting an entry in the name service maps if needed.</p> <p>Example:</p> <pre>local6.warning @&lt;loghost.company.com&gt;</pre> <p>After modifying the file, tell the syslog daemon to reread it by issuing the following command:</p> <pre>kill -SIGHUP `cat /var/run/syslogd.pid`</pre> <p>At a minimum, the following files should be logged to a remote syslog server:</p> <pre>/var/log/vmkernel /var/log/secure /var/log/messages /var/log/vmware/*.log /var/log/vmware/vpx/vpxa.log</pre>
<b>Test</b>	<p>To check that remote logging is configured:</p> <pre>cat /etc/syslog.conf   grep @</pre> <p>To check that remote logging traffic is permitted outbound from the host:</p> <pre>esxcfg-firewall -q   grep 514</pre> <p>To check that syslog service is configured to run:</p> <pre>chkconfig -list   grep syslog</pre>

Configuration Element	Description
Code Number	COL02
Name	Configure NTP time synchronization.
Description	By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC), you can make it simpler to track and correlate an

## VMware vSphere 4.1 Security Hardening Guide

	intruder's actions when reviewing the relevant log files.
<b>Risk or Control</b>	Incorrect time settings might make it difficult to inspect and correlate log files to detect attacks and would make auditing inaccurate.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	NTP can be configured on an ESX host using the vSphere Client, or using a remote command line such as vCLI or PowerCLI.
<b>Test</b>	<ul style="list-style-type: none"> <li>• Query the NTP configuration to make sure that a valid time source has been configured</li> <li>• Make sure that the NTP service is running on the host</li> </ul>

### Console Hardening

Configuration Element	Description
<b>Code Number</b>	COH01
<b>Name</b>	Partition the disk to prevent the root file system from filling up.
<b>Description</b>	<p>If the root file system fills up, it can seriously degrade the performance of ESX management capabilities or even make them unresponsive.</p> <p>When you install ESX 4.1, the default partitioning creates only three partitions. To protect against the root file system's filling up, you can create additional separate partitions for the directories /home, /tmp, and /var/log. These are all directories that have the potential to fill up, and if they are not isolated from the root partition, you might experience a denial of service if the root partition is full and unable to accept any more writes. The ESX Partitioning" chapter in the <i>ESX and vCenter Server Installation Guide</i> covers disk partitions in more detail:</p> <p><a href="http://pubs.vmware.com/vsphere-esx-4-1/install_guide/c_esx_partitioning.html">http://pubs.vmware.com/vsphere-esx-4-1/install_guide/c_esx_partitioning.html</a></p>
<b>Risk or Control</b>	Prevents a denial of service against the management of that host.
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	/etc/fstab

## VMware vSphere 4.1 Security Hardening Guide

<b>Test</b>	Run the “df” command and ensure that the directories for /home, /tmp, and /var/log are mounted on their own partitions.
-------------	---

The service console has a number of files that specify its configurations. Editing of these files can result in significant configuration changes, including possibly changes that can open the host to attack or exploitation. Most of these files are not normally edited by hand, although in some cases this might be necessary. The following is a list of service console configuration files that are particularly important.

- /etc/profile
- /etc/ssh/sshd\_config
- /etc/pam.d/system-auth
- /etc/grub.conf
- /etc/krb.conf
- /etc/krb5.conf
- /etc/krb.realms
- /etc/login.defs
- /etc/openldap/ldap.conf
- /etc/nscd.conf
- /etc/ntp
- /etc/ntp.conf
- /etc/passwd
- /etc/group
- /etc/nsswitch.conf
- /etc/resolv.conf
- /etc/sudoers
- /etc/shadow

In addition, ESX configuration files located in the /etc/vmware directory store all the VMkernel information.

Operational Element	Description
Code Number	COH03
Name	Establish and maintain file system integrity.

## VMware vSphere 4.1 Security Hardening Guide

<b>Description</b>	It is essential to monitor the integrity of certain critical system files within the ESX service console. In addition, the permissions of numerous critical files should be configured to prevent unnecessary access from occurring.
<b>Risk or Control</b>	Direct tampering with configuration files could result in undetectable changes.
<b>Recommendation Level</b>	DMZ
<b>Condition or Steps</b>	Configuration files, especially those listed, should be monitored for integrity and unauthorized tampering, using a commercial tool such as Tripwire, or by using a checksum tool such as sha1sum, which is included in the service console. These files should also be backed up regularly, either by using backup agents or by doing backups based on file copying.

<b>Configuration Element</b>	<b>Description</b>
<b>Code Number</b>	COH04
<b>Name</b>	Ensure that permissions of important files and utility commands have not been changed from default.
<b>Description</b>	Various files and utilities are installed with particular file permissions to enable certain functionality without requiring unnecessary privilege levels for the user accessing them.
<b>Risk or Control</b>	Changing permissions from default on these important files can have an effect on the functionality of the ESX host and might potentially cause these commands to not run properly and, as such, cause a denial of service.
<b>Recommendation Level</b>	DMZ
<b>Parameters or Objects Configuration</b>	<p>The <code>/usr/sbin/esxcfg-*</code> commands, which are all installed by default with permissions 555.</p> <p>The log files discussed in the previous section, all of which have permissions 600, except for the directory <code>/var/log/vmware/webAccess</code>, which has permissions 755, and the virtual machine log files, which have permissions 644.</p> <p>Certain system commands that have the SUID bit. These commands are listed here:</p>

## VMware vSphere 4.1 Security Hardening Guide

[http://pubs.vmware.com/vsphere-esx-4-1/server\\_config/r\\_default\\_setuid\\_applications.html](http://pubs.vmware.com/vsphere-esx-4-1/server_config/r_default_setuid_applications.html)

For all of these files, the user and group owner should be root.

### Console Access

Parameter Element	Description
Code Number	COA01
Name	Prevent tampering at boot time.
Description	A grub password can be used to prevent users from booting into single-user mode or passing options to the kernel during boot.
Threat	By passing in boot parameters, it might be possible to influence the host so that it behaves improperly, perhaps in a manner that is hard to detect.
Recommendation Level	DMZ
Parameter Setting	During the ESX installation, the advanced option allows you to set a grub password. This can also be set by directly editing <code>/boot/grub/grub.conf</code> . See the “Installing VMware ESX” chapter in the <i>ESX and vCenter Server Installation Guide</i> for more details.
Effect on Functionality	Unless the password is entered, the server boots only the kernel with the default options.

Parameter Element	Description
Code Number	COA02
Name	Require authentication for single-user mode.
Description	Anyone with physical access can access the service console as root if a password is not set for single-user mode access.
Threat	When this recommendation is followed, if an attacker gains access to the console, they can log in only as an ordinary user and won't necessarily be able to escalate privilege level without additional effort.

## VMware vSphere 4.1 Security Hardening Guide

<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	Add the line ~~:S:wait:/sbin/sulogin to /etc/inittab
<b>Effect on Functionality</b>	If the root password is lost, there will be no way to access the system.

Parameter Element	Description
<b>Code Number</b>	COA03
<b>Name</b>	Ensure that root access via SSH is disabled.
<b>Description</b>	Because the root user of the service console has almost unlimited capabilities, securing this account is the most important step you can take to secure the ESX host. By default, all insecure protocols, such as FTP, Telnet, and HTTP, are disabled. Remote access via SSH is enabled, but not for the root account.
<b>Threat</b>	By allowing root access via SSH, the ability to audit who is executing commands or performing tasks is negated. It is preferable to require users to log in to the system using their own account, and then elevate privileges to perform tasks that require this, using "su" or "sudo."
<b>Recommendation Level</b>	Enterprise
<b>Parameter Setting</b>	The line "PermitRootLogin" in the /etc/sshd_conf should be set to "no."
<b>Effect on Functionality</b>	The root user will not be able to log in via SSH.

Parameter Element	Description
<b>Code Number</b>	COA04
<b>Name</b>	Disallow console root login.
<b>Description</b>	You can disallow root access, even on the console of the ESX host—that is, when you log in using a screen and keyboard attached to the server itself, or to a remote session attached to the server's console. This approach forces

## VMware vSphere 4.1 Security Hardening Guide

	<p>anyone who wants to access the system to first log in using a regular user account, then use sudo or su to perform tasks.</p> <p>The net effect is that administrators can continue to access the system, but they never have to log in as root. Instead, they use sudo to perform particular tasks or su to perform arbitrary commands.</p>
<b>Threat</b>	When this recommendation is followed, if an attacker gains access to the console, they can log in only as an ordinary user and won't necessarily be able to escalate privilege level without additional effort.
<b>Recommendation Level</b>	SSLF
<b>Parameter Setting</b>	<p>To prevent direct root login on the console, modify the file <code>/etc/securetty</code> to be empty. While logged in as root, enter the following command:</p> <pre>cat /dev/null &gt; /etc/securetty</pre> <p>You should first create a nonprivileged account on the host to enable logins; otherwise, you might find yourself locked out of the host. This nonprivileged account should be a local account—that is, one that does not require remote authentication—so that if the network connection to the directory service is lost, access to the host is still possible. You can ensure this access by defining a local password for this account, using the <code>passwd</code> command.</p>
<b>Effect on Functionality</b>	After you do this, only nonprivileged accounts will be allowed to log in at the console. Root login at the console will no longer be possible.

Configuration Element	Description
<b>Code Number</b>	COA05
<b>Name</b>	Limit access to the su command.
<b>Description</b>	Because su is such a powerful command, you should limit access to it. By default, only users who are members of the wheel group in the service console have permission to run su. If a user attempts to run su - to gain root privileges and that user is not a member of the wheel group, the su - attempt fails and the event is logged.
<b>Threat</b>	

<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	<p>Besides controlling who has access to the su command, through the pluggable authentication module (PAM) infrastructure, you can specify what type of authentication is required to successfully execute the command. In the case of the su command, the relevant PAM configuration file is <code>/etc/pam.d/su</code>. To allow only members of the wheel group to execute the su command, and then only after authenticating with a password, find the line beginning with <code>auth required</code> and remove the leading pound sign (<code>#</code>) so it reads:</p> <pre>auth required /lib/security/\$ISA/pam_wheel.so use_uid</pre>

The sudo utility should be used to control which privileged commands users can run while logged in to the service console. Among the commands you should regulate are all of the `esxcfg-*` commands as well as those that configure networking and other hardware on the ESX host. You should decide which set of commands should be available to more junior administrators and which commands you should allow only senior administrators to execute. You can also use sudo to restrict access to the su command.

Use the following tips to help you configure sudo:

- Configure local and remote sudo logging (see “Maintain Proper Logging” on page 12).
- Create a special group, such as `vi_admins`, and allow only members of that group to use sudo.
- Use sudo aliases to determine the authorization scheme, then add and remove users in the alias definitions instead of in the commands specification.
- Be careful to permit only the minimum necessary operations to each user and alias. Permit very few users to run the su command, because su opens a shell that has full root privileges but is not auditable.
- If you have configured authentication using a directory service, sudo uses it by default for its own authentication. This behavior is controlled by the `/etc/pam.d/sudo` file, on the line for `auth`. The default setting—`service=system-auth`—tells sudo to use whatever authentication scheme has been set globally using the `esxcfg-auth` command.
- Require users to enter their own passwords when performing operations. This is the default setting. Do not require the root password, because this presents a security risk, and do not disable password checking. In sudo, the authentication persists for a brief period of time before sudo asks for a password again.

For further information and guidelines for using sudo, see <http://www.gratisoft.us/sudo/>.



## VMware vSphere 4.1 Security Hardening Guide

Configuration Element	Description
<b>Code Number</b>	COA06
<b>Name</b>	Configure and use sudo to control administrative access.
<b>Description</b>	The sudo utility should be used to control which privileged commands users can run while logged in to the service console.
<b>Risk or Control</b>	
<b>Recommendation Level</b>	Enterprise
<b>Parameters or Objects Configuration</b>	Parameters to be configured are in the <code>/etc/sudoers</code> file. Among the commands you should regulate are all of the <code>esxcfg-*</code> commands as well as those that configure networking and other hardware on the ESX host. You should decide which set of commands should be available to more junior administrators and which commands you should allow only senior administrators to execute. You can also use sudo to restrict access to the <code>su</code> command. Because each situation will be different, each configuration will be different, so no specific guidance can be given here.
<b>Test</b>	Check the configuration in the <code>/etc/sudoers</code> file and ensure that it meets your policy.