VMware vSphere™ 4.0 Security Hardening Guide

May 2010

vmware®

Table of Contents

VMware vSphere Hardening Guide Introduction

Scope

This set of documents provides guidance on how to securely deploy VMware® vSphere™ 4.0 (“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

NOTE: 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 data, 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.

- **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. 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: Virtual machine (vmx) parameters
- VMP: General virtual machine protection

VMware 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

VMware vNetwork (Virtual Networking)

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

VMware 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.
Threat	Description of the specific threat exposed by this feature. Include characterization of vulnerability.
Recommendation Level	<See recommendation-level descriptions>.
Parameter Setting	Where the parameter is defined, and what the recommended or not recommended values are. Also indicates 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).
Effect on Functionality	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:

PARAMETER ELEMENT	DESCRIPTION
Code	VMX01
Name	Prevent virtual disk shrinking.
Description	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.
Threat	Repeated disk shrinking can make virtual disk unavailable. Capability is available to nonadministrative users in the guest.
Recommendation Level	Enterprise

Parameter Setting	isolation.tools.diskWiper.disable=TRUE
	isolation.tools.diskShrink.disable=TRUE

Effect on Functionality	

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

Example:

CONFIGURATION ELEMENT	DESCRIPTION	
Code	NAR02	
Name	Ensure that VMotion™ traffic is isolated.	
Description	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.	
Risk or Control	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.	
Recommendation Level	Enterprise.	SSLF
Parameters or Objects Configuration	VMotion port group should be in a dedicated VLAN on a common virtual switch (vSwitch). The vSwitch can be shared with production (virtual machine) traffic, as long as the VMotion port group's VLAN is not used by production virtual machines.	VMotion port group should be on a management-only vSwitch.
Effect on Functionality		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.
Test	• Check for usage of VLAN ID on non-VMotion port groups. • Check that VLAN is isolated and not routed in the physical network.	In addition to Enterprise tests: • Check that VMotion port group vSwitch does not contain any nonmanagement port groups. • Check that the physical network is not accessed by any other nonmanagement 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
Code	Code String
Name	Short name of guideline.
Description	Description of the operational pattern or condition.
Risk or Control	Description of the risk being mitigated.
Recommendation Level	<See recommendation level descriptions>.
Condition or Steps	Concise description of the specific conditions to meet or avoid, and/or the steps needed to achieve this.

Here is an example:

CONFIGURATION ELEMENT	DESCRIPTION
Code	HCM01
Name	Do not use default self-signed certificates for ESX/ESXi communication.
Description	Replace default self-signed certificates with those from a trusted certification authority (CA), either a commercial CA or an organizational CA.
Risk or Control	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.
Recommendation Level	Enterprise
Parameters or objects configuration	Information on how to replace default self-signed certificates can be found in both the *ESXi Configuration Guide* and the *ESX Configuration Guide*, "Security" chapter, "Authentication and User Management" sections, "Encryption and Security Certificates for ESX/ESXi" subsection. This section covers the following advanced customization options: • Configuring SSL timeouts • Configuration for certificates in nondefault locations The two guides can be found at these URLs: • http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_esxi_server_config.pdf • http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_esx_server_config.pdf
Test	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 performance 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
Code	VMX01
Name	Prevent virtual disk shrinking.
Description	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.
Threat	Repeated disk shrinking can make a virtual disk unavailable. Capability is available to nonadministrative users in the guest.
Recommendation Level	Enterprise

Parameter Setting	isolation.tools.diskWiper.disable=TRUE
	isolation.tools.diskShrink.disable=TRUE

Effect on Functionality	

PARAMETER ELEMENT	DESCRIPTION
Code	VMX02
Name	Prevent other users from spying on administrator remote consoles.
Description	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.
Threat	If an administrator in the virtual machine logs in using a VMware remote console during their session, a nonadministrator in the virtual machine might connect to the console and observe the administrator's actions. This could also result in an administrator's 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.
Recommendation Level	DMZ
Parameter Setting	RemoteDisplay.maxConnections=1
Effect on Functionality	Only one remote console connection to the virtual machine will be permitted. Other attempts will be rejected until the first session disconnects.

PARAMETER ELEMENT	DESCRIPTION
Code	VMX03
Name	Disable copy/paste to remote console.

Description	When VMware Tools runs in a virtual machine, by default you can copy and paste between the guest operating system and the computer where the remote console is running. As soon as the console window gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard for the virtual machine console. It is recommended that you disable copy-and-paste operations for the guest operating system.
Threat	If a user copies sensitive information to the clipboard before using the console, the user—perhaps unknowingly—exposes sensitive data to the virtual machine.
Recommendation Level	Enterprise

Parameter Setting	isolation.tools.copy.disable=TRUE
	isolation.tools.paste.disable=TRUE
	isolation.tools.dnd.disable=TRUE
	isolation.tools.setGUIOptions.enable=FALSE

Effect on Functionality	Copy-and-paste to/from remote console will not work.

Virtual Devices

PARAMETER ELEMENT	DESCRIPTION
Code	VMX10
Name	Ensure that unauthorized devices are not connected.
Description	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. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE. 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.
Threat	Any enabled or connected device represents another potential attack channel.
Recommendation Level	Enterprise
Parameter Setting	The following parameters should NOT be present unless the device is required: 1. Floppy drives: floppyX.present 2. Serial ports: serialX.present 3. Parallel ports: parallelX.present 4. USB controller: usb.present 5. CD-ROM: ideX:Y.present
Effect on Functionality	

PARAMETER ELEMENT	DESCRIPTION
Code	VMX11
Name	Prevent unauthorized removal, connection and modification of devices.

Description	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. 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.
Threat	By default, a rogue user with nonadministrator privileges in a virtual machine can: • Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive • Disconnect a network adaptor to isolate the virtual machine from its network, which is a denial of service • Modify settings on a device
Recommendation Level	Enterprise

Parameter Setting	isolation.device.connectable.disable=TRUE
	isolation.device.edit.disable=TRUE

Effect on Functionality	

Virtual machine communications interface (VMCI) is a new type of interface designed to provide efficient and controlled communication between virtual machines and trusted endpoints on the host, and from virtual machine to virtual machine. The VMkernel is considered a trusted endpoint.

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 virtual machines 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.

The interface currently has only two settings: enabled and restricted. 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. At the time of this writing, there is no other usage for this interface.

PARAMETER ELEMENT	DESCRIPTION
Code	VMX12
Name	Disable virtual machine-to-virtual machine communication through VMCI.
Description	If the interface is not restricted, a virtual machine can detect and be detected by all others with the same option enabled within the same host. This might be the intention , but custom-built software can have unexpected vulnerabilities that might potentially lead to an exploit. Additionally, it is possible for a virtual machine to detect how many others are within the same ESX system by simply registering the virtual machine. This information might also be used for a potentially malicious objective. By default, the setting is FALSE.
Threat	The virtual machine can be exposed to others within the same system as long as there is at least one program connected to the VMCI socket interface.

Recommendation Level	Enterprise
Parameter Setting	vmci0.unrestricted=FALSE
Effect on Functionality	

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.

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	
Code	VMX20	
Name	Limit virtual machine log file size and number.	
Description	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. 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. 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.	
Threat	Uncontrolled logging can lead to denial of service due to the datastore's being filled.	
Recommendation Level	Enterprise	SSLF

Parameter Setting	log.rotateSize=1000000
	log.keepOld=10
		Isolation.tools.log.disable=TRUE

Effect on Functionality		Virtual machine logs unavailable for troubleshooting and support.

PARAMETER ELEMENT	DESCRIPTION
Code	VMX21
Name	Limit informational messages from the virtual machine to the VMX file.

Description	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.
Threat	Uncontrolled size for the VMX file can lead to denial of service if the datastore is filled.
Recommendation Level	Enterprise
Parameter Setting	tools.setInfo.sizeLimit=1048576
Effect on Functionality	

PARAMETER ELEMENT	DESCRIPTION
Code	VMX22
Name	Avoid using independent nonpersistent disks.
Description	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. 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 virtual machine is logged remotely on a separate server, such as a syslog server or equivalent Windows-based event collector.
Threat	Without a persistent record of activity on a virtual machine, administrators might never know whether they have been attacked or hacked.
Recommendation Level	DMZ
Parameter Setting	If remote logging of events and activity is not configured for the guest, scsiX:Y.mode should be either: 1. Not present 2. Not set to independent nonpersistent
Effect on Functionality	Won't be able to make use of nonpersistent mode, which allows rollback to a known state when rebooting the virtual machine.

Virtual Machine Management APIs

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
Code	VMX30
Name	Disable remote operations within the guest.
Description	The VIX API enables systems administrators to write programs and scripts that automate virtual machine operations, as well as guest operating systems within the virtual machines themselves. If enabled, the system administrator can execute scripts or programs that use the VIX API to execute tasks within the guest OS.
Threat	An adversary potentially can execute unauthorized scripts within the guest OS.

Recommendation Level	Enterprise
Parameter Setting	guest.command.enabled=FALSE
Effect on Functionality	

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 4.0 leverages the guest SDK API to get to the accurate counters from the hypervisor. The programming guide for vSphere guest SDK 4.0 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 virtual machine data).

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

- GUESTLIB_HOST_CPU_NUM_CORES
- 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 virtual machine 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 virtual machine 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:

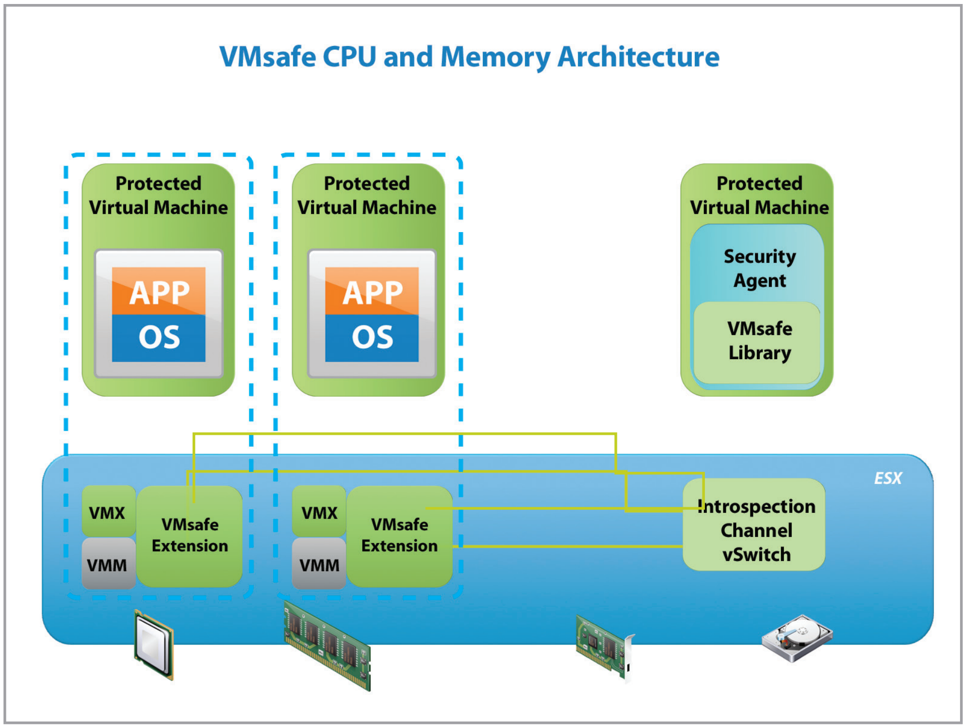
- VMsafe memory and CPU API (VMsafe memory/CPU): Inspections of memory accesses and CPU states.
- VMsafe network packet inspection API (VMsafe-Net): The VMsafe-Net enables you to create agents that inspect network packets at a point in the packet stream between the virtual network adaptor (vNIC) and a vSwitch that sits in front of a physical network adaptor (pNIC). 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 virtual machine'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 virtual machine to view and modify the CPU and memory contents of other virtual machines on the host, it must have access to the CPU/memory APIs. This access is enabled by attaching the virtual machine to a special VMsafe introspection vSwitch. The following diagram shows how the VMsafe CPU/memory API works.


VMsafe CPU and Memory Architecture
Protected Virtual Machine
APP
OS
Protected Virtual Machine
APP
OS
Protected Virtual Machine
Security Agent
VMsafe Library
ESX
VMX
VMM
VMsafe Extension
VMX
VMM
VMsafe Extension
Introspection Channel vSwitch

The following two groups of parameter settings control the VMsafe CPU/memory API:

Security Virtual Appliance

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. The isolated network is provided through a special introspection virtual switch and must use the following naming:

- vSwitch name: vmsafe
- Port group name: vmsafe-appliances

Protected Virtual Machines

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 virtual machine 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 ELEMENT	DESCRIPTION
Code	VMX51
Name	Restrict access to VMsafe CPU/memory APIs.
Description	You should ensure that the only virtual machines configured on the VMsafe CPU/memory introspection vSwitch are those that you have specifically installed to perform this task.
Threat	An attacker might compromise all other virtual machines by making use of this introspection channel.
Recommendation Level	Enterprise
Parameter Setting	If a virtual machine is not running a VMsafe CPU/memory product, ensure that the following parameter is **not** present in its VMX file: ethernetX.networkName=”vmsafe-appliances” where X is a digit.
Effect on Functionality	

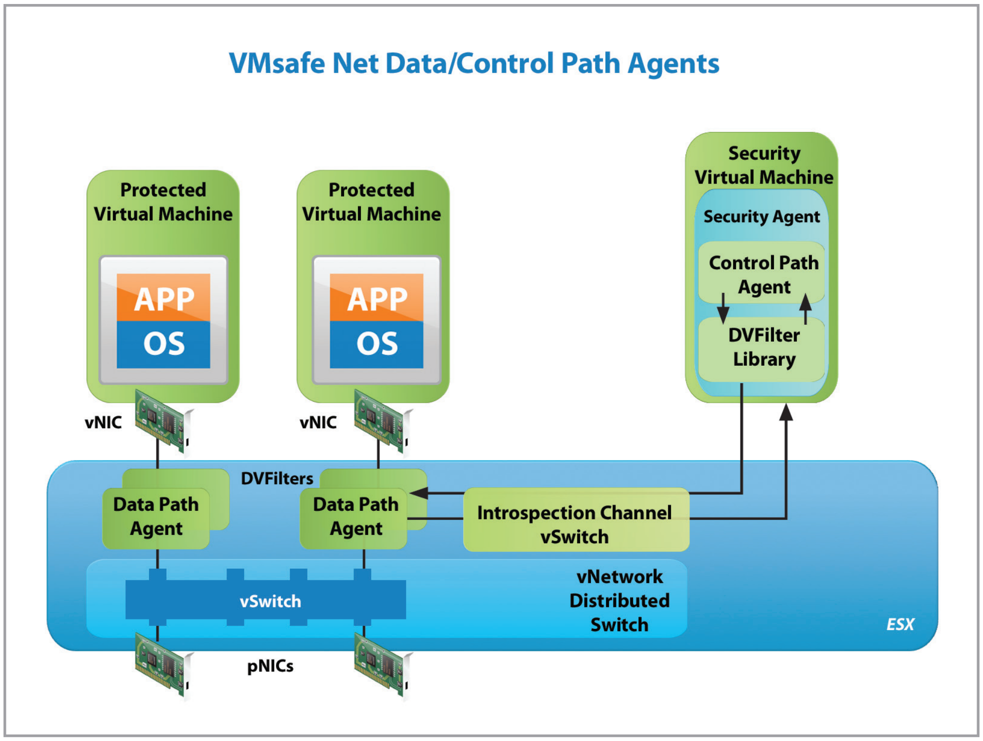
PARAMETER ELEMENT	DESCRIPTION
Code	VMX52
Name	Control access to virtual machines through VMsafe CPU/memory APIs.
Description	A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address 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 virtual machines for which you want this to be done.
Threat	An attacker might compromise the virtual machine by making use of this introspection channel.
Recommendation Level	Enterprise

Parameter Setting	If a virtual machine is not supposed to be protected by a VMsafe CPU/memory product, ensure that the following is **not** present in its VMX file:
	vmsafe.enable=TRUE
	vmsafe.agentAddress=”www.xxx.yyy.zzz”
	vmsafe.agentPort=”nnnn”
	The latter two parameters are based on how the VMsafe security virtual appliance is configured; they should not be present at all if the virtual machine is not to be protected.

Effect on Functionality	

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. The following diagram shows how the VMsafe CPU/memory API works.



The following two groups of parameter settings control the VMsafe network API:

Control Path Security Virtual Appliance

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. The isolated network is provided through a special introspection virtual switch and must use the following naming:

- vSwitch name: *dvfilter*
- Port group name: *dvfilter-appliances*

Protected Virtual Machines

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 virtual machine 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	VMX54
Name	Restrict access to VMsafe network APIs.
Description	You should ensure that the only virtual machines configured on the VMsafe network introspection vSwitch are those that you have specifically installed to perform this task.
Threat	An attacker might compromise all other virtual machines by making use of this introspection channel.
Recommendation Level	Enterprise
Parameter Setting	If a virtual machine is not running a VMsafe network security appliance, ensure that the following parameter is not present in its VMX file: ethernetX.networkName=”dvfilter-appliances” where X is a digit.
Effect on Functionality	

Parameter Element	Description
Code	VMX55
Name	Control access to virtual machines through VMsafe network APIs.
Description	A virtual machine must be configured explicitly to accept access by the VMsafe network API. This should be done only for virtual machines for which you want this to be done.
Threat	An attacker might compromise the virtual machine by making use of this introspection channel.
Recommendation Level	Enterprise
Parameter Setting	If a virtual machine is not supposed to be protected by a VMsafe CPU/memory product, ensure that the following is not 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 XX. If the virtual machine is supposed to be protected, ensure that the name of the data path kernel is set correctly.
Effect on Functionality	

General Virtual Machine Protection

OPERATIONAL ELEMENT	DESCRIPTION
Code	VMP01
Name	Secure virtual machines as you would secure physical machines.
Description	A key to understanding the security requirements of a virtualized environment is the recognition that a 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.
Risk or Control	The guest operating system that runs in the virtual machine is subject to the same security risks as a physical system.
Recommendation Level	Enterprise

Condition or Steps	Ensure that antivirus, antispyware, 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
Code	VMP02
Name	Disable unnecessary or superfluous functions inside virtual machines.
Description	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. Virtual machines 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.
Risk or Control	Any service running in a virtual machine provides a potential avenue of attack.
Recommendation Level	Enterprise
Condition or Steps	Some of these steps include: • Disable unused services in the operating system. For example, if the system runs a file server, make sure to turn off any Web services. • Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adaptors. This is described in the "Removing Unnecessary Hardware Devices" section in the *ESX Configuration Guide*. • 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.

OPERATIONAL ELEMENT	DESCRIPTION
Code	VMP03
Name	Use templates to deploy virtual machines whenever possible.
Description	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.
Risk or Control	Manual installation of the OS and applications into a virtual machine introduces the risk of misconfiguration due to human or process error.
Recommendation Level	Enterprise
Condition or Steps	Provide templates for virtual machine 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 virtual machine-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
Code	VMP04
Name	Prevent virtual machines from taking over resources.
Description	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.
Risk or Control	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.
Recommendation Level	DMZ
Condition or Steps	Use shares or reservations to guarantee resources to critical virtual machines. 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.

OPERATIONAL ELEMENT	DESCRIPTION
Code	VMP05
Name	Minimize use of the virtual machine console.
Description	The virtual machine console enables you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show.
Risk or Control	The virtual machine 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 virtual machine console sessions are open simultaneously.
Recommendation Level	Enterprise
Condition or Steps	Instead of virtual machine console, use native remote management services, such as terminal services and ssh, to interact with virtual machines. Grant virtual machine console access only when necessary.

VMware ESX/ESXi Host

Installation

OPERATIONAL ELEMENT	DESCRIPTION
Code	HIN01
Name	Verify integrity of software before installation.
Description	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.
Risk or Control	Software tampering can be used to break security.
Recommendation Level	Enterprise
Condition or Steps	Always check the SHA1 hash after downloading an ISO from download.vmware.com 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.

Storage

PARAMETER ELEMENT	DESCRIPTION
Code	HST01
Name	Ensure bidirectional CHAP authentication is enabled for iSCSI traffic.
Description	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.
Threat	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.
Recommendation Level	DMZ
Parameter Setting	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.
Effect on Functionality	

OPERATIONAL ELEMENT	DESCRIPTION	
Code	HST02	
Name	Ensure uniqueness of CHAP authentication secrets.	
Description	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.	
Risk or Control	With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device.	
Recommendation Level	DMZ	SSLF
Condition or Steps	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
Code	HST03
Name	Mask and zone SAN resources appropriately.

Description	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.
Risk or Control	
Recommendation Level	Enterprise
Condition or Steps	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
Code	HCM01
Name	Do not use default self-signed certificates for ESX/ESXi communication.
Description	Replace default self-signed certificates with those from a trusted CA, either commercial or organizational.
Risk or Control	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.
Recommendation Level	Enterprise
Parameters or Objects Configuration	Information on how to replace default self-signed certificates can be found in both the *ESXi Configuration Guide* and the *ESX Configuration Guide*, “Security” chapter, “Authentication and User Management” section, “Encryption and Security Certificates for ESX/ESXi” subsection. This section covers the following advanced customization options: • Configuring SSL timeouts • Configuration for certificates in nondefault locations The two guides can be found at these URLs: • http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_esxi_server_config.pdf • http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_esx_server_config.pdf
Test	Ensure that any certificates presented by the host can be verified by a trusted certification authority.

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 configuration of these services is stored in the proxy.xml file on both ESX and ESXi. The locations are as follows:

- ESX: on the service console, /etc/vmware/hostd/proxy.xml
- ESXi: through the file interface, which can be accessed in a couple of ways:
  - Directly via the HTTPS interface: https://<hostname>/host/proxy.xml
  - Using the vCLI vifs. For example: *vifs* --server <hostname> --username <username> --get /host/proxy.xml <directory>/proxy.xml

For information on supported ways to modify the proxy.xml file, see the following KB article: http://kb.vmware.com/kb/1017022.

Each service is contained in an XML element under the following tree:

```
<ConfigRoot>
  <EndpointList>
    <_length>10</_length>
   <_type>vim.ProxyService.EndpointSpec[]</_type>
    <e id=”0”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
      <accessMode>httpsWithRedirect</accessMode>
      <port>8309</port>
     <serverNamespace>/</serverNamespace>
    </e>
    <e id=”1”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpAndHttps</accessMode>
      <port>8309</port>
      <serverNamespace>/client/clients.xml</serverNamespace>
    </e>
    <e id=”2”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpAndHttps</accessMode>
      <port>12001</port>
     <serverNamespace>/ha-nfc</serverNamespace>
    </e>
    <e id=”3”>
     <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
     <accessMode>httpsWithRedirect</accessMode>
     <pipeName>/var/run/vmware/proxy-mob</pipeName>
     <serverNamespace>/mob</serverNamespace>
    </e>
    <e id=”4”>
      <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpAndHttps</accessMode>
      <port>12000</port>
     <serverNamespace>/nfc</serverNamespace>
    </e>
    <e id=”5”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
      <accessMode>httpsWithRedirect</accessMode>
      <port>8307</port>
     <serverNamespace>/sdk</serverNamespace>
    </e>
    <e id=”6”>
     <_type>vim.ProxyService.NamedPipeTunnelSpec</_type>
     <accessMode>httpOnly</accessMode>
      <pipeName>/var/run/vmware/proxy-sdk-tunnel</pipeName>
     <serverNamespace>/sdkTunnel</serverNamespace>
    </e>
    <e id=”7”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpsWithRedirect</accessMode>
      <port>8308</port>
      <serverNamespace>/ui</serverNamespace>
    </e>
    <e id=”8”>
     <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpsOnly</accessMode>
      <port>8089</port>
     <serverNamespace>/vpxa</serverNamespace>
    </e>
    <e id=”9”>
      <_type>vim.ProxyService.LocalServiceSpec</_type>
     <accessMode>httpsWithRedirect</accessMode>
      <port>8889</port>
     <serverNamespace>/wsman</serverNamespace>
    </e>
  </EndpointList>
```

Services can be modified by changing entries in their node; they can be disabled by removing the node entirely. Changes take effect when the host is rebooted or the host agent (hostd) is restarted.

- On ESX: log into the service console and execute the command “service mgmt-vmware restart.”
- On ESXi: log into the DCUI and use the “Restart Management Agents” operation.

PARAMETER ELEMENT	DESCRIPTION
Code	HCM02
Name	Disable managed object browser.
Description	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.
Threat	This interface might potentially be used to perform malicious configuration changes or actions.
Recommendation Level	SSLF
Parameter Setting	Perform the following edits on the proxy.xml file: 1. Remove the managed object browser element. This element can be identified as the one with element “<serverNamespace>/mob</serverNamespace>.” Remove or comment out the *entire* element; that is, “<e id=’n’>” and everything within it. 2. Renumber the subsequent <e id=”n”> to reflect the removed element, so that there are no skipped numbers. 3. Decrease the value of the “<_length>” element by one. Then restart the host agent.
Effect on Functionality	The managed object browser will no longer be available for diagnostics.

PARAMETER ELEMENT	DESCRIPTION
Code	HCM03
Name	Disable vSphere Web Access (ESX **only**).
Description	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. In most cases, users should manage virtual machines through vCenter Server, using either the vSphere Client or the vCenter vSphere Web Access. NOTE: ESXi does not have vSphere Web Access; this guideline is not relevant for ESXi.
Threat	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.
Recommendation Level	DMZ
Parameter Setting	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.
Effect on Functionality	vSphere Web Access will no longer be available.

PARAMETER ELEMENT	DESCRIPTION
Code	HCM04
Name	Ensure that ESX is configured to encrypt all sessions.
Description	Sessions with the ESX server should be encrypted because transmitting data in plain text can be viewed as it travels through the network.
Threat	The use of unencrypted client sessions leaves communications between the different components of vSphere open to MiTM attacks.
Recommendation Level	Enterprise
Parameter Setting	<httpPort> and <accessMode> XML settings in the proxy.xml file.
Effect on Functionality	In the proxy.xml file, ensure for all the different entries that `<httpPort>-1</httpPort>` is set and that the `<accessMode> </accessMode>` parameters are not set to `http`. They can be set to either `httpsWithRedirect` or `httpsOnly`.

Logging

The following sets of recommendations do not pertain to ESX 4.0 (i.e., the “classic” ESX architecture, with the console OS). They apply to only the ESXi architecture.

ESXi 4.0 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
Name	Configure remote syslog.
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. You can also 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; it also provides a long-term audit record.
Recommendation Level	Enterprise
Parameters or Objects Configuration	Remote syslog can be configured on an ESXi host, using a remote command line such as vCLI or PowerCLI, or using an API client.
Test	Query the syslog configuration to make sure that a valid syslog server has been configured, including the correct port.

CONFIGURATION ELEMENT	DESCRIPTION
Code	HLG02
Name	Configure persistent logging.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Parameters or Objects Configuration	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 *vSphere Basic System Administration Guide* in the "Configuring Hosts and vCenter Server" chapter, in the "System Log Files: Configure Syslog on ESXi Hosts" section.

Test	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
Code	HLG03
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 intruder's actions when reviewing the relevant log files.
Risk or Control	Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.
Recommendation Level	Enterprise
Parameters or Objects configuration	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.
Test	• Query the NTP configuration to make sure that a valid time source has been configured. • Make sure that the NTP service is running on the host.

Management

The Common Information Model (CIM) is an open standard that defines a framework for agent-less, standards-based monitoring of hardware resources for 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
Code	HMT01
Name	Control access by CIM-based hardware monitoring tools.
Description	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.
Threat	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.
Recommendation Level	Enterprise

Parameters or Objects Configuration	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. 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: • Host > Config > SystemManagement • Host > CIM > CIMInteraction This role can be either local to the host or centrally defined on vCenter Server, depending on how the particular monitoring applications work.
Test	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 4.0 contains a different SNMP agent from that in ESX 4.0, and it supports only versions 1 and 2c. It provides the same notifications as ESX 4.0 and adds notifications for hardware-related sensors. Unlike ESX 4.0, 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
Code	HMT02
Name	Ensure proper SNMP configuration (ESXi **only**).
Description	If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured.
Risk or Control	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.
Recommendation Level	Enterprise
Parameters or Objects Configuration	SNMP can be configured on an ESXi host, using a remote command line such as vCLI or PowerCLI, or using an API client.
Test	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.

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

OPERATIONAL ELEMENT	DESCRIPTION
Code	HMT03
Name	Establish and maintain configuration file integrity (ESXi **only**).
Description	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.
Risk or Control	Tampering with these files has the potential to enable unauthorized access to the host configuration and virtual machines.
Recommendation Level	DMZ
Condition or Steps	The accessible and relevant configuration files in ESXi 4.0 are found by browsing to https://<hostname>/host. 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. 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.

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.

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

- vSwitch name: *vmsafe*
- Port group name: *vmsafe-appliances*

CONFIGURATION ELEMENT	DESCRIPTION
Code	HMT10
Name	Prevent unintended use of VMsafe CPU/memory APIs.
Description	If you are not using any products that make use of the VMsafe CPU/memory API, the VMsafe CPU/memory introspection vSwitch should not even be present.
Risk or Control	If the API is enabled, an attacker might attempt to connect a virtual machine to it, thereby potentially providing access to the CPU and memory of other virtual machines on the host.
Recommendation Level	Enterprise
Parameters or Objects Configuration	If a VMsafe CPU/memory product is not being used on the host, ensure that no vSwitch named "vmsafe" exists on the host.
Test	Options include: • Check via vSphere Client GUI • Query using CLI (e.g., vCLI, PowerCLI) • Employ code that uses the vSphere 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. 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.

- vSwitch name: *dvfilter*
- Port group name: *dvfilter-appliances*

CONFIGURATION ELEMENT	DESCRIPTION
Code	HMT11
Name	Prevent unintended use of VMsafe network APIs.
Description	If you are not using any products that make use of the VMsafe network API, the VMsafe network introspection vSwitch should not even be present.
Risk or Control	If the API is enabled, an attacker might attempt to connect a virtual machine to it, thereby potentially providing access to the network of other virtual machines on the host.
Recommendation Level	Enterprise
Parameters or Objects Configuration	If a VMsafe network security appliance is not being used on the host, ensure that no vSwitch named "dvfilter" exists on the host.
Test	Options include: • Check via vSphere Client GUI • Query using CLI (e.g., vCLI, PowerCLI) • Employ code that uses the vSphere API

Host Console

The following sets of recommendations do not pertain to ESX 4.0 (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. One particular built-in local group has special meaning. If you give a user membership in the localadmin group, that user has the ability to log in to the DCUI, which is the interface available at the console of an ESXi host that allows for basic host configuration—modifying networking settings and the root password, for example. Assignment to this group enables an administrative user to perform tasks on the DCUI without logging in as root. However, this is a very powerful privilege, because access to the DCUI allows someone to change the root password or even power-off the host. Therefore, only the most trusted administrators should be granted membership to the localadmin group.

CONFIGURATION ELEMENT	DESCRIPTION
Code	HCN01
Name	Ensure that only authorized users have access to the DCUI.
Description	Users who are members of the local group called "localadmin" have the ability to log in to the DCUI. Only those who are authorized should be members of this group.
Risk or Control	Anyone with credentials to access the DCUI can reconfigure the host or reboot and turn it off.
Recommendation Level	Enterprise
Parameters or Objects Configuration	Check the users in the local group named "localadmin" and ensure that only authorized users are present.
Test	Unauthorized users should not be able to enter credentials and log in to the DCUI.

Lockdown mode is available on any ESXi 4.0 host that you have added to a vCenter Server. Enabling lockdown mode disables all remote root access to ESXi 4.0 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.
- In a vSphere Client session or using vCLI commands direct to the ESXi 4.0 system, using a local user account defined on the host.

By default, no local user accounts exist on the ESXi system. You must create those accounts before enabling lockdown mode and must create them in a vSphere Client session connected directly to the ESXi system. Changes to a host are limited to those that can be made with the privileges granted to a particular user locally on that host.

NOTE: 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
Code	HCN02
Name	Enable lockdown mode to restrict root access.
Description	Lockdown mode can be enabled after an ESXi host is added to vCenter Server. Enabling lockdown mode disables all remote root access to ESXi 4.0 machines. Any subsequent local changes to the host must be made: • Using the DCUI • In a vSphere Client session or using vCLI commands to vCenter Server • In a vSphere Client session or using vCLI commands direct to the ESXi 4.0 system
Threat	Security best practices dictate that the root password should be known to as few individuals as possible. The root account should not be used if any alternative is possible. It is an anonymous account, and activity by the root user cannot be definitively associated with a specific individual.
Recommendation Level	Enterprise
Parameter Setting	To do this manually, in the vSphere Client, in the configuration tab for a host, in the security profile setting, click the checkbox for "Lockdown Mode." This can also be done using PowerCLI or with an API client. Lockdown mode can also be enabled and disabled from the DCUI.
Effect on Functionality	Enabling lockdown prevents all API-based access by the root account to the ESXi host. This includes: vSphere Client, vCLI, PowerCLI, and any API-based client. Non-root accounts are not affected.

CONFIGURATION ELEMENT	DESCRIPTION
Code	HCN03
Name	Avoid adding the root user to local groups.
Description	It is possible to add the local root account to local user groups on the host. However, doing this might allow one to subvert lockdown mode. If root is a member of a particular group, and then this group is granted an administrative local role, then root will be able to log in even if lockdown mode is enabled.
Risk or Control	Putting root in a local group, and then granting a local access role to that group, subverts lockdown mode because it allows the root user to continue logging into the host.
Recommendation Level	Enterprise
Parameters or Objects Configuration	Make sure that the local root user is not a member of any groups other than the defaults.
Test	While lockdown mode is enabled, ensure that root cannot still log in or perform any tasks.

ESXi has a special technical support mode, which is an interactive command line available only on the console of the server. Technical support mode is unsupported unless used in consultation with VMware Technical Support and must be activated before it can be used. Access to this mode requires the root password of the server in addition to access to the console of the server, either physically or through a remote KVM or iLO interface.

Technical support mode is designed to be used only in cases of emergency, when management agents that provide the remote interfaces are inoperable and they cannot be restarted through the DCUI. There is no reason to use technical support mode for any purpose apart from technical support. Technical support mode is on by default, but you can disable it entirely.

Technical support mode is secured in the following ways:

- It is accessible only on the local console; unlike SSH or Telnet, it cannot be accessed remotely. Therefore, physical access to the host—or something equivalent to physical access, such as HP ILO, Dell DRAC, IBM RSA, or a similar remote console tool—is absolutely required for access to technical support mode. Most organizations have sufficient forms of protection on physical (or physical equivalent) access to the host (e.g., door locks, key cards, and authentication for the remote console).
- It requires the root password before access is granted. Any individuals who have both physical (or console) access and the root password are already fully privileged and can do anything they want on the system. The presence of technical support mode does not augment or reduce this risk.

You can audit technical support mode using the following information:

- Whenever someone activates technical support mode, the time and date of activation are sent to the system log messages file.
- All unsuccessful attempts to access technical support mode (i.e., someone enters the incorrect root password) are recorded in the system log.
- The time and date of all successful accesses to technical support mode are sent to the system log.

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. Actions performed while in technical support mode are not logged. Any access to technical support mode should be correlated with a specific call to VMware Technical Support. If there is no corresponding support session, you should immediately suspect malicious activity and inspect the system for tampering.

If you are unable to audit technical support mode to a degree that matches your security risk posture, you should disable it for all of your ESXi hosts. For details on disabling technical support mode, see VMware Knowledge Base article 1003677 (http://kb.vmware.com/kb/1003677).

PARAMETER ELEMENT	DESCRIPTION
Code	HCN04
Name	Disable tech support mode.
Description	Technical support mode is an interactive command line available only on the console of the server. It is unsupported unless used in consultation with VMware Technical Support and must be activated before it can be used. Access to this mode requires the root password of the server in addition to access to the console of the server, either physically or through a remote KVM or iLO interface.
Threat	Anyone logged into technical support mode can assume complete control of the host, including reconfiguring and stealing a virtual machine.
Recommendation Level	SSLF
Parameter Setting	Technical support mode is governed by a particular kernel parameter *VMkernel.Boot.techSupportMode*. This parameter can be unset via either the vSphere Client or an API client (e.g., the PowerCLI). For details on disabling technical support mode, see VMware Knowledge Base article 1003677 (http://kb.vmware.com/kb/1003677).
Effect on Functionality	If technical support mode is disabled, supportability and diagnosability of the host might be greatly limited. Because reenabling technical support mode requires a reboot, in some cases an issue might not be resolvable without forcefully shutting down virtual machines.

VMware 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
- Among ESX/ESXi hosts—for example, for VMware High Availability coordination
- Between ESX/ESXi or vCenter and systems running client software such as the vSphere Client or a VI
- SDK application
- Between ESX/ESXi and ancillary management services, such as DNS, NTP, syslog and the user authentication service
- Between ESX/ESXi and third-party management tools, such as third-party virtual switch management, hardware monitoring, systems management and backup tools
- Between vCenter and supporting services, such as the vCenter database and the user authentication service
- Between vCenter 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 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.

CONFIGURATION ELEMENT	DESCRIPTION	
Code	NAR01	
Name	Ensure that vSphere management traffic is on a restricted network.	
Description	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: • Service console interface on ESX • Management VMkernel interface on ESXi	
Risk or Control	Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems.	
Recommendation Level	Enterprise	SSLF
Parameters or Objects Configuration	The vSphere management port group should be in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (virtual machine) traffic, as long as the vSphere management port group's VLAN is not used by production virtual machines.	The vSphere management port group should be on a management-only vSwitch.
Effect on Functionality		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 be possible to achieve.
Test	• Check for usage of VLAN ID on nonmanagement port groups. • 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 virtual machine traffic cannot be routed to this network.	In addition to enterprise tests: • Check that the management-only vSwitch does not contain any nonmanagement port groups.

CONFIGURATION ELEMENT	DESCRIPTION
Code	NAR02
Name	Ensure that VMotion traffic is isolated.
Description	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.
Risk or Control	Attackers can sniff VMotion traffic to obtain memory contents of a virtual machine. They might also potentially stage a MiTM attack in which the contents are modified during migration.

Recommendation Level	Enterprise	SSLF
Parameters or Objects Configuration	VMotion port group should be in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (virtual machine) traffic, as long as the VMotion port group's VLAN is not used by production virtual machines.	VMotion port group should be on a management-only vSwitch.
Effect on Functionality		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.
Test	• Check for usage of VLAN ID on non-VMotion port groups. • Check that VLAN is isolated and not routed in the physical network.	In addition to enterprise tests: • Check that VMotion port group vSwitch does not contain any nonmanagement port groups. • Check that the physical network is not accessed by any other nonmanagement entity.

CONFIGURATION ELEMENT	DESCRIPTION	
Code	NAR03	
Name	Ensure that IP-based storage traffic is isolated.	
Description	Virtual machines might share virtual switches and VLANs with the IP-based storage configurations. IP-based storage includes: • iSCSI • NFS This type of configuration might expose IP-based storage traffic to 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.	
Risk or Control	IP-based storage frequently is not encrypted and therefore can be viewed by anyone with access to this network.	
Recommendation Level	Enterprise	SSLF
Parameters or Objects Configuration	Storage port groups should be in a dedicated VLAN on a common vSwitch. The vSwitch can be shared with production (virtual machine) traffic, as long as the storage port group's VLAN is not used by production virtual machines.	Storage port group should be on a management-only vSwitch.

Effect on Functionality		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.
Test	• Check for usage of VLAN ID on non-storage port groups. • Check that VLAN is isolated and not routed in the physical network.	In addition to enterprise tests: • Check that storage port group vSwitch does not contain any nonmanagement port groups. • Check that the physical network is not accessed by any other nonmanagement entity.

OPERATIONAL ELEMENT	DESCRIPTION	
Code	NAR04	
Name	Strictly control access to management network.	
Description	However 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.	
Risk or Control	If an attacker gains access to the management network, it provides the staging ground for further attack.	
Recommendation Level	DMZ	SSLF
Condition or Steps	Configure a controlled gateway 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). 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 VNC) 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.

VMware 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
Code	NCN02
Name	Ensure that there are no unused ports on a distributed vSwitch port group.
Description	The number of ports in a distributed port group can be adjusted to exactly match the number of virtual machines assigned to that port group.
Risk or Control	Limiting the number of ports in a port group limits the potential for a virtual machine administrator, either accidentally or maliciously, to move a virtual machine to an unauthorized network.
Recommendation Level	DMZ
Parameters or Objects Configuration	"Number of Ports" setting in the settings page of a port group.
Test	Can be done manually through the vSphere Client. 1. While connected to the vCenter Server: Navigate to Home → Inventory → Networking in the vSphere Client and click on the vDS in question. 2. Click on the "Ports" Tab. 3. Check if all of the "ports" in the list have a virtual machine associated with them in the "connected" column. The equivalent steps can be automated using scripting or the SDK.

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.

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 virtual machines 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 initial MAC address.
Threat	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.
Recommendation Level	Enterprise
Parameter Setting	MAC address changes set to reject (accept by default) on all vSwitches.
Effect on Functionality	This will prevent virtual machines 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
Code	NCN04
Name	Ensure that the “Forged Transmits” policy is set to reject.
Description	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.
Threat	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.
Recommendation Level	Enterprise
Parameter Setting	“Forged Transmits” parameter should be set to “Reject” on all vSwitches.
Effect on Functionality	This will prevent virtual machines 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
Code	NCN05
Name	Ensure that the "Promiscuous Mode" policy is set to reject.
Description	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.
Threat	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.
Recommendation Level	Enterprise
Parameter Setting	"Promiscuous Mode" parameter should be set to "Reject" on all vSwitches.
Effect on Functionality	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 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
Code	NCN06
Name	Ensure that port groups are not configured to the value of the native VLAN.
Description	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. 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 will 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).
Risk or Control	If the ESX virtual switch port group uses the native VLAN ID, traffic from those virtual machines will not be visible to the native VLAN on the switch, because the switch is expecting untagged traffic.
Recommendation Level	Enterprise
Parameters Setting	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 not configured to use whatever value is set for the native VLAN.

PARAMETER ELEMENT	DESCRIPTION
Code	NCN07
Name	Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT).
Description	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 virtual machine 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.
Risk or Control	If VGT is enabled inappropriately, it might cause denial of service or allow a guest virtual machine to interact with traffic on an unauthorized VLAN.
Recommendation Level	Enterprise
Parameters Setting	VLAN ID setting on all port groups should not be set to 4095 unless VGT is required.

PARAMETER ELEMENT	DESCRIPTION
Code	NCN08
Name	Ensure that port groups are not configured to VLAN values reserved by upstream physical switches.
Description	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.
Risk or Control	Using a reserved VLAN might result in a denial of service on the network.
Recommendation Level	Enterprise
Parameters Setting	VLAN ID setting on all port groups should not be set to reserved values of the physical switch.

OPERATIONAL ELEMENT	DESCRIPTION
Code	NCN10
Name	Ensure that port groups are configured with a clear network label.
Description	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.
Risk or Control	Without these descriptions, identifying port groups and their functions becomes difficult as the network becomes more complex.
Recommendation Level	Enterprise
Condition or Steps	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. Scripted method (vCLI command): vicfg-vswitch –l command.

OPERATIONAL ELEMENT	DESCRIPTION
Code	NCN11
Name	Ensure that all vSwitches have a clear network label.
Description	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.
Risk or Control	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 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.
Recommendation Level	Enterprise
Condition or Steps	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. Scripted method (vCLI command): vicfg-vswitch –l command.

OPERATIONAL ELEMENT	DESCRIPTION
Code	NCN12
Name	Fully document all VLANs used on vSwitches.
Description	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.
Risk or Control	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 virtual machine to an unauthorized VLAN.
Recommendation Level	Enterprise
Condition or Steps	Both standard and distributed vSwitch configurations can be viewed in the vSphere Client or by using the vSphere API. For a standard vSwitch, vicfg-vswitch –l will list all port groups and their VLAN association. Compare this list with the physical switch configuration.

OPERATIONAL ELEMENT	DESCRIPTION
Code	NCN13
Name	Ensure that only authorized administrators have access to virtual networking components.
Description	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, virtual machine administrators should have access only to port groups in which their virtual machines reside. Network administrators should have permissions to all virtual networking components but not have access to virtual machines. 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.

Risk or Control	This control mitigates the risk of misconfiguration, whether accidental or malicious, and enforces key security concepts of separation of duties and least privilege.
Recommendation Level	Enterprise
Condition or Steps	Ensure that vSphere permissions to specific port groups are granted only to those individuals who need it.

Physical Network

OPERATIONAL ELEMENT	DESCRIPTION
Code	NPN01
Name	Ensure that physical switch ports are configured with spanning tree disabled.
Description	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.
Risk or Control	If these are not set, potential performance and connectivity issues might arise.
Recommendation Level	Enterprise
Condition or Steps	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
Code	NPN02
Name	Ensure that the *non-negotiate* option is configured for trunk links between external physical switches and virtual switches in VST mode.
Description	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 *non-negotiate* and on 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 *non-negotiate* and on options is that on mode still sends out DTP frames, whereas the non-negotiate option does not.
Risk or Control	The non-negotiate option should be used for all VLAN trunks, to minimize unnecessary network traffic for virtual switches in VST mode.
Recommendation Level	Enterprise
Condition or Steps	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
Code	NPN03
Name	Ensure that VLAN trunk links are connected only to physical switch ports that function as trunk links.
Description	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.
Risk or Control	Misconfiguration of the physical switch ports might lead to undesirable performance, including frames being dropped or misdirected.
Recommendation Level	Enterprise
Condition or Steps	Routinely check physical switch ports to ensure that they are properly configured as trunk ports.

VMware 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
Code	VSH01
Name	Maintain supported operating system, database, and hardware for vCenter.
Description	vCenter Server resides on a Windows-based operating system and therefore requires a supported version of Windows.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	For OS and database compatibility, see the vSphere Compatibility Matrixes white paper: http://www.vmware.com/pdf/vsphere4/r40/vsp_compatibility_matrix.pdf For hardware requirements, see the *ESX and vCenter Server Installation Guide* white paper: http://www.vmware.com/pdf/vsphere4/r40/vsp_40_esx_vc_installation_guide.pdf

OPERATIONAL ELEMENT	DESCRIPTION
Code	VSH02
Name	Keep vCenter Server system properly patched.
Description	By staying up to date on Window patches, vulnerabilities in the OS can be mitigated.

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

OPERATIONAL ELEMENT	DESCRIPTION
Code	VSH04
Name	Avoid user login to vCenter Server system.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	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
Code	VSH05
Name	Install vCenter Server using a service account instead of a built-in Windows account.
Description	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. The user account must be an administrator on the local machine. In the installation wizard, you specify the account name as DomainName\Username. If 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. 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.

Risk or Control	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.
Recommendation Level	DMZ
Parameters or Objects Configuration	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.
Test	• Check to see that the vCenter processes are running as the service account. • Check to make sure that the service account has only local administrator role.

CONFIGURATION ELEMENT	DESCRIPTION	
Code	VSH06	
Name	Restrict usage of vSphere administrator privilege.	
Description	By default, vCenter Server grants full administrative rights to the local administrator’s account, which can be accessed by domain administrators.	
Risk or Control	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.	
Recommendation Level	Enterprise	DMZ
Condition or Steps	1. Create an ordinary user account that will be used to manage vCenter (example vi-admin). 2. Make sure the user does not belong to any local groups, such as administrator. 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. 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. 5. Remove the permissions in the vCenter for the local administrator group.	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: 1. Logged in as vi-admin, grant full administrative rights to the minimum number of individuals required, typically senior IT staff. 2. Log out as vi-admin, and then protect the password. 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.
Test	Observe the assigned permissions in vSphere; make sure that neither “Administrator” nor any other account or group has any privileges.	

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
Code	VSC01
Name	Do not use default self-signed certificates.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	For new certificate installations on vSphere, see the “Replacing vCenter Server Certificates” white paper: http://www.vmware.com/pdf/vsp_4_vcserver_certificates.pdf For existing certificate installations on vSphere, see the “vSphere Upgrade Guide” white paper : http://www.vmware.com/pdf/vsphere4/r40/vsp_40_upgrade_guide.pdf
Test	Ensure that any certificates presented by the host can be verified by a trusted certification authority.

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

PARAMETER ELEMENT	DESCRIPTION
Code	VSC03
Name	Restrict access to SSL certificates.

Description	By default, any user on the vCenter Server system can access the directory containing the SSL certificates. The directory that contains the SSL certificates needs to be accessed only by the service account user on a regular basis. Occasionally, when collecting data for support purposes, the vCenter Server system administrator might need to access it.
Threat	The SSL certificate can be used to impersonate vCenter and decrypt the vCenter database password.
Recommendation Level	SSLF
Parameter Setting	Change the Windows file permission on the SSL certificate directory so that only the vCenter service account can access it.
Effect on Functionality	Supportability limitations: • Will prevent a complete support log from being collected when the vc-support script is issued • Will prevent the administrator from being able to change the vCenter database password

OPERATIONAL ELEMENT	DESCRIPTION
Code	VSC04
Name	Always verify SSL certificates.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	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 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:
  - vSphere Client
  - vMA (the vSphere Management Assistant)
  - A Windows system from which the PowerCLI is to be used
  - 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
Code	VSC05
Name	Restrict network access to vCenter Server system.
Description	Restrict access to only those essential components required to communicate with vCenter.
Risk or Control	Blocking access by unnecessary systems mitigates general attacks on the Windows system.
Recommendation Level	DMZ
Parameters or Objects Configuration	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.
Test	

CONFIGURATION ELEMENT	DESCRIPTION
Code	VSC06
Name	Block access to ports not being used by vCenter.
Description	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.
Risk or Control	Blocking unneeded ports can mitigate general attacks on the Windows system.
Recommendation Level	DMZ
Parameters or Objects Configuration	A list of ports used by vCenter can be found in this VMware Knowledge Base article: http://kb.vmware.com/kb/1012382 Here is a partial list of examples of where ports might be blocked: • 636/TCP: If the vCenter will not be part of a linked-mode vCenter group • 1521/TCP: If the VCDB is not Oracle Make sure not to block any ports for functionality that are actually in use in your environment.
Test	

PARAMETER ELEMENT	DESCRIPTION
Code	VSC07
Name	Disable managed object browser.
Description	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.
Threat	This interface might potentially be used to perform malicious configuration changes or actions.

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

PARAMETER ELEMENT	DESCRIPTION
Code	VSC08
Name	Disable vSphere Web Access.
Description	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.
Threat	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.
Recommendation Level	DMZ
Parameter Setting	To completely delete the vSphere Web Access service from vCenter Server: 1. Select **Start > Programs > Administrative Tools > Services**. 2. Stop the VMware VirtualCenter Management Webservices service. 3. Use Windows Explorer to open C:\Program Files\VMware\Infrastructure\tomcat\webapps and delete the ui directory. 4. (Optional) Use Windows Explorer to open C:\Program Files\VMware\Infrastructure\tomcat\work\Catalina\localhost and delete the ui directory. 5. Start the VMware VirtualCenter Management Webservices service. See VMware Knowledge Base article **#1009420** for more details. NOTE: Any upgrade to vCenter Server will recreate this file.
Effect on Functionality	vSphere Web Access will no longer be available.

PARAMETER ELEMENT	DESCRIPTION
Code	VSC09
Name	Disable datastore browser.
Description	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 virtual machine files. This is governed by the users permissions on vCenter Server. 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.
Threat	This is a Web interface and therefore has some of the general risks associated with all Web interfaces.

Recommendation Level	SSLF
Parameter Setting	To disable the datastore browser, edit the vpxd.cfg file and ensure that the following element is set: <enableHttpDatastoreAccess>false</enableHttpDatastoreAccess> This should be the only occurrence of this element, and it should be within the <vpxd> … </vpxd> element in vpxd.cfg
Effect on Functionality	You will no longer be able to browse and view datastore files using 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
Code	VSD01
Name	Use least privileges for the vCenter Server database user.
Description	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.
Risk or Control	Least privileges mitigates attacks if the vCenter database account is compromised.
Recommendation Level	Enterprise
Parameters or Objects Configuration	The privileges needed for vCenter on both Oracle and Microsoft SQL Server are given in the *vSphere Upgrade Guide*, “Preparing for the Upgrade to vCenter Server” chapter, “Prerequisites for the vCenter Server Upgrade” section, “Database Prerequisites” subsection. This document can be found here: http://www.vmware.com/pdf/vsphere4/r40_u1/vsp_40_u1_upgrade_guide.pdf NOTE: This section indicates which privileges are needed for installation and upgrade, and which are needed just for ongoing operation.
Test	

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, 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 mitigate 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
Code	VCL01
Name	Restrict the use of Linux-based clients.
Description	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.
Risk or Control	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. With proper controls, this restriction can be relaxed if deemed appropriate. These controls include: • Restriction of management network access only to authorized systems • Use of firewalls to restrict access to vCenter only by authorized hosts • Use of jump-box systems for exclusive access to vCenter
Recommendation Level	DMZ
Condition or Steps	Options include: • 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
Code	VCL02
Name	Verify the integrity of vSphere Client.
Description	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.
Risk or Control	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.

Recommendation Level	Enterprise
Condition or Steps	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 **Plug-ins** → **Manage Plug-ins** and clicking the **Installed Plug-ins** 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 4.0 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
Code	VUM01
Name	Use least privileges for the Update Manager database user.
Description	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 *VMware Update Manager Administration Guide*. 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.
Risk or Control	Least privileges mitigates attacks if the Update Manager database account is compromised.
Recommendation Level	Enterprise
Parameters or Objects Configuration	For Oracle: After installation, only the following permissions are needed for normal operation: *create session, create any table, drop any table*. For SQL Server: After installation, the *dba_owner* role or *sysadmin* role can be removed from the MSDB database (it is still required, however, for the Update Manager database). Check the latest *VMware Update Manager Administration Guide* for any updates to these configurations.

OPERATIONAL ELEMENT	DESCRIPTION
Code	VUM02
Name	Keep Update Manager system properly patched.
Description	By staying up to date on Windows patches, vulnerabilities in the OS can be mitigated.
Risk or Control	If an attacker can obtain access and elevate privileges on the Update Manager system, it can compromise the patching process.
Recommendation Level	Enterprise
Condition or Steps	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
Code	VUM03
Name	Provide Windows system protection on the Update Manager system.
Description	By providing OS-level protection, vulnerabilities in the OS can be mitigated.
Risk or Control	If an attacker can obtain access and elevate privileges on the Update Manager system, it can compromise the patching process.
Recommendation Level	Enterprise
Condition or Steps	Provide Windows system protection, such as antivirus, in accordance with industry-standard guidelines, or internal guidelines where appropriate.

OPERATIONAL ELEMENT	DESCRIPTION
Code	VUM04
Name	Avoid user login to Update Manager system.
Description	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.
Risk or Control	Anyone logged in to the Update Manager can potentially cause harm, either intentionally or unintentionally, by altering settings and modifying processes.
Recommendation Level	Enterprise
Condition or Steps	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
Code	VUM05
Name	Do not configure Update Manager to manage its own virtual machine or that of its vCenter Server.
Description	Although you can install both Update Manager and vCenter Server on virtual machines and place them on the same ESX/ESXi host, you should not configure Update Manager to manage the patches on those virtual machines.
Risk or Control	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.

Recommendation Level	Enterprise
Parameters or Objects Configuration	If installed in virtual machines, ensure that Update Manager does not manage the patching of the virtual machine on which it runs, or the virtual machine on which the associated vCenter Server runs.
Test	

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		
Code	VUM10		
Name	Limit the connectivity between Update Manager and public patch repositories.		
Description	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.		
Risk or Control	Any channel to the Internet represents a threat.		
Recommendation Level	Enterprise	DMZ	SSLF
Parameters or Objects Configuration	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).
Test	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
Code Number	CON01
Name	Ensure that ESX firewall is configured to high security.
Description	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.
Risk or Control	Prevention of network-based exploits.
Recommendation Level	Enterprise
Parameters or Objects Configuration	The following commands configure high security on the firewall: esxcfg-firewall — blockIncoming esxcfg-firewall — blockOutgoing
Test	Ensure that outbound connections are blocked and only selected inbound connections are allowed.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	CON02
Name	Limit network access to applications and services.
Description	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. For more information and recommendations on running third-party software in the service console, see http://www.vmware.com/vmtn/resources/516.
Risk or Control	Prevention of network-based exploits.
Recommendation Level	Enterprise
Parameters or Objects Configuration	All services not required explicitly for business purposes should be disabled.
Test	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
Code Number	CON03
Name	Do not run NFS or NIS clients in the service console.
Description	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 **all** outbound IPv4 connections. 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.
Risk or Control	Turning on these services effectively disables the service console firewall for outbound connections.
Recommendation Level	Enterprise
Parameters Setting	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
Code Number	COM01
Name	Do not apply Red Hat patches to the service console.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	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 http://www.vmware.com/security.

OPERATIONAL ELEMENT	DESCRIPTION
Code Number	COM02
Name	Do not rely upon tools that check only for Red Hat patches.
Description	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.
Risk or Control	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.
Recommendation Level	Enterprise
Condition or Steps	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 *ESX Server 4 Configuration Guide*.

OPERATIONAL ELEMENT	DESCRIPTION
Code Number	COM03
Name	Do not manage the service console as a Red Hat Linux host.
Description	The usual redhat-config-* commands are not present, nor are other components such as the X server.
Risk or Control	Attempts to manage the service console as a typical Red Hat Linux host might result in misconfigurations that affect security, including availability.
Recommendation Level	Enterprise
Condition or Steps	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
Code Number	COM04
Name	Use vSphere Client and vCenter Server to administer the hosts instead of service console.
Description	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.
Risk or Control	By using alternatives to the service console, the need to access it is reduced, thereby minimizing the risk due to misuse.
Recommendation Level	Enterprise
Condition or Steps	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. Some advanced tasks, such as initial configuration for password policies, cannot be performed via the vSphere 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
Code Number	COP01
Name	Use a directory service for authentication.
Description	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. 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.
Risk or Control	Centralized control of user authentication greatly reduces the chance of misconfiguration or inappropriate access.
Recommendation Level	Enterprise
Parameters or Objects Configuration	In the default installation, ESX 3.5–4.0 cannot use active directory to define user accounts. However, it can use active directory to authenticate users. In other words, you can define individual user accounts on the host, and then use the local active directory domain to manage the passwords and account status. You must create a local account for each user who requires local access on the service console. This should not be seen as a burden; in general, only relatively few people should have access to the service console, so it is better that the default is for no one to have access unless you have created an account explicitly for that user. AD, NIS, Kerberos, and LDAP are all supported directory services. Authentication on the service console is controlled by the command esxcfg-auth. You can find information on this command in its man page. Type man esxcfg-auth at the command line when logged in to the service console. For information on authentication with active directory, see the technical note at http://www.vmware.com/vmtn/resources/582. It is also possible to use third-party packages, such as Winbind or Centrify, to provide tighter integration with active directory. Consult the documentation for those solutions for guidance on how to deploy them securely.
Test	The esxcfg-auth –probe command will list all of the files that are generated and edited by the esxcfg-auth command. The entries in those files will be different depending on which authentication mechanism you choose.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COP02
Name	Establish a password policy for password complexity.
Description	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. 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.

Risk or Control	This recommendation addresses the risk of passwords being guessed or cracked.
Recommendation Level	DMZ

Parameters or Objects Configuration	`esxcfg-auth --usepamqc`
	This command requires six parameters in the following order:
	• Minimum length of a single character class password
	• Minimum length of a password that has characters from two character classes
	• Minimum number of words in a passphrase
	• Minimum length of a password that has characters from three character classes
	• Minimum length of a password that has characters from four character classes
	• Maximum number of characters reused from the previous password
	If you pass a value of -1 for any of the six parameters, it disables that option.
	For example, the command line
	`esxcfg-auth --usepamqc=-1 -1 -1 12 8 -1`
	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 classes and disables the final parameter.

Test	Check the following line in the /etc/pam.d/system-auth-generic file: "password required /lib/security/$ISA/pam_passwdqc.so": 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.

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

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COP04
Name	Establish a maximum password aging policy.
Description	These controls govern how long a user password can be active before the user is required to change it.
Risk or Control	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.
Recommendation Level	DMZ
Parameters or Objects Configuration	To set the maximum password age, use the following command: `esxcfg-auth --passmaxdays=n` where n is the maximum number of days for a password to live.
Test	Run the following command to see what the password maximum life setting is set to: `grep -i max_days /etc/login.defs` This number should be compared to your policy.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COP05
Name	Establish a password policy for minimum days before a password is changed.
Description	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.
Risk or Control	This recommendation addresses the risk of passwords being guessed or cracked.
Recommendation Level	DMZ
Parameters or Objects Configuration	`esxcfg-auth --passmindays=n`
Test	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.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COP06
Name	Ensure that vpxuser auto-password change in vCenter meets policy.
Description	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.
Risk or Control	If an attacker obtains the vpxuser password through brute force, the password can be used only for a limited amount of time.
Recommendation Level	DMZ
Parameters or Objects Configuration	Configure the following parameter in the vCenter Server advanced settings in the vSphere Client: vCenterVirtualCenter.VimPasswordExpirationInDays Ensure that the value is set lower than the password aging policy on the COS.

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

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
Parameters or Objects Configuration	Syslog behavior is controlled by the configuration file /etc/syslog.conf. For logs you want to send to a remote log host, add a line with @<loghost.company.com> after the message type, where <loghost.company.com> 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. Example: local6.warning @<loghost.company.com> After modifying the file, tell the syslog daemon to reread it by issuing the following command: kill -SIGHUP `cat /var/run/syslogd.pid` At a minimum, the following files should be logged to a remote syslog server: /var/log/vmkernel /var/log/secure /var/log/messages /var/log/vmware/*log. /var/log/vmware/vpx/vpxa.log

Test	To check that remote logging is configured:
	`cat /etc/syslog.conf | grep @`
	To check that remote logging traffic is permitted outbound from the host:
	`esxcfg-firewall -q | grep 514`
	To check that syslog service is configured to run:
	`chkconfig -list | grep syslog`

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 intruder's actions when reviewing the relevant log files.
Risk or Control	Incorrect time settings might make it difficult to inspect and correlate log files to detect attacks and would make auditing inaccurate.
Recommendation Level	Enterprise

Parameters or Objects Configuration	NTP can be configured on an ESX host using the vSphere Client, or using a remote command line such as vCLI or PowerCLI.
Test	• Query the NTP configuration to make sure that a valid time source has been configured • Make sure that the NTP service is running on the host

Console Hardening

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COH01
Name	Partition the disk to prevent the root file system from filling up.
Description	If the root file system fills up, it can seriously degrade the performance of ESX management capabilities or even make them unresponsive. When you install ESX 4.0, 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 *ESX and vCenter Server Installation Guide* covers disk partitions in more detail (http://pubs.vmware.com/vsp40u1/install/c_esx_partitioning.html#1_9_18_1).
Risk or Control	Prevents a denial of service against the management of that host.
Recommendation Level	Enterprise
Parameters or Objects Configuration	/etc/fstab
Test	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.
Description	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.
Risk or Control	Direct tampering with configuration files could result in undetectable changes.
Recommendation Level	DMZ
Condition or Steps	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.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COH04
Name	Ensure that permissions of important files and utility commands have not been changed from default.
Description	Various files and utilities are installed with particular file permissions to enable certain functionality without requiring unnecessary privilege levels for the user accessing them.
Risk or Control	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.
Recommendation Level	DMZ
Parameters or Objects Configuration	The /usr/sbin/esxcfg-* commands, which are all installed by default with permissions 555. The log files discussed in the previous section, all of which have permissions 600, except for the directory /var/log/vmware/webAccess, which has permissions 755, and the virtual machine log files, which have permissions 644. Certain system commands that have the SUID bit. These commands are listed here: http://pubs.vmware.com/vsp40u1/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 /boot/grub/grub.conf.. See the "Installing VMware ESX" chapter in the *ESX and vCenter Server Installation Guide* 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.
Recommendation Level	SSLF
Parameter Setting	Add the line ~~:S:wait:/sbin/sulogin to /etc/inittab
Effect on Functionality	If the root password is lost, there will be no way to access the system.

PARAMETER ELEMENT	DESCRIPTION
Code Number	COA03
Name	Ensure that root access via SSH is disabled.
Description	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.
Threat	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."
Recommendation Level	Enterprise
Parameter Setting	The line "PermitRootLogin" in the /etc/sshd_conf should be set to "no."
Effect on Functionality	The root user will not be able to log in via SSH.

PARAMETER ELEMENT	DESCRIPTION
Code Number	COA04
Name	Disallow console root login.
Description	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 anyone who wants to access the system to first log in using a regular user account, then use "sudo" or "su" to perform tasks. 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.
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.
Recommendation Level	SSLF
Parameter Setting	To prevent direct root login on the console, modify the file /etc/securetty to be empty. While logged in as root, enter the following command: cat /dev/null > /etc/securetty 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 passwd command.
Effect on Functionality	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
Code Number	COA05
Name	Limit access to the "su" command.
Description	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.
Threat	
Recommendation Level	Enterprise
Parameters or Objects Configuration	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 /etc/pam.d/su. 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 auth required and remove the leading pound sign (#) so it reads: auth required /lib/security/$ISA/pam_wheel.so use_uid

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/.

CONFIGURATION ELEMENT	DESCRIPTION
Code Number	COA06
Name	Configure and use “sudo” to control administrative access.
Description	The “sudo” utility should be used to control which privileged commands users can run while logged in to the service console.
Risk or Control	
Recommendation Level	Enterprise
Parameters or Objects Configuration	Parameters to be configured are in the /etc/sudoers file. 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. Because each situation will be different, each configuration will be different, so no specific guidance can be given here.
Test	Check the configuration in the /etc/sudoers file and ensure that it meets your policy.

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