CENTER FOR INTERNET SECURITY

ARCHIVE

CIS VMware ESXi 5.1 Benchmark

v1.0.1 - 06-23-2014

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for VMware ESXi 5.1. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware ESXi 5.1 Update 2.

Consensus Guidance

This benchmark was created using a consensus review process comprised subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - Intended for environments or use cases where security is paramount.
  - Act as defense in depth measures.
  - May negatively inhibit the utility or performance of the technology.

Acknowledgements

The VMware vSphere 5.1 Hardening Guide was an excellent resources in the development of this Benchmark. CIS extends special recognition to the development team of that comprehensive guide. Readers are encouraged to visit http://vmware.com/go/securityguide and http://blogs.vmware.com/vsphere/author/mfoley to download VMware's hardening guide and other free security resources made available by VMware.

Additional special recognition to Mike Foley as the principal author of the VMware's vSphere 5.1 Hardening Guide and to Jordan Rakoske and Iben Rodriguez for their significant contributions to the development of this document.

Recommendations

1 Install

1.1 Keep ESXi system properly patched (Scored)

Profile Applicability:

- Level 1

Description:

VMware Update Manager is a tool used to automate patch management for vSphere hosts and Virtual machines. Creating a baseline for patches is a good way to ensure all hosts are at the same patch level.

Rationale:

By staying up to date on ESXi patches, vulnerabilities in the hypervisor can be mitigated. An educated attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges on an ESXi host.

Audit:

Employ a process to keep ESXi hosts up to date with patches in accordance with industry-standards and internal guidelines. VMware Update Manager is an automated tool that can greatly assist with this. VMware also publishes Advisories on security patches, and offers a way to subscribe to email alerts for them.

Remediation:

Leverage the VMware Update Manager to test and apply patches as they become available.

Impact:

VMs must be powered off in order to update the host ESXi server.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.update_manager.doc/GUID-EF6BEE4C-4583-4A8C-81B9-5B074CA2E272.html

1.2 Verify Image Profile and VIB Acceptance Levels (Scored)

Profile Applicability:

- Level 1

Description:

The ESXi Image Profiles supports four VIB acceptance levels. A VIB (vSphere Installation Bundle) is a collection of files that are packaged into an archive. The VIB contains a signature file that is used to verify the level of trust.

Rationale:

Verify the ESXi Image Profile to only allow signed VIBs. An unsigned VIB represents untested code installed on an ESXi host.

The ESXi Image profile supports four acceptance levels:

1. VMwareCertified - VIBs created, tested and signed by VMware
2. VMwareAccepted - VIBs created by a VMware partner but tested and signed by VMware
3. PartnerSupported - VIBs created, tested and signed by a certified VMware partner
4. CommunitySupported - VIBs that have not been tested by VMware or a VMware partner.

Community Supported VIBs are not supported and do not have a digital signature. To protect the security and integrity of your ESXi hosts do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts.

Audit:

Perform the following to procedure:

1. Connect to each ESX/ESXi host using the ESXi Shell or vCLI and execute the command "esxcli software acceptance get" to verify the acceptance level is at either "VMware Certified", "VMware Supported", or "PartnerSupported".
2. Connect to each ESX/ESXi host using the vCLI and execute the command "esxcli software vib list" and verify the acceptance level for each VIB is either "VMware Certified", "VMware Supported", or "Partner Supported"

Additionally, the following PowerCLI command may be used:

```
# List the Software AcceptanceLevel for each host
Foreach ($VMHost in Get-VMHost ) {
```

```
$ESXCli = Get-EsxCli -VMHost $VMHost
$VMHost | Select Name, @{N="AcceptanceLevel";E={$ESXCli.software.acceptance.get()}}
}
# List only the vibs which are not at "VMwareCertified" or "VMwareAccepted" or
"PartnerSupported" acceptance level
Foreach ($VMHost in Get-VMHost ) {
$ESXCli = Get-EsxCli -VMHost $VMHost
$ESXCli.software.vib.list() | Where { ($_.AcceptanceLevel -ne "VMwareCertified") -and
($_.AcceptanceLevel -ne "VMwareAccepted") -and ($_.AcceptanceLevel -ne
"PartnerSupported") }
}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set the Software AcceptanceLevel for each host
Foreach ($VMHost in Get-VMHost ) {
$ESXCli = Get-EsxCli -VMHost $VMHost
$ESXCli.software.acceptance.Set("PartnerSupported")
}
```

Default Value:

The default level is PartnerSupported

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.install.doc/GUID-56600593-EC2E-4125-B1A0-065BDD16CF2D.html

1.3 Verify no unauthorized kernel modules are loaded on the host (Scored)

Profile Applicability:

- Level 1

Description:

ESXi hosts by default do not permit the loading of kernel modules that lack valid digital signatures. This feature can be overridden which would result in unauthorized kernel modules to be loaded.

Rationale:

VMware provides digital signatures for kernel modules. By default the ESXi host does not permit loading of kernel modules that lack a valid digital signature. However, this behavior can be overridden allowing unauthorized kernel modules to be loaded. Untested or malicious kernel modules loaded on the ESXi host can put the host at risk for instability and/or exploitation.

Audit:

Each ESXi host should be monitored for unsigned kernel modules. To list all the loaded kernel modules from the ESXi Shell or vCLI run: "esxcli system module list". For each module, verify the signature by running: `esxcli system module get -m <module>`. Secure the host by disabling unsigned modules and removing the offending VIBs from the host.

Additionally, the following PowerCLI command may be used:

```
# List the system modules and Signature Info for each host
Foreach ($VMHost in Get-VMHost ) {
$ESXCli = Get-EsxCli -VMHost $VMHost
$ESXCli.system.module.list() | Foreach {
$ESXCli.system.module.get($_.Name) | Select @{N="VMHost";E={$VMHost}}, Module,
License, Modulefile, Version, SignedStatus, SignatureDigest, SignatureFingerPrint
}
}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# To disable a module:
$ESXCli = Get-EsxCli -VMHost MyHost
$ESXCli.system.module.set($false, $false, "MyModuleName")
```

Note: evacuate VMs and place the host into maintenance mode before disabling kernel modules.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-E9B71B85-FBA3-447C-8A60-DEE2AE1A405A.html http://kb.vmware.com/kb/2042473
2. http://kb.vmware.com/kb/2042473

1.4 Ensure that the Forged Transmits policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the Forged Transmits policy is set to reject.

Rationale:

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. Forged transmissions should be set to accept by default. This means the dvPortgroup 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.

Audit:

1. Verify by using the vSphere Web Client to connect to the vCenter Server and as administrator:
2. Go to Home > Networking.
3. Select each VDS and edit each dvPortgroup connected to active VM's requiring securing.
4. Edit Settings for each PortGroup under Security.
5. Verify that the Forged transmits value is set to "Reject"

Additionally, the following PowerCLI command may be used:

```
# List all dvPortGroups and their Security Settings
Get-VirtualPortGroup -Distributed | Select Name, `
@{N="MacChanges";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept"
} Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) {
"Accept" } Else { "Reject"} }}
```

Remediation:

1. Configure by using the vSphere Web Client to connect to the vCenter Server and as administrator:
2. Go to Home > Networking.
3. Select each VDS and edit each dvPortgroup connected to active VM's requiring securing.
4. Edit Settings for each PortGroup under Security.
5. Set the Forged transmits value to "Reject"

Impact:

This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the dvPortgroups that these applications are connected to.

1.5 Ensure that VDS Netflow traffic is only being sent to authorized collector IP Addresses (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that VDS Netflow traffic is only being sent to authorized collector IP Addresses.

Rationale:

The vSphere vDS can export Netflow information about traffic crossing the vDS. Netflow exports are not encrypted and can contain information about the virtual network making it easier for a MITM attack to be executed successfully. If Netflow export is required, verify that all vDS Netflow target IP Addresses are correct.

Audit:

1. From the Web or vSphere Clients, verify that Netflow destinations are correct.
2. Edit the VDS properties.
3. In the Netflow tab, verify the Collector Settings > IP Address and Port.

Remediation:

1. From the Web or vSphere Clients.
2. Configure the Netflow destinations to be correct.
3. Edit the VDS properties.
4. In the Netflow tab, set the Collector Settings > IP Address and Port.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.networking.doc/GUID-E19FECAD-8629-4E8A-B61C-1F1C16770B3B.html

1.6 Restrict port-level configuration overrides on vDS (Scored)

Profile Applicability:

- Level 1

Description:

Restrict port-level configuration overrides on vDS.

Rationale:

Port-level configuration over-rides are disabled by default. Once enabled, this allows for different security settings to be set from what is established at the Port-Group level. There are cases where particular VM's require unique configurations, but this should be monitored so it is only used when authorized. If over-rides are not monitored, anyone who gains access to a VM with a less secure VDS configuration could exploit that broader access.

Audit:

1. From the Web or vSphere Clients.
2. Verify that Port Mirror destination interfaces are correct.
3. Edit the VDS properties.
4. In the Port Mirror tab, verify the Destination VLAN, Port or Uplink ID's.

Remediation:

1. From the Web or vSphere Clients.
2. Verify that Port Mirror destination interfaces are correct.
3. Edit the VDS properties and in the Port Mirror tab.
4. Configure the Destination VLAN, Port or Uplink ID's.

Default Value:

Port-level configuration over-rides are disabled by default. This is the prescribed state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.networking.doc/GUID-EA78AD26-F099-4136-9EA6-AD60626D3EF7.html

2 Communication

2.1 Configure NTP time synchronization (Scored)

Profile Applicability:

- Level 1

Description:

NTP(Network Time Protocol) synchronization should be configured and enabled on each VMware ESXi host. Verify that the NTP time server is correct for each host to ensure accurate time for system event logs.

Rationale:

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, you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.

Audit:

1. From the vSphere web client select the host
2. Click "Manage" -> "Time Configuration"
3. Click the "Edit..." button.
4. Provide the name/IP of your NTP servers
5. Start the NTP service
6. Change the startup policy to "Start and stop with host"

Notes: verify the NTP firewall ports are open. 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.

Additionally, the following PowerCLI command may be used:

```
# List the NTP Settings for all hosts
Get-VMHost | Select Name, @{N="NTPSetting";E={$_ | Get-VMHostNtpServer}}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set the NTP Settings for all hosts
# If an internal NTP server is used replace pool.ntp.org with
# the IP address of the internal NTP server
$NTPServers = "pool.ntp.org", "pool2.ntp.org" Get-VMHost | Add-VmHostNtpServer
$NTPServers
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vcli.examples.doc/cli_manage_networks.11.9.html

2.2 Configure the ESXi host firewall to restrict access to services running on the host (Scored)

Profile Applicability:

- Level 1

Description:

The ESXi Firewall is enabled by default and allows ping (ICMP) and communication with DHCP/DNS clients. Confirm that access to services are only allowed by authorized IP's/networks to protect from outside attacks.

Rationale:

Unrestricted access to services running on an ESXi host can expose a host to outside attacks and unauthorized access. Reduce the risk by configuring the ESXi firewall to only allow access from authorized networks.

Audit:

1. From the vSphere web client
2. Select the host
3. Go to "Manage" -> "Security Profile"
4. In the "Firewall" section select "Edit...".
5. For each enabled service, (e.g. ssh, vSphere Web Access, http client) provide a range of allowed IP addresses.

Additionally, the following PowerCLI command may be used:

```
# List all services for a host
Get-VMHost HOST1 | Get-VMHostService
# List the services which are enabled and have rules defined for specific IP ranges to
access the service
Get-VMHost HOST1 | Get-VMHostFirewallException | Where {$_.Enabled -and (-not
$_.ExtensionData.AllowedHosts.AllIP)}
# List the services which are enabled and do not have rules defined for specific IP
ranges to access the service
Get-VMHost HOST1 | Get-VMHostFirewallException | Where {$_.Enabled -and
($_.ExtensionData.AllowedHosts.AllIP)}
```

Remediation:

To implement the recommended configuration state, run the following ESXi shell command:

```
# /etc/init.d/[SERVICE] STOP
```

Impact:

Only systems in the IP whitelist/ACL will be able to connect to services on the ESXi server.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-DD4322FF-3DC4-4716-8819-6688938F99D7.html

2.3 Disable Managed Object Browser (MOB) (Scored)

Profile Applicability:

- Level 1

Description:

The Managed Object Browser (MOB) is a web-based server application that lets you examine objects that exist on the server side. This is installed and started automatically when vCenter is installed.

Rationale:

The managed object browser (MOB) 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 meant to be used primarily for debugging the vSphere SDK. Because there are no access controls the MOB could also be used as a method to obtain information about a host being targeted for unauthorized access.

Audit:

To determine if the MOB is enabled run the following command from the ESXi shell:

```
vim-cmd proxysvc/service_list
```

Remediation:

To implement the recommended configuration state, run the following ESXi shell command:

```
vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"
```

Note: You cannot disable the MOB while a host is in lockdown mode.

Impact:

The MOB will no longer be available for diagnostics. Some 3rd party tools use this interface to gather information. Testing should be done after disabling the MOB to verify 3rd party applications are still functioning as expected.

To re-enable the MOB temporarily: ~ # vim-cmd proxysvc/add_np_service "/mob" httpsWithRedirect /var/run/vmware/proxy-mob

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-0EF83EA7-277C-400B-B697-04BDC9173EA3.html

2.4 Do not use default self-signed certificates for ESXi communication (Scored)

Profile Applicability:

- Level 1

Description:

The default certificates are not signed by a commercial certificate authority (CA). These default x.509 certificates should be replaced with those issued by a trusted CA.

Rationale:

Using the default self-signed certificates may increase risk related to Man-in-The-Middle (MiTM) attacks. Replace default self-signed certificates with those from a trusted CA, either commercial or organizational.

Audit:

View the details of the SSL certificate presented by the ESXi host and determine if it is issued by a trusted CA, either commercial or organizational.

Remediation:

Leverage VMware's SSL Certificate Automation Tool to install CA-signed SSL certificates. Fore more information on this tool, please see http://kb.vmware.com/kb/2041600.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-A261E6D8-03E4-48ED-ADB6-473C2DAAB7AD.html
2. http://kb.vmware.com/kb/2015499
3. http://kb.vmware.com/kb/2034833

2.5 Enable SSL for Network File copy (NFC) (Scored)

Profile Applicability:

- Level 2

Description:

Enable SSL encryption for the Network File Copy function used during Virtual Machine migration or clone operations between two ESXi hosts.

Rationale:

NFC (Network File Copy) is the name of the mechanism used to migrate or clone a VM between two ESXi hosts over the network. By default, SSL is used only for the authentication of the transfer, but if desired, SSL can also be enabled on the data transfer. Without this setting VM contents could potentially be sniffed if the management network is not adequately isolated and secured.

Audit:

Perform the following:

1. From the vSphere client select "Administration -> vCenter Server Settings -> Advanced Settings"
2. Check if the `config.nfc.useSSL` key exists and is set to `true`

Additionally, the following PowerCLI command may be used:

```
# Check Network File Copy NFC uses SSL. OS Administrator Privileges will
# be needed on your server for this to complete
$vCenter = "<MyvCenterFQDN>"
[XML]$file = Get-Content "\\$vCenter\C$\ProgramData\VMware\VMware
VirtualCenter\vpxd.cfg"
if ($file.config.nfc.Usessl) { "SSL Setting is compliant" } Else { "SSL Setting is not
set or is unreadable"}
```

Remediation:

Perform the following:

1. From the vSphere client select "Administration -> vCenter Server Settings -> Advanced Settings"
2. Check if the config.nfc.useSSL key exists
3. If the key does not exist, add it to the list of keys
4. Set the value of the key to `true`

Impact:

Using SSL may reduce performance of actions involving NFC, such as VM clone or migration.

Default Value:

The prescribed state is not the default state.

References:

1. http://kb.vmware.com/kb/2010332

2.6 Ensure proper SNMP configuration (Scored)

Profile Applicability:

- Level 1

Description:

Verify that SNMP (Simple Network Management Protocol) is configured and that all the settings are correct. If SNMP is not being used, it should be disabled.

Note: ESXi 5.1 supports SNMPv3 which provides stronger security than SNMPv1 or SNMPv2, including key authentication and encryption.

Rationale:

If SNMP is not being used, it should remain disabled. If it is being used, the proper trap destination should be configured. If SNMP is not properly configured, monitoring information can be sent to a malicious host.

Audit:

Perform the following:

1. From the ESXi Shell or vCLI run the following to determine if SNMP is being used:

```
esxcli system snmp get
```

2. If SNMP is not being used, make sure that it is disabled by running:

```
esxcli system snmp set --enable false.
```

3. If SNMP is being used, refer to the vSphere Monitoring and Performance guide, chapter 8 for steps to configure the required parameters.

Additionally, the following PowerCLI command may be used:

```
# List the SNMP Configuration of a host (single host connection required)
Get-VMHost | Get-VMHostSnmp
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Update the host SNMP Configuration (single host connection required)
Get-VmHostSNMP | Set-VMHostSNMP -Enabled:$true -ReadOnlyCommunity '<secret>'
```

Notes:

- SNMP must be configured on each ESXi host
- SNMP settings can be configured using Host Profiles

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.monitoring.doc/GUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html

2.7 Prevent unintended use of dvfilter network APIs (Scored)

Profile Applicability:

- Level 1

Description:

Confirm that dvfilter API is not configured if not is use. If you are using virtual security appliances that leverage this API then configuration may be necessary.

Rationale:

If you are not using products that make use of the dvfilter network API (e.g. VMSafe), the host should not be configured to send network information to a VM. If the API is enabled, an attacker might attempt to connect a VM to it, thereby potentially providing access to the network of other VMs on the host. If you are using a product that makes use of this API then verify that the host has been configured correctly.

Audit:

If a dvfilter-based network security appliance is not being used on the host, ensure that the following kernel parameter has a blank value: `/Net/DVFilterBindIpAddress`.

1. From the vSphere web client select the host and click "Manage" -> "Advanced System Settings".
2. Enter `Net.DVFilterBindIpAddress` in the filter.
3. Verify `Net.DVFilterBindIpAddress` has an empty value.

4. If an appliance is being used, then make sure the value of this parameter is set to the proper IP address.

Additionally, the following PowerCLI command may be used:

```
# List Net.DVFilterBindIpAddress for each host
Get-VMHost | Select Name, @{N="Net.DVFilterBindIpAddress";E={$_ | Get-
VMHostAdvancedConfiguration Net.DVFilterBindIpAddress | Select -ExpandProperty
Values}}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set Net.DVFilterBindIpAddress to null on all hosts
Get-VMHost HOST1 | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Net.DVFilterBindIpAddress -Value "" }
```

Impact:

This will prevent a dvfilter-based network security appliance such as a firewall from functioning if not configured correctly.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.ext_solutions.doc/GUID-6013E15D-92CE-4970-953C-ACCB36ADA8AD.html

2.8 When adding ESXi hosts to Active Directory use the vSphere Authentication Proxy to protect passwords (Scored)

Profile Applicability:

- Level 1

Description:

If you are using Host Profiles to join ESXi hosts to Active Directory then vSphere Authentication Proxy should be used to keep credentials from being sent over the network.

Rationale:

If you configure your host to join an Active Directory domain using Host Profiles the active directory credentials are saved in the host profile and are transmitted over the network. To avoid having to save active directory credentials in the Host Profile and to avoid transmitting active directory credentials over the network use the vSphere Authentication Proxy.

Audit:

Perform the following:

1. From the vSphere web client, navigate to "Host Profiles"
2. Select the host profile.
3. Select "Manage" -> "Edit Host profile".
4. Expand "Security and Services" -> "Security Settings" -> "Authentication Configuration".
5. Select "Active Directory configuration".
6. Ensure "Join Domain Method" is set to "Use vSphere Authentication Proxy to add the host do domain".

Additionally, the following PowerCLI command may be used:

```
# Ensure the host profile is using vSphere Authentication proxy to add the host to the
# domain
Get-VMHost | Select Name, `
@{N="HostProfile";E={$_ | Get-VMHostProfile}}, `
@{N="JoinADEnabled";E={($_ | Get-
VmHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory.Enable
d}}, `
@{N="JoinDomainMethod";E={(($_ | Get-
VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirectory |
Select -ExpandProperty Policy | Where {$_.Id -eq
"JoinDomainMethodPolicy"}).Policyoption.Id}}
# Check each host and their domain membership status
Get-VMHost | Get-VMHostAuthentication | Select VmHost, Domain, DomainMembershipStatus
```

Remediation:

To implement the recommended configuration state, perform the following:

1. From the vSphere web client, navigate to "Host Profiles"
2. Select the host profile.
3. Select "Manage" -> "Edit Host profile".
4. Expand "Security and Services" -> "Security Settings" -> "Authentication Configuration".
5. Select "Active Directory configuration".
6. Set the "Join Domain Method" to "Use vSphere Authentication Proxy to add the host do domain".

7. Provide the IP address of the authentication proxy.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-084B74BD-40A5-4A4B-A82C-0C9912D580DC.html

3 Logging

3.1 Configure a centralized location to collect ESXi host core dumps (Scored)

Profile Applicability:

- Level 1

Description:

The VMware vSphere Network Dump Collector service allows for collecting diagnostic information from a host that experiences a critical fault.

Rationale:

When a host crashes, an analysis of the resultant core dump is essential to being able to identify the cause of the crash to identify a resolution. Installing a centralized dump collector helps ensure that core files are successfully saved and made available in the event an ESXi host should ever panic.

Audit:

Run the following ESXi shell command to determine if the host is configured as prescribed:

```
esxcli system coredump network get
```

Remediation:

To implement the recommended configuration state, run the following ESXi shell command:

```
# Configure remote Dump Collector Server
esxcli system coredump network set -v [VMK#] -i [DUMP_SERVER] -o [PORT]
# Enable remote Dump Collector
esxcli system coredump network set -e true
```

Impact:

No impact on functionality.

Default Value:

The prescribed state is not the default state.

References:

1. http://kb.vmware.com/kb/1032051 http://kb.vmware.com/kb/2003042

3.2 Configure Host Profiles to monitor and alert on configuration changes (Scored)

Profile Applicability:

- Level 1

Description:

The Host Profiles feature monitors host configurations against an established profile and provides notification when unauthorized configurations take place.

Rationale:

Monitoring for configuration drift and unauthorized changes is critical to ensuring the security of an ESXi hosts. Host Profiles provide an automated method for monitoring host configurations against an established template and for providing notification in the event deviations are detected.

Audit:

There are 3 ways to monitor an ESXi host's compliance to the host profile:

1. Navigate to the Host Profiles list in the vSphere Client.

1. Select the profile to check.
2. In the Hosts and Clusters tab, select the host or cluster from the list under Entity Name.
3. Click Check Compliance Now.
4. The compliance status is updated as Compliant, Unknown, or Non-compliant.

2. Schedule the "Check compliance of a profile" task to run once in the future or multiple times, at a recurring interval. This task checks that a host's configuration matches the configuration specified in a host profile. By default, this interval is set to check once a day.

3. Set the following alarms to alert on various events.

1. Alarm Settings -> Alarm Type: "Hosts" -> "Monitor for specific events" -> Triggers: "Host profile applied", "Host compliant with profile", "Host noncompliant with profile"
2. Alarm Settings -> Alarm Type: "Clusters" -> "Monitor for specific events" -> Triggers: "Cluster compliance checked"

Remediation:

Perform the following:

1. Configure a reference ESXi host with the desired configuration and use the host to create a Host Profile.
2. Attach the host profile to other hosts with identical hardware configurations.
3. Monitor hosts compliance to the host profile from the vSphere Client.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.hostprofiles.doc/GUID-78BB234A-D735-4356-9CCF-19DD55DB8060.html

3.3 Configure persistent logging for all ESXi host (Scored)

Profile Applicability:

- Level 1

Description:

System logs are required for auditing and diagnostic purposes. If you do not store system logs permanently, for example on a datastore, they disappear after a reboot. Ensuring persistent logging is set can prevent the loss of logs on reboot.

Rationale:

ESXi can be configured to store log files on an in-memory file system. This occurs when the host's `/scratch` directory is linked to `/tmp/scratch`. When this is done only a single day's worth of logs are stored at any time, in addition log files will be reinitialized upon each reboot. This presents a security risk as user activity logged on the host is only stored temporarily and will not be preserved across reboots. This can also complicate auditing and make it harder to monitor events and diagnose issues. ESXi host logging should always be configured to a persistent datastore.

Audit:

Perform the following:

1. Logon to the ESXi shell.

2. Run "`ls -al /`" to verify `/scratch` is not linked to `/tmp/scratch`.

Additionally, the following PowerCLI command may be used:

```
# List Syslog.global.logDir for each host
Get-VMHost | Select Name, @{N="Syslog.global.logDir";E={$_ | Get-
VMHostAdvancedConfiguration Syslog.global.logDir | Select -ExpandProperty Values}}
```

Remediation:

Perform the following:

1. Logon to the ESXi shell.
2. Run "`ls -al /`" to verify `/scratch` is not linked to `/tmp/scratch`.
3. If `/scratch` is linked to `/tmp/scratch` change it to a persistent datastore.
4. Identify the datastore path where you want to place scratch.
5. Login to the vSphere web client.
6. Navigating to the host.
7. Select "Manage" -> "Advanced System Settings".
8. Enter `Syslog.global.LogDir` in the filter.
9. Set the `Syslog.global.LogDir` to the desired datastore path.

Alternatively, run the following PowerCLI command:

```
# Set Syslog.global.logDir for each host
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Syslog.global.logDir -Value "<NewLocation>" }
```

Note: the `Syslog.global.LogDir` must be set for each host. The host syslog parameters can also be configured using the vCLI or PowerCLI, or using an API client.

Impact:

Additional disk space will be required to store log files.

Default Value:

When booting from a local disk: YES

When booting from USB/SD: NO

When using Auto Deploy Stateless Installs: NO

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.install.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html http://kb.vmware.com/kb/1033696

3.4 Configure remote logging for ESXi hosts (Scored)

Profile Applicability:

- Level 1

Description:

By default ESXI logs are stored on a local scratch volume or ramdisk. To preserve logs further configure centralized logging for the ESXI hosts.

Rationale:

Remote logging to a central log host provides a secure, centralized store for ESXi logs. By gathering host log files onto a central host you can more 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. Logging to a secure, centralized log server also helps prevent log tampering and also provides a long-term audit record.

Audit:

Perform the following:

1. Install/Enable a syslog host (i.e vSphere Syslog Collector).
2. From the vSphere web client select the host and click "Manage" -> "Advanced Sytem Settings"
3. Enter `Syslog.global.logHost` in the filter.
4. Ensure the `Syslog.global.logHost` to the hostname of your syslog server.

Additionally, the following PowerCLI command may be used:

```
# List Syslog.global.logHost for each host
Get-VMHost | Select Name, @{N="Syslog.global.logHost";E={$_ | Get-
VMHostAdvancedConfiguration Syslog.global.logHost | Select -ExpandProperty Values}}
```

Remediation:

Perform the following:

1. Install/Enable a syslog host (i.e vSphere Syslog Collector).
2. From the vSphere web client select the host and click "Manage" -> "Advanced Sytem Settings"

3. Enter `Syslog.global.logHost` in the filter.
4. Set the `Syslog.global.logHost` to the hostname of your syslog server.

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set Syslog.global.logHost for each host
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
Syslog.global.logHost -Value "<NewLocation>" }
```

Note: When setting a remote log host it is also recommended to set the "Syslog.global.logDirUnique" to true. You must configure the syslog settings for each host. The host syslog parameters can also be configured using the vCLI or PowerCLI, or using an API client.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.install.doc/GUID-471EFE67-9035-473E-8217-6B67E493A518.html

4 Access

4.1 Create a non-root user account for local admin access (Scored)

Profile Applicability:

- Level 1

Description:

Create at least one named user account and use this account in lieu of a shared "root" account.

Rationale:

By default each ESXi host has a single "root" admin account that is used for local administration and to connect the host to vCenter Server. To avoid sharing a common root account it is recommended on each host to create at least one named user account and assign it full admin privileges and to use this account in lieu of a shared "root" account. Set a highly complex password for the "root" account and secure it in a safe location. Limit the use of "root" but do not remove the "root" account.

Audit:

Perform the following:

1. Connect directly to the ESXi host using the vSphere Client.
2. Login as root or another authorized user.
3. Select the "Local Users & Groups" tab and view the local users.
4. Ensure at least one user exists that posses the following:
    1. Shell access has been granted to this user.
    2. Select the "Permissions" tab and verify the "Administrator" role has been granted to the user.
5. Repeat this for each ESXi hosts.

Remediation:

Local ESXi user accounts cannot be created using the vSphere web client, you must use the vSphere client.

1. Connect directly to the ESXi host using the vSphere Client.
2. Login as root.
3. Select the "Local Users & Groups" tab
4. Add a local user, be sure to grant shell access to this user.

5. Select the "Permissions" tab.
6. Assign the "Administrator" role to the user.
7. Repeat this for each ESXi hosts.

Notes:

1. Even if you add your ESXi host to an Active Directory domain it is still recommended to add at least one local user account to ensure admins can still login in the event the host ever becomes isolated and unable to access Active Directory.
2. Adding local user accounts can be automated using Host Profiles.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-670B9B8C-3810-4790-AC83-57142A9FE16F.html

4.2 Ensure the vpxuser account's password is automatically changed every 10 or fewer days (Scored)

Profile Applicability:

- Level 1

Description:

When a host is added to the vCenter Server inventory, vCenter Server creates a special user account called `vpxuser` on the host. `vpxuser` is a privileged account that acts as a proxy for all actions initiated through vCenter Server. Ensure that vpxuser's password is set to change every 10 or fewer days.

Rationale:

Ensuring that the password expires frequently limits the amount of time an attacker can use the `vpxuser` password if it is compromised.

Audit:

From the vSphere web client:

1. Select the vCenter Server and go to "Manage" -> "Advanced Settings".
2. Enter `VimPasswordExpirationInDays` in the filter.
3. Ensure `VirtualCenter.VimPasswordExpirationInDays` is set to 10 or less.

Additionally, the following PowerCLI command may be used:

```
# List the vCenter Password Expiration Value
Get-AdvancedSetting -Entity $defaultVIServer -Name
"VirtualCenter.VimPasswordExpirationInDays"
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set the vCenter Password Expiration Value to 10
Get-AdvancedSetting -Entity $defaultVIServer -Name
"VirtualCenter.VimPasswordExpirationInDays" | Set-AdvancedSetting -Value 10
```

Impact:

The password aging policy must not be shorter than the interval that is set to automatically change the `vpxuser` password, otherwise vCenter might get locked out of an ESXi host.

Default Value:

Password automatically changes every 30 days.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-96210743-0C17-4AE9-89FC-76778EC9D06E.html

4.3 Establish a password policy for password complexity (Scored)

Profile Applicability:

- Level 1

Description:

Require the use of passwords that are not easily guessed and that are difficult for password generators to determine.

Rationale:

ESXi uses the `pam_passwdqc.so` plug-in to set password strength and complexity. It is important to use passwords that are not easily guessed and that are difficult for password generators to determine.

Note: ESXi imposes no restrictions on the root password. Password strength and complexity rules only apply to non-root users.

Audit:

Perform the following:

1. Login to the ESXi shell as a user with administrator privileges.
2. Open `/etc./pam.d/passwd`
3. Locate the following line:

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=N
min=N0,N1,N2,N3,N4
```

4. Confirm N is less than or equal to 5
5. Confirm N0 is set to `disabled`
6. Confirm N1 is set to `disabled`
7. Confirm N2 is set to `disabled`
8. Confirm N3 is set to `disabled`
9. Confirm N4 is set to `14` or greater

This above requires all passwords to be 14 or more characters long and comprised of at least one character from four distinct character sets. Additionally, a maximum of 5 login attempts are permitted.

Remediation:

Perform the following:

1. Login to the ESXi shell as a user with administrator privileges.
2. Open `/etc./pam.d/passwd`
3. Locate the following line:

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=N
min=N0,N1,N2,N3,N4
```

4. Set N is less than or equal to 5
5. Set N0 to `disabled`
6. Set N1 to `disabled`
7. Set N2 to `disabled`
8. Set N3 to `disabled`

9. Set N4 to `14` or greater

This above requires all passwords to be 14 or more characters long and comprised of at least one character from four distinct character sets. Additionally, a maximum of 5 login attempts are permitted.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-F48903DA-8A66-47C7-9796-CD12339B2164.html
2. http://www.openwall.com/passwdqc/README.shtml

4.4 Use Active Directory for local user authentication (Scored)

Profile Applicability:

- Level 1

Description:

ESXi can be configured to use a directory service such as Active Directory to manage users and groups. It is recommended that a directory service be used.

Rationale:

Joining ESXi hosts to an Active Directory (AD) domain will eliminate the need to create and maintain multiple local user accounts. Using AD for user authentication simplifies the ESXi host configuration, ensures password complexity and reuse policies are enforced and reduces the risk of security breaches and unauthorized access.

Audit:

Execute the following PowerCLI command:

```
# Check each host and their domain membership status
Get-VMHost | Get-VMHostAuthentication | Select VmHost, Domain, DomainMembershipStatus
```

Remediation:

From the vSphere Web Client:

1. Select the host and go to "Manage" -> "Authentication Services" and click the "Join Domain" button.
2. Provide the domain name along with the user credentials for an AD user that has the rights to join computers to the domain.

To implement the recommended configuration state, run the following PowerCLI command:

```
# Join the ESXI Host to the Domain
Get-VMHost HOST1 | Get-VMHostAuthentication | Set-VMHostAuthentication -Domain
domain.local -User Administrator -Password Passw0rd -JoinDomain
```

Notes:

1. Host Profiles can be used to automate adding hosts to an AD domain.
2. Consider using the vSphere Authentication proxy to avoid transmitting AD credentials over the network.
3. If the AD group "ESX Admins" (default) is created all users and groups that are assigned as members to this group will have full administrative access to all ESXi hosts the domain.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-A61A8FA4-A4AF-475C-860E-3FD8947F0D0B.html http://kb.vmware.com/kb/1025569.

4.5 Verify Active Directory group membership for the "ESX Admins" group (Not Scored)

Profile Applicability:

- Level 1

Description:

The AD group used by vSphere is defined by the `esxAdminsGroup` attribute. By default, this attribute is set to "ESX Admins". All members of the "ESX Admins" group are granted full administrative access to all ESXi hosts in the domain. Monitor AD for the creation of this group and limit membership to highly trusted users and groups.

Rationale:

An unauthorized user having membership in the group set by the `esxAdminsGroup` attribute will have full administrative access to all ESXi hosts. Given this, such users may compromise the confidentiality, availability, and integrity of the all ESXi hosts and the respective data and processes they influence.

Audit:

From Active Directory, monitor the membership of the group name that is defined by the advanced host setting: `Config.HostAgent.plugins.hostsvc.esxAdminsGroup`. As with any default group, consider changing this name to avoid possible exploits) and verify only authorized user and group accounts are members of this group.

If full admin access for the AD ESX admins group is not desired you can disable this behavior using the advanced host setting:
"`Config.HostAgent.plugins.hostsvc.esxAdminsGroupAutoAdd`"

Remediation:

1. Verify the setting of the `esxAdminsGroup` attribute ("ESX Admins" by default).
2. Check the list of members for that Microsoft Active Directory group.
3. Remove any unauthorized users from that group.

Impact:

Coordination between vSphere admins and Active Directory admins is needed.

Default Value:

The AD group used by vSphere is defined by the `esxAdminsGroup` attribute. By default, this attribute is set to "ESX Admins"

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.host.AuthenticationManager.html

5 Console

5.1 Disable DCUI to prevent local administrative control (Scored)

Profile Applicability:

- Level 2

Description:

The Direct Console User Interface (DCUI) can be disabled to prevent any local administration from the Host. Once the DCUI is disabled any administration of the ESXi host will be done through vCenter.

Rationale:

The DCUI allows for low-level host configuration such as configuring IP address, hostname and root password as well as diagnostic capabilities such as enabling the ESXi shell, viewing log files, restarting agents, and resetting configurations. Actions performed from the DCUI are not tracked by vCenter Server. Even if Lockdown Mode is enabled, users who are members of the DCUI.Access list can perform administrative tasks in the DCUI bypassing RBAC and auditing controls provided through vCenter. DCUI access can be disabled. Disabling it prevents all local activity and thus forces actions to be performed in vCenter Server where they can be centrally audited and monitored.

Audit:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "Direct Console UI".
6. Very the Startup Policy is set to "Start and Stop Manually".

Additionally, the following PowerCLI command may be used:

```
# List DCUI settings for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "DCUI" }
```

Remediation:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "Direct Console UI".
6. Click "Stop".
7. Change the Startup Policy "Start and Stop Manually".

Additionally, the following PowerCLI command will implement the recommended configuration state:

```
# Set DCUI to start manually rather than automatic for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "DCUI" } | Set-VMHostService -
Policy Off
```

Impact:

Disabling the DCUI can create a potential "lock out" situation should the host become isolated from vCenter Server. Recovering from a "lock out" scenario requires re-installing ESXi. Consider leaving DCUI enabled and instead enable lockdown mode and limit the users allowed to access the DCUI using the DCUI.Access list.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-6779F098-48FE-4E22-B116-A8353D19FF56.html

5.2 Disable ESXi Shell unless needed for diagnostics or troubleshooting (Scored)

Profile Applicability:

- Level 1

Description:

The ESXi shell should only be enabled when running diagnostics or troubleshooting. Otherwise it should be disabled on each host.

Rationale:

ESXi Shell is an interactive command line environment available from the Direct Console User Interface (DCUI) or remotely via SSH. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell should only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere client or vCLI/PowerCLI.

Audit:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "ESXi Shell".
6. Click "Stop".
7. Ensure the Startup Policy is set "Start and Stop Manually"

Additionally, the following PowerCLI command may be used:

```
# Check if ESXi Shell is running and set to start
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM" } | Select VMHost, Key,
Label, Policy, Running, Required
```

Note: A host warning is displayed in the web client anytime the ESXi Shell is enabled on a host.

Remediation:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "ESXi Shell".
6. Click "Stop".
7. Change the Startup Policy "Start and Stop Manually"

Additionally, the following PowerCLI command will implement the recommended configuration state:

```
# Set ESXi Shell to start manually rather than automatic for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM" } | Set-VMHostService -
Policy Off
```

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/2004746

5.3 Disable SSH (Scored)

Profile Applicability:

- Level 1

Description:

Disable Secure Shell (SSH) for each ESXi host to prevent remote access to the ESXi shell. only enable if needed for troubleshooting or diagnostics.

Rationale:

The ESXi shell, when enabled, can be accessed directly from the host console through the DCUI or remotely using SSH. Remote access to the host should be limited to the vSphere Client, remote command-line tools (vCLI/PowerCLI), and through the published APIs. Under normal circumstances remote access to the host using SSH should be disabled.

Audit:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "SSH".
6. Ensure the Startup Policy is set to "Start and Stop Manually".

Additionally, the following PowerCLI command may be used:

```
# Check if SSH is running and set to start
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM-SSH" } | Select VMHost, Key,
Label, Policy, Running, Required
```

Note: A host warning is displayed in the web client anytime SSH is enabled on a host.

Remediation:

Perform the following:

1. From the vSphere web client select the host.
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Services".
4. Click "Edit...".
5. Select "SSH".
6. Click "Stop".
7. Change the Startup Policy "to Start and Stop Manually".

Additionally, the following PowerCLI command will implement the recommended configuration state:

```
# Set SSH to start manually rather than automatic for all hosts
Get-VMHost | Get-VMHostService | Where { $_.key -eq "TSM-SSH" } | Set-VMHostService -
Policy Off
```

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-12E27BF3-3769-4665-8769-DA76C2BC9FFE.html

5.4 Enable lockdown mode to restrict remote access (Scored)

Profile Applicability:

- Level 1

Description:

Lockdown mode disables local access to the ESXi host. All management must be done from vCenter to ensure proper permissions and roles are being applied when using lockdown mode.

Rationale:

Enabling lockdown mode disables direct access to an ESXi host requiring the host be managed remotely from vCenter Server. Lockdown limits ESXi host access to the vCenter server. This is done to ensure the roles and access controls implemented in vCenter are always enforced and users cannot bypass them by logging into a host directly. By forcing all

interaction to occur through vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced. Note: Lockdown mode does not apply to users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH even when the host is in lockdown mode. Note that users listed in the DCUI.Access list for each host are allowed to override lockdown mode and login to the DCUI. By default the "root" user is the only user listed in the DCUI.Access list.

Audit:

From the vSphere web client:

1. Select the host
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Lockdown Mode".
4. Click "Edit...".
5. Ensure the "Enable Lockdown Mode" checkbox is set

Additionally, the following PowerCLI command may be used:

```
# To check if Lockdown mode is enabled
Get-VMHost | Select Name,@{N="Lockdown";E={$_.Extensiondata.Config.adminDisabled}}
```

Remediation:

From the vSphere web client:

1. Select the host
2. Select "Manage" -> "Security Profile".
3. Scroll down to "Lockdown Mode".
4. Click "Edit...".
5. Select the "Enable Lockdown Mode" checkbox.

To implement the recommended configuration state, run the following PowerCLI command:

```
# Enable lockdown mode for each host
Get-VMHost | Foreach { $_.EnterLockdownMode() }
```

Impact:

There are some operations, such as backup and troubleshooting, that require direct access to the host. In these cases Lockdown Mode can be disabled on a temporary basis for specific hosts as needed, and then re-enabled when the task is completed.

Note: Lockdown mode does not apply to users listed in the DCUI.Access list, which by default includes the root user.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html http://kb.vmware.com/kb/1008077

5.5 Remove keys from SSH authorized_keys file (Scored)

Profile Applicability:

- Level 1

Description:

For day-to-day operations the ESXi host should be in Lockdown mode with the Secure Shell (SSH) service disabled. Lockdown mode does not prevent root users from logging in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH even when the host is in lockdown mode.

Rationale:

ESXi hosts come with SSH which can be enabled to allow remote access without requiring user authentication. To enable password free access copy the remote users public key into the `/etc/ssh/keys-root/authorized_keys` file on the ESXi host. The presence of the remote user's public key in the `authorized_keys` file identifies the user as trusted, meaning the user is granted access to the host without providing a password.

Note: Lockdown mode does not apply to root users who log in using authorized keys. When you use an authorized key file for root user authentication, root users are not prevented from accessing a host with SSH even when the host is in lockdown mode.

Audit:

To check for SSH keys added to the `authorized_keys` file:

1. Logon to the ESXi shell as root or an authorized admin user.

2. Verify the `/etc/ssh/keys-root/authorized_keys` file is empty.

Remediation:

To check for SSH keys added to the authorized_keys file:

1. Logon to the ESXi shell as root or an authorized admin user.
2. Verify the contents of the `/etc/ssh/keys-root/authorized_keys` file.
3. If the file is not empty remove any keys found in the file.

Impact:

Disabling the SSH `authorized_keys` access may limit your ability to run unattended remote scripts.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-392ADDE9-FD3B-49A2-BF64-4ACBB60EB149.html

5.6 Set a timeout to automatically terminate idle ESXi Shell and SSH sessions (Scored)

Profile Applicability:

- Level 1

Description:

Set a timeout to automatically terminate any idle ESXi shell and SSH sessions.

Rationale:

If a user forgets to logout of their SSH session the idle connection will remain indefinitely increasing the potential for someone to gain privileged access to the host. The `ESXiShellInteractiveTimeOut` allows you to automatically terminate idle shell sessions.

Audit:

From the vSphere web client:

1. Select the host.
2. Click "Manage" -> "Advanced System Settings".
3. Type `ESXiShellInteractiveTimeOut` in the filter.
4. Set the attribute to `300` or less.

Note: A value of 0 disables the ESXi ShellInteractiveTimeOut.

It is recommended to set the `ESXiShellTimeOut` together with `ESXiShellInteractiveTimeOut`.

Additionally, the following PowerCLI command may be used:

```
# List UserVars.ESXiShellInteractiveTimeOut for each host
Get-VMHost | Select Name, @{N="UserVars.ESXiShellInteractiveTimeOut";E={$_ | Get-
VMHostAdvancedConfiguration UserVars.ESXiShellInteractiveTimeOut | Select -
ExpandProperty Values}}
```

Remediation:

From the vSphere web client:

1. Select the host.
2. Click "Manage" -> "Advanced System Settings".
3. Type ESXiShellInteractiveTimeOut in the filter.
4. Set the attribute to the desired value.

Note: A value of 0 disables the ESXi ShellInteractiveTimeOut.

Additionally, the following PowerCLI command will implement the recommended configuration state:

```
# Set Remove UserVars.ESXiShellInteractiveTimeOut to 300 on all hosts
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
UserVars.ESXiShellInteractiveTimeOut -Value 300 }
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-A1D310D7-F00B-4827-9469-EC2C318A0C30.html http://kb.vmware.com/kb/2004746

5.7 Set a timeout for Shell Services (Scored)

Profile Applicability:

- Level 2

Description:

Set a timeout to automatically stop the service for ESXi shell and SSH sessions.

Rationale:

When the ESXi Shell or SSH services are enabled on a host they will run indefinitely. To avoid having these services left running set the `ESXiShellTimeOut`. The `ESXiShellTimeOut` defines a window of time after which the ESXi Shell and SSH services will automatically be terminated.

Audit:

From the vSphere web client:

1. Select the host and click "Manage" -> "Advanced System Settings".
2. Type `ESXiShellTimeOut` in the filter.
3. Ensure the attribute is set to 3600 seconds (1 hour) or less. This value is in seconds.

Additionally, the following PowerCLI command may be used:

```
# List UserVars.ESXiShellTimeOut in minutes for each host
Get-VMHost | Select Name, @{N="UserVars.ESXiShellTimeOut";E={$_ | Get-
VMHostAdvancedConfiguration UserVars.ESXiShellTimeOut | Select -ExpandProperty
Values}}
```

Remediation:

From the vSphere web client:

1. Select the host and click "Manage" -> "Advanced System Settings".
2. Type `ESXiShellTimeOut` in the filter.
3. Set the attribute to 3600 seconds (1 hour) or less.

Note: A value of 0 disables the ESXi ShellTimeOut. It is recommended to set the `ESXiShellInteractiveTimeOut` together with `ESXiShellTimeOut`.

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set UserVars.ESXiShellTimeOut to 3660 on all hosts
Get-VMHost | Foreach { Set-VMHostAdvancedConfiguration -VMHost $_ -Name
UserVars.ESXiShellTimeOut -Value 3600 }
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-862CA8EF-C8CE-4322-864E-86D0803015A5.html
2. https://blogs.vmware.com/vsphere/2012/09/vsphere-5-1-new-esxishellinteractivetimeout.html
3. http://kb.vmware.com/kb/2004746

5.8 Set DCUI.Access to allow trusted users to override lockdown mode (Not Scored)

Profile Applicability:

- Level 1

Description:

Create a list of highly trusted users that would be able to override lockdown mode and access the DCUI in the event a host became isolated.

Rationale:

Lockdown disables direct host access requiring admins manage hosts from vCenter. However, if a host becomes isolated from vCenter the admin would become locked out and would be unable to manage the host. To avoid potentially becoming locked out of an ESXi hosts that is running in locked down mode set the DCUI.Access to a list of highly trusted users that are allowed to override the lockdown mode and access the DCUI.

Audit:

From the vSphere client:

1. Select the host.
2. Select "Manage" -> "Advanced System Settings".
3. Type "DCUI.Access" in the filter.
4. Set the "DCUI.Access" attribute to a comma separated list the users who are allowed to override lockdown mode.

Notes: By default only the "root" user is a member of the DCUI.Access list. It is not recommended to remove root from the DCUI.Access list as this will revoke the root users admin privileges on the host.

Additionally, the following ESXi shell command may be used:

```
vim-cmd hostsvc/advopt/view DCUI.Access
```

Remediation:

To implement the recommended configuration state, run the following ESXi shell command:

```
vim-cmd hostsvc/advopt/update DCUI.Access string [USERS]
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-D92BB375-9F94-449E-838E-51086C43CF80.html

6 Storage

6.1 Enable bidirectional CHAP authentication for iSCSI traffic (Scored)

Profile Applicability:

- Level 1

Description:

By enabling bidirectional CHAP authentication, an additional level of security enables the initiator to authenticate the target.

Rationale:

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. 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. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.

Audit:

Perform the following:

1. In the vSphere client navigate to the host.
2. Select "Configuration" -> "Storage Adaptors" -> "iSCSI Initiator Properties" -> "CHAP" -> "CHAP (Target Authenticates Host)".
3. Verify "Use Chap" is selected with a Name and a "Secret" configured.

Additionally, the following PowerCLI command may be used:

```
# List Iscsi Initiator and CHAP Name if defined
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Select VMHost, Device,
ChapType, @{N="CHAPName";E={$_.AuthenticationProperties.ChapName}}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set the Chap settings for the Iscsi Adapter
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use desired
parameters here
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html

6.2 Ensure uniqueness of CHAP authentication secrets (Scored)

Profile Applicability:

- Level 1

Description:

CHAP (Challenge-Handshake Authentication Protocol) requires both Client and Host to know the secret (Password) to establish connection. When setting up CHAP ensure each host connects with a unique secret.

Rationale:

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. With a single shared secret, compromise of one host can allow an attacker to authenticate to the storage device.

Audit:

In the vSphere Client:

1. Navigate to the host.
2. Select "Configuration" -> "Storage Adaptors" -> "iSCSI Initiator Properties" -> "CHAP" -> "CHAP (Target Authenticates Host)".
3. Verify that a different authentication secret is configured for each ESXi host.

Additionally, the following PowerCLI command may be used:

```
# List Iscsi Initiator and CHAP Name if defined
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Select VMHost, Device,
ChapType, @{N="CHAPName";E={$_.AuthenticationProperties.ChapName}}
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Set the Chap settings for the Iscsi Adapter
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "Iscsi"} | Set-VMHostHba # Use desired
parameters here
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html

7 vNetwork

This section contains recommendations for configuring aspects of the vNetwork, such as VLANs, vSwitches, and VDSs.

7.1 VDS

This section contains recommendations for configuring vSphere Distributed Switches (VDS).

7.1.1 Disable VDS network healthcheck if not used (Scored)

Profile Applicability:

- Level 1

Description:

Disable VDS network healthcheck if not used.

Rationale:

Network Healthcheck is disabled by default. Once enabled, the healthcheck packets contain information on host#, vds# port#, which an attacker would find useful. It is recommended that network healthcheck be used for troubleshooting, and turned off when troubleshooting is finished.

Audit:

1. Using the vSphere Web Client, select each VDS.
2. Go to Manage > Settings > Health check".
3. Verify that VLAN and MTU Check and Teaming and Failover Check are both disabled.

Remediation:

1. Using the vSphere Web Client.
2. Select each VDS.
3. Go to Manage > Settings > Health check".
4. Disable the VLAN and MTU Check and Teaming and Failover Check settings.

Impact:

Limit the use of this feature only to when actively troubleshooting VLAN or MTU issues on a VDS.

Default Value:

The default value is the prescribed value.

7.1.2 Ensure that the MAC Address Change policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the MAC Address Change policy is set to reject.

Rationale:

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. This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the dvPortgroups that these applications are connected to.

Audit:

1. Verify by using the vSphere Client to connect to the vCenter Server and logging in as an administrator.
2. Go to "Home > Inventory > Networking".
3. Select each dvPortgroup connected to active VMs requiring securing.
4. Go to tab "Summary > Edit Settings > Policies > Security".
5. "Mac Address Changes" = "Reject"

Additionally, the following PowerCLI command may be used:

```
# List all dvPortGroups and their Security Settings
Get-VirtualPortGroup -Distributed | Select Name, `
@{N="MacChanges";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept"
} Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if
```

```
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) {
"Accept" } Else { "Reject"} }}
```

Remediation:

1. Configure by using the vSphere Client to connect to the vCenter Server and logging in as an administrator.
2. Go to "Home > Inventory > Networking".
3. Select each dvPortgroup connected to active VMs requiring securing.
4. Go to tab "Summary > Edit Settings > Policies > Security".
5. Set "Mac Address Changes" = "Reject"

Impact:

This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. This will also affect applications that require a specific MAC address for licensing. An exception should be made for the dvPortgroups that these applications are connected to.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.host.NetworkPolicy.SecurityPolicy.html

7.1.3 Ensure that the Promiscuous Mode policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Configure the vDS Promiscuous Mode setting to reject.

Rationale:

When promiscuous mode is enabled for a dvPortgroup, all virtual machines connected to the dvPortgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that dvPortgroup. Promiscuous mode is disabled by default on the ESXi host, and this is the recommended setting. However, there might be a

legitimate reason to enable it for debugging, monitoring or troubleshooting reasons. Security devices might require the ability to see all packets on a vSwitch. An exception should be made for the dvPortgroups that these applications are connected to, in order to allow for full-time visibility to the traffic on that dvPortgroup.

Audit:

1. Verify by using the vSphere Client to connect to the vCenter Server and logging in as an administrator.
2. Go to "Home > Inventory > Networking".
3. Select each dvPortgroup connected to active VM's requiring securing.
4. Go to tab "Summary > Edit Settings > Policies > Security".
5. Configure "Promiscuous Mode" = "Reject"

Additionally, the following PowerCLI command may be used:

```
# List all dvPortGroups and their Security Settings
Get-VirtualPortGroup -Distributed | Select Name, `
@{N="MacChanges";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.MacChanges.Value) { "Accept"
} Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.AllowPromiscuous.Value) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if
($_.ExtensionData.Config.DefaultPortConfig.SecurityPolicy.ForgedTransmits.Value) {
"Accept" } Else { "Reject"} }}
```

Remediation:

1. Verify by using the vSphere Client to connect to the vCenter Server and logging in as an administrator.
2. Go to "Home > Inventory > Networking".
3. Select each dvPortgroup connected to active VMs requiring securing.
4. Go to tab "Summary > Edit Settings > Policies > Security".
5. Configure "Promiscuous Mode" = "Reject"

Impact:

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.

Default Value:

Promiscuous mode is disabled by default. This is the prescribed setting.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.host.NetworkPolicy.SecurityPolicy.html

7.1.4 Ensure that there are no unused ports on a distributed virtual port group (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that there are no unused ports on a distributed virtual port group.

Rationale:

The number of ports available on a vdSwitch distributed port group can be adjusted to exactly match the number of virtual machine vNICs that need to be assigned to that dvPortgroup. Limiting the number of ports to just what is needed limits the potential for an administrator, either accidentally or maliciously, to move a virtual machine to an unauthorized network. This is especially relevant if the management network is on a dvPortgroup, because it could help prevent someone from putting a rogue virtual machine on this network.

Audit:

1. Connect to the vCenter Server with vSphere Client.
2. Navigate to Home > Inventory > Networking.
3. Find all dvSwitches.
4. Verify that the number of ports available total is only the amount required for legitimate virtual machine connections to that dvPortgroup.

Additionally, the following PowerCLI command may be used:

```
# Check for the number of free ports on all VDS PortGroups
Function Get-FreeVDSPort {
Param (
[parameter(Mandatory=$true,ValueFromPipeline=$true)]
$VDSPG
)
Process {
$nicTypes =
"VirtualE1000","VirtualE1000e","VirtualPCNet32","VirtualVmxnet","VirtualVmxnet2","Virt
ualVmxnet3"
$ports = @{}
$VDSPG.ExtensionData.PortKeys | Foreach {
$ports.Add($_,$VDSPG.Name)
```

```
}

$VDSPG.ExtensionData.Vm | Foreach {
$VMView = Get-View $_
$nic = $VMView.Config.Hardware.Device | where {$nicTypes -contains $_.GetType().Name -
and $_.Backing.GetType().Name -match "Distributed"}
$nic | where {$_.Backing.Port.PortKey} | Foreach
{$ports.Remove($_.Backing.Port.PortKey)}
}
($ports.Keys).Count
}
}
Get-VirtualPortGroup -Distributed | Select Name, @{N="NumFreePorts";E={Get-FreeVDSPort
-VDSPG $_}}
```

Remediation:

1. Connect to the vCenter Server with vSphere Client (Home > Inventory > Networking view, find all dvSwitches) or the Web Client (Networking > vDS name > dvPortgroup name > Manage > Edit Settings > General)
2. Configure the number of ports available to be only the amount required for legitimate virtual machine connections to that dvPortgroup.

Impact:

The VDS or dvPortgroup on the VDS will not have any extra available port capacity.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.dvs.DistributedVirtualPortgroup.html

7.1.5 Ensure that VDS Port Mirror traffic is only being sent to authorized collector ports or VLANs (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that VDS Port Mirror traffic is only being sent to authorized collectors.

Rationale:

The vSphere VDS can mirror traffic from one port to another in order to allow for packet capture devices to collect specific traffic flows. Port mirroring will send a copy of all traffic specified in un-encrypted format. This mirrored traffic contains the full data in the packets

captured and can result in total compromise of that data if misdirected. If Port Mirroring is required, verify that all Port Mirror Destination VLAN, Port and Uplink ID's are correct.

Audit:

1. From the Web or vSphere Clients.
2. Verify that Port Mirror destination interfaces are correct.
3. Edit the VDS properties and in the Port Mirror tab.
4. Verify the Destination VLAN, Port, and Uplink ID's.

Remediation:

1. From the Web or vSphere Clients.
2. Configure the Port Mirror destination interfaces to be correct.
3. Edit the VDS properties.
4. In the Port Mirror tab, configure the Destination VLAN, Port, and Uplink ID's.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.networking.doc/GUID-CFFD9157-FC17-440D-BDB4-E16FD447A1BA.html

7.1.6 Verify that the autoexpand option for VDS dvPortgroups is disabled (Scored)

Profile Applicability:

- Level 1

Description:

Disable the autoexpand option for vDS dvPortgroups.

Rationale:

If the "no-unused-dvports" guideline is followed, there should be only the exact number of ports on a vDS that are actually needed. The Autoexpand feature on vDS dvPortgroups can override that limit. The feature allows dvPortgroups to automatically add 10 virtual distributed switch ports to a dvPortgroup that has run out of available ports. The risk is that maliciously or inadvertently, a virtual machine that is not supposed to be part of that portgroup is able to affect confidentiality, integrity or authenticity of data of other virtual machines on that portgroup. To reduce the risk of inappropriate dvPortgroup access, the

autoexpand option on VDS should be disabled. By default the option is disabled, but regular monitoring should be implemented to verify this has not been changed.

Audit:

1. Connect to the vCenter Server using the Web Client.
2. Open the settings for Networking > (vDS name) > (dvPortgroup name) > Manage > Edit Settings > General
3. Verify that "Port allocation" is set to "Fixed".
4. Verify that the "Number of Ports" is set to the exact amount required for legitimate virtual machine connections to that dvPortgroup.

Additionally, the following PowerCLI command may be used:

```
# Check if auto expand is enabled on vDS
Get-VirtualPortGroup -Distributed | Select Name,
@{N="AutoExpand";E={$_.ExtensionData.Config.AutoExpand}}
```

Remediation:

1. Connect to the vCenter Server using the Web Client.
2. Open the settings for Networking > (vDS name) > (dvPortgroup name) > Manage > Edit Settings > General
3. Configure "Port allocation" to "Fixed".
4. Configure the "Number of Ports" to the exact amount required for legitimate virtual machine connections to that dvPortgroup.

Default Value:

The default state is the prescribed state.

References:

1. http://kb.vmware.com/kb/1022312

7.2 VLAN

This section contains recommendations for VLAN configuration.

7.2.1 Ensure that port groups are not configured to the value of the native VLAN (Scored)

Profile Applicability:

- Level 1

Description:

Do not use Native VLAN ID 1.

Rationale:

ESXi 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 ESXi specified as VLAN 1 will be tagged with a 1; therefore, traffic from ESXi 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). If the ESXi virtual switch port group uses the native VLAN ID, traffic from those VMs will not be visible to the native VLAN on the switch, because the switch is expecting untagged traffic.

Audit:

If the default value of 1 for the native VLAN is being used, the ESXi 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.

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches, their Portgroups and VLAN Ids
Get-VirtualPortGroup -Standard | Select virtualSwitch, Name, VlanID
```

Remediation:

If the default value of 1 for the native VLAN is being used, the ESXi 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.

7.2.2 Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT) (Scored)

Profile Applicability:

- Level 1

Description:

Don't use VLAN 4095 except for Virtual Guest Tagging (VGT).

Rationale:

When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest VM without modifying the VLAN tags, leaving it up to the guest to deal with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself. If VGT is enabled inappropriately, it might cause denial of service or allow a guest VM to interact with traffic on an unauthorized VLAN.

Audit:

VLAN ID setting on all port groups should not be set to 4095 unless VGT is required.

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches, their Portgroups and VLAN Ids
Get-VirtualPortGroup -Standard | Select virtualSwitch, Name, VlanID
```

Remediation:

VLAN ID setting on all port groups should not be set to 4095 unless VGT is required.

7.2.3 Ensure that port groups are not configured to VLAN values reserved by upstream physical switches (Not Scored)

Profile Applicability:

- Level 1

Description:

Ensure that port groups are not configured to VLAN values reserved by upstream physical switches

Rationale:

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 through 1024 and 4094, while Nexus switches typically reserve 3968 through 4047 and 4094. Check with the documentation for your specific switch. Using a reserved VLAN might result in a denial of service on the network.

Audit:

VLAN ID setting on all port groups should not be set to reserved values of the physical switch.

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches, their Portgroups and VLAN Ids
Get-VirtualPortGroup -Standard | Select virtualSwitch, Name, VlanID
```

Remediation:

VLAN ID setting on all port groups should not be set to reserved values of the physical switch.

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches, their Portgroups and VLAN Ids
Get-VirtualPortGroup -Standard | Select virtualSwitch, Name, VlanID
```

References:

1. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/vlans.html#wp1038758
2. http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/layer2/7x/b_5500_Layer2_Config_7x/b_5500_Layer2_Config_7x_chapter_010.html#con_1143823

7.3 vSwitch

This section contains recommendations for securing vSwitches.

7.3.1 Ensure that the vSwitch Forged Transmits policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Set the vSwitch Forged Transmits policy is set to reject for each vSwitch.

Rationale:

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. 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.

Audit:

Verify by using the vSphere Client to connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch(?) > Properties > Ports > vSwitch > Default Policies > Security"
4. Ensure "Forged Transmits" is set to "Reject"

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches and their Security Settings
Get-VirtualSwitch -Standard | Select VMHost, Name, `
@{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" }
Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) {
"Accept" } Else { "Reject"} }}
```

Remediation:

Verify by using the vSphere Client to connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch(?) > Properties > Ports > vSwitch > Default Policies > Security"
4. Set "Forged Transmits" to "Reject"

Additionally, the following ESXi shell command may be used:

```
# esxcli network vswitch standard policy security set -v vSwitch2 -f false
```

Impact:

This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. 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.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.networking.doc/GUID-74E2059A-CC5E-4B06-81B5-3881C80E46CE.html

7.3.2 Ensure that the vSwitch MAC Address Change policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the MAC Address Change policy within the vSwitch is set to reject.

Rationale:

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. This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. 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.

Audit:

Verify by using the vSphere Client to connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch(?) > Properties > Ports > vSwitch > Default Policies > Security"
4. Ensure "Mac Address Changes" is set to "Reject".

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches and their Security Settings
Get-VirtualSwitch -Standard | Select VMHost, Name, `
@{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" }
Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) {
"Accept" } Else { "Reject"} }}
```

Remediation:

Using the vSphere Client, connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch(?) > Properties > Ports > vSwitch > Default Policies > Security"
4. Set "Mac Address Changes" to "Reject".

Additionally, perform the following to implement the recommended configuration state using the ESXi shell:

```
# esxcli network vswitch standard policy security set -v vSwitch2 -m false
```

Impact:

This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality. An example of an application like this is Microsoft Clustering, which requires systems to effectively share a MAC address. This will also affect how a layer 2 bridge will operate. 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.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.networking.doc/GUID-74E2059A-CC5E-4B06-81B5-3881C80E46CE.html

7.3.3 Ensure that the vSwitch Promiscuous Mode policy is set to reject (Scored)

Profile Applicability:

- Level 1

Description:

Ensure that the Promiscuous Mode Policy within the vSwitch is set to reject.

Rationale:

When promiscuous mode is enabled for a virtual switch all virtual machines connected to the dvPortgroup have the potential of reading all packets crossing that network. Promiscuous mode is disabled by default on the ESXi Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons. Security devices might require the ability to see all packets on a vSwitch. An exception should be made for the dvPortgroups that these applications are connected to, in order to allow for full-time visibility to the traffic on that dvPortgroup.

Audit:

Verify by using the vSphere Client to connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch name > Properties > Ports > vSwitch > Default Policies > Security"

4. Ensure "Promiscuous Mode" is set to "Reject"

Additionally, the following PowerCLI command may be used:

```
# List all vSwitches and their Security Settings
Get-VirtualSwitch -Standard | Select VMHost, Name, `
@{N="MacChanges";E={if ($_.ExtensionData.Spec.Policy.Security.MacChanges) { "Accept" }
Else { "Reject"} }}, `
@{N="PromiscuousMode";E={if ($_.ExtensionData.Spec.Policy.Security.PromiscuousMode) {
"Accept" } Else { "Reject"} }}, `
@{N="ForgedTransmits";E={if ($_.ExtensionData.Spec.Policy.Security.ForgedTransmits) {
"Accept" } Else { "Reject"} }}
```

Remediation:

Using the vSphere Client, connect to the vCenter Server and as administrator:

1. Go to "Home > Inventory > Hosts and clusters".
2. Select each ESXi host with active virtual switches connected to active VM's requiring securing.
3. Go to tab "Configuration > Network > vSwitch name > Properties > Ports > vSwitch > Default Policies > Security"
4. Set "Promiscuous Mode" = "Reject"

Additionally, perform the following to implement the recommended configuration state via the ESXi shell:

```
# esxcli network vswitch standard policy security set -v vSwitch2 -p false
```

Impact:

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.

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/1004099

8 Virtual Machines

8.1 Communication

8.1.1 Disable VM communication through VMCI (Scored)

Profile Applicability:

- Level 1

Description:

Configure the Virtual Machine Communication Interface (VMCI) to restrict VM communication.

Rationale:

If the interface is not restricted, a VM can detect and be detected by all other VMs with the same option enabled within the same host. This might be the intended behavior, but custom-built software can have unexpected vulnerabilities that might potentially lead to an exploit. Additionally, it is possible for a VM to detect how many other VMs are within the same ESXI system by simply registering the VM. This information might also be used for a potentially malicious objective. By default, the setting is FALSE. The VM can be exposed to other VMs within the same system as long as there is at least one program connected to the VMCI socket interface.

Guest-to-guest communications (virtual machine to virtual machine) are deprecated in the vSphere 5.1 release. This functionality will be removed in the next major release. VMware will continue support for host to guest communications.

Audit:

Check virtual machine configuration file and verify that `vmci0.unrestricted` is set to `FALSE`

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "vmci0.unrestricted" | Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "vmci0.unrestricted" -value $false
```

Impact:

Virtual machines will be unable to communicate using VMCI technology.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/ws8x_esx51_vmci_sockets.pdf

8.1.2 Limit informational messages from the VM to the VMX file (Scored)

Profile Applicability:

- Level 1

Description:

Limit informational messages from the virtual machine to the VMX file to avoid filling the datastore and causing a Denial of Service (DoS).

Rationale:

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. Uncontrolled size for the VMX file can lead to denial of service if the datastore is filled.

Audit:

Check virtual machine configuration file and verify that tools.setInfo.sizeLimit is set to `1048576`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "tools.setInfo.sizeLimit" | Select Entity, Name,
Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "tools.setInfo.sizeLimit" -value 1048576
```

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.1.3 Limit sharing of console connections (Scored)

Profile Applicability:

- Level 1

Description:

Limit the max number of console connections to prevent non-administrators from observing the VMs screen.

Rationale:

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. If an administrator in the VM logs in using a VMware remote console during their session, a non-administrator in the VM might connect to the console and observe the administrator's actions. Also, this could result in an administrator losing console access to a virtual machine. For example if a jump box is being used for an open console session, and the admin loses connection to that box, then the console session remains open. Allowing two console sessions permits debugging via a shared session. For highest security, only one remote console session at a time should be allowed.

Audit:

Check virtual machine configuration file and verify that `RemoteDisplay.maxConnections` is set to `1`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "RemoteDisplay.maxConnections" | Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "RemoteDisplay.maxConnections" -value 1
```

Impact:

Only one remote console connection to the VM will be permitted. Other attempts will be rejected until the first session disconnects.

Default Value:

The prescribed state is not the default state.

References:

1. http://kb.vmware.com/kb/2015407

8.2 Devices

8.2.1 Disconnect unauthorized devices - Floppy Devices (Scored)

Profile Applicability:

- Level 1

Description:

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Rationale:

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. Any enabled or connected device represents another potential attack channel.

Audit:

The following parameters should either NOT be present or should be set to FALSE, unless Floppy drives are required: floppyX.present

Additionally, the following PowerCLI command may be used:

```
# Check for Floppy Devices attached to VMs
Get-VM | Get-FloppyDrive | Select Parent, Name, ConnectionState
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Remove all Floppy drives attached to VMs
Get-VM | Get-FloppyDrive | Remove-FloppyDrive
```

Impact:

Virtual machine will need to be powered off to reverse change if any of these devices are needed at a later time.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-822B2ED3-D8D2-4F57-8335-CA46E915A729.html

8.2.2 Disconnect unauthorized devices - CD/DVD Devices (Scored)

Profile Applicability:

- Level 1

Description:

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Rationale:

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. Any enabled or connected device represents another potential attack channel.

Audit:

The following parameters should either NOT be present or should be set to FALSE, unless CD-ROM is required: ideX:Y.present

Additionally, the following PowerCLI command may be used:

```
# Check for CD/DVD Drives attached to VMs
Get-VM | Get-CDDrive
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Remove all CD/DVD Drives attached to VMs
Get-VM | Get-CDDrive | Remove-CDDrive
```

Impact:

Virtual machine will need to be powered off to reverse change if any of these devices are needed at a later time.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-822B2ED3-D8D2-4F57-8335-CA46E915A729.html

8.2.3 Disconnect unauthorized devices - Parallel Devices (Scored)

Profile Applicability:

- Level 1

Description:

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Rationale:

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. Any enabled or connected device represents another potential attack channel.

Audit:

The following parameters should either NOT be present or should be set to FALSE, unless Parallel ports are required: parallelX.present

Additionally, the following PowerCLI command may be used:

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Check for Parallel ports attached to VMs
Get-VM | Get-ParallelPort
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Remove all Parallel Ports attached to VMs
Get-VM | Get-ParallelPort | Remove-ParallelPort
```

Impact:

Virtual machine will need to be powered off to reverse change if any of these devices are needed at a later time.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-822B2ED3-D8D2-4F57-8335-CA46E915A729.html

8.2.4 Disconnect unauthorized devices - Serial Devices (Scored)

Profile Applicability:

- Level 1

Description:

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Rationale:

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. Any enabled or connected device represents another potential attack channel.

Audit:

The following parameters should either NOT be present or should be set to FALSE, unless Serial ports are required: serialX.present

Additionally, the following PowerCLI command may be used:

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Check for Serial ports attached to VMs
Get-VM | Get-SerialPort
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# In this Example you will need to add the functions from this post:
http://blogs.vmware.com/vipowershell/2012/05/working-with-vm-devices-in-powercli.html
# Remove all Serial Ports attached to VMs
Get-VM | Get-SerialPort | Remove-SerialPort
```

Impact:

Virtual machine will need to be powered off to reverse change if any of these devices are needed at a later time.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-822B2ED3-D8D2-4F57-8335-CA46E915A729.html

8.2.5 Disconnect unauthorized devices - USB Devices (Scored)

Profile Applicability:

- Level 1

Description:

Any enabled or connected device represents a potential attack channel. Users and processes without privileges on a virtual machine can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security. Removing unnecessary hardware devices can help prevent attacks.

Rationale:

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. Any enabled or connected device represents another potential attack channel.

Audit:

The following parameters should either NOT be present or should be set to FALSE, unless USB controllers are required: usb.present

Additionally, the following PowerCLI command may be used:

```
# Check for USB Devices attached to VMs
Get-VM | Get-USBDevice
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Remove all USB Devices attached to VMs
Get-VM | Get-USBDevice | Remove-USBDevice
```

Impact:

Virtual machine will need to be powered off to reverse change if any of these devices are needed at a later time.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-822B2ED3-D8D2-4F57-8335-CA46E915A729.html

8.2.6 Prevent unauthorized removal, connection, and modification of devices (Scored)

Profile Applicability:

- Level 1

Description:

Prevent unauthorized removal, connection, and modification of devices.

Rationale:

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.

By default, a rogue user with non-administrator 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 adapter to isolate the virtual machine from its network, which is a denial of service.
- Modify settings on a device.

Audit:

Check virtual machine configuration file and verify that `isolation.device.edit.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.device.edit.disable" | Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.device.edit.disable" -value $true
```

Impact:

Device interaction is blocked inside the guest OS using VMware tools.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-C5898E50-2182-4B71-BADC-C9BFA409FB6C.html
2. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.3 Guest

8.3.1 Disable unnecessary or superfluous functions inside VMs (Not Scored)

Profile Applicability:

- Level 1

Description:

Reduce the number of potential attack vectors by disabling unnecessary system components that are not needed to support the application or service running on the virtual machine.

Rationale:

By disabling unnecessary system components that are not needed to support the application or service running on the system, you reduce the number of parts that can be attacked. VMs often don't require as many services or functions as ordinary physical servers; so when virtualizing, you should evaluate whether a particular service or function is truly needed. Any service running in a VM provides a potential avenue of attack.

Audit:

Verify the following are disabled:

1. Unused services in the operating system. For example, if the system runs a file server, make sure to turn off any Web services.
2. 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 ESXI Configuration Guide.
3. Screen savers. X-Windows if using a Linux, BSD, or Solaris guest operating system.

Remediation:

Some of these steps include:

1. Disable unused services in the operating system. For example, if the system runs a file server, make sure to turn off any Web services.
2. 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 ESXI Configuration Guide.

3. 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.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-6BFA8CA7-610F-4E6B-9FC6-D656917B7E7A.html

8.3.2 Minimize use of the VM console (Not Scored)

Profile Applicability:

- Level 1

Description:

Grant access to the Virtual Machine console only when needed. Use custom roles to provide fine grained permissions.

Rationale:

The VM console enables you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show. The VM console also provides power management and removable device connectivity controls, which might potentially allow a malicious user to bring down a virtual machine. In addition, it also has a performance impact on the service console, especially if many VM console sessions are open simultaneously.

Audit:

Instead of VM console, use native remote management services, such as terminal services and ssh, to interact with virtual machines. Grant VM console access only when necessary.

1. From the vSphere Client, select an object in the inventory.
2. Click the Permissions tab to view the user and role pair assignments for that object.
3. Next, navigate to Administration\Roles section of vCenter.
4. Select the role in question and choose edit to see which effective privileges are enabled.
5. Only Authorized users should have a role which allows them a privilege under the Virtual Machine\Interaction section of the role editor.

Remediation:

By default the vCenter roles "Virtual Machine Power User" and "Virtual Machine Administrator" have the "Virtual Machine.Interaction.Console Interaction" privilege. Do not allow unauthorized individuals to have these roles on a virtual machine or folder of virtual machines.

1. From the vSphere Client, navigate to Administration\Roles section of vCenter.
2. Create a custom role and choose edit to enable only the minimum needed effective privileges.
3. Next, select an object in the inventory.
4. Click the Permissions tab to view the user and role pair assignments for that object.
5. Remove any default "Admin" or "Power User" roles and assign the new custom role as needed.

References:

1. http://www.vmware.com/support/developer/PowerCLI/PowerCLI51/html/Invoke-VMScript.html
2. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-3D47149A-947D-4608-88B3-E5811129EFA8.html

8.3.3 Use secure protocols for virtual serial port access (Not Scored)

Profile Applicability:

- Level 1

Description:

Virtual serial ports allow virtual machines to communicate over the network. Doing so allows you to redirect the virtual serial port connection to a TCP/IP connection on the ESXi host. If virtual serial ports are needed be sure they are configured to use secure protocols.

Rationale:

Serial ports are interfaces for connecting peripherals to the virtual machine. They are often used on physical systems to provide a direct, low-level connection to the console of a server. Serial ports allow for debug level access, which often does not have strong controls like logging or privileges.

Audit:

Check that no clear text protocols are configured:

- tcp - an unencrypted TCP connection (IPv4 or IPv6)
- tcp4 - an unencrypted TCP connection (IPv4 only)
- tcp6 - an unencrypted TCP connection (IPv6 only)
- telnet telnet over TCP without SSL. The virtual machine and remote system can negotiate and use SSL if the remote system supports the telnet authentication option. If not, the connection uses unencrypted text (plain text)

Only these secure protocols should be configured:

- ssl - the equivalent of TCP+SSL
- tcp+ssl - SSL over TCP over IPv4 or IPv6
- tcp4+ssl - SSL over TCP over IPv4
- tcp6+ssl - SSL over TCP over IPv6
- telnet over TCP with SSL. The virtual machine and remote system can negotiate and use SSL if the remote system supports the telnet authentication option. If not, the connection uses unencrypted text (plain text)
- telnets - telnet over SSL over TCP. In this case, SSL negotiation begins immediately and you cannot use the telnet authentication option.

Remediation:

Configuring Virtual Serial Port Communications with Secure Network Protocols:

- ssl - the equivalent of TCP+SSL
- tcp+ssl - SSL over TCP over IPv4 or IPv6
- tcp4+ssl - SSL over TCP over IPv4
- tcp6+ssl - SSL over TCP over IPv6
- telnet over TCP with SSL. The virtual machine and remote system can negotiate and use SSL if the remote system supports the telnet authentication option. If not, the connection uses unencrypted text (plain text)
- telnets - telnet over SSL over TCP. In this case, SSL negotiation begins immediately and you cannot use the telnet authentication option.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.vm.device.VirtualSerialPort.URIBackingInfo.html
2. http://kb.vmware.com/kb/2004954
3. http://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.vsp.doc/virtual_serial_port_using_proxy_Chapter1.3.2.html

8.3.4 Use templates to deploy VMs whenever possible (Not Scored)

Profile Applicability:

- Level 1

Description:

Use a hardened base operating system template image to create other, application-specific templates and use the application-specific templates to deploy virtual machines.

Rationale:

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. Manual installation of the OS and applications into a VM introduces the risk of misconfiguration due to human or process error.

Audit:

Verify that new virtual machine deployments are completed using hardened, patched, and properly configured OS templates.

Remediation:

Provide templates for VM creation that contain hardened, patched, and properly configured OS deployments. If possible, pre-deploy applications in templates as well, although care should be taken that the application doesn't depend upon VM-specific information to be deployed. In vSphere, you can convert a template to a virtual machine and back again quickly, which makes updating templates quite easy.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vm_admin.doc/GUID-9062F225-E01B-42BA-8AFB-8EA4069068FE.html

8.4 Monitor

8.4.1 Control access to VMs through the dvfilter network APIs (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure VMs protected by dvfilter network APIs correctly.

Rationale:

A VM must be configured explicitly to accept access by the dvfilter network API. This should be done only for VMs for which you want this to be done. An attacker might compromise the VM by making use of this introspection channel.

Audit:

If a VM is supposed to be protected:

- Verify that the following in its VMX file: `ethernet0.filter1.name = dv-filter1` where `ethernet0` is the network adapter interface of the virtual machine that is to be protected, `filter1` is the number of the filter that is being used, and `dv-filter1` is the name of the particular data path kernel module that is protecting the VM.
- Ensure that the name of the data path kernel is set correctly.

If a VM is not supposed to be protected:

- Verify that the following is not in its VMX file: `ethernet0.filter1.name = dv-filter1` where `ethernet0` is the network adapter interface of the virtual machine that is to be protected, `filter1` is the number of the filter that is being used, and `dv-filter1` is the name of the particular data path kernel module that is protecting the VM.

Remediation:

If a VM is supposed to be protected:

- Configure the following in its VMX file: `ethernet0.filter1.name = dv-filter1` where `ethernet0` is the network adapter interface of the virtual machine

that is to be protected, filter1 is the number of the filter that is being used, and `dv-filter1` is the name of the particular data path kernel module that is protecting the VM.
- Ensure that the name of the data path kernel is set correctly.

If a VM is not supposed to be protected:

- Remove the following from its VMX file: `ethernet0.filter1.name = dv-filter1` where `ethernet0` is the network adapter interface of the virtual machine that is to be protected, filter1 is the number of the filter that is being used, and `dv-filter1` is the name of the particular data path kernel module that is protecting the VM.

Impact:

Incorrectly configuring this option can negatively impact functionality of tools that use vmsafe API.

Incorrectly configuring this option can prevent VMs from connecting to the network.

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/1714
2. http://kb.vmware.com/kb/1028151

8.4.2 Control VMsafe Agent Address (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure the `vmsafe.agentAddress` option in the virtual machine configuration file correctly.

Rationale:

The VMsafe CPU/memory API allows a security virtual machine to inspect and modify the contents of the memory and CPU registers on other VMs, for the purpose of detecting and preventing malware attacks. However, an attacker might compromise the VM by making

use of this introspection channel; therefore you should monitor for unauthorized usage of this API. A VM must be configured explicitly to accept access by the VMsafe CPU/memory API.

This involves three parameters to perform the following:

1. Enable the API
2. Set the IP address used by the security virtual appliance on the introspection vSwitch
3. Set the port number for that IP address.

If the VM is being protected by such a product, then make sure the latter two parameters are set correctly. This should be done only for specific VMs for which you want this protection.

Audit:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and verify that `vmsafe.agentAddress` is not present.

If it is being protected by a VMsafe CPU/Memory product then make sure the `vmsafe.agentAddress` is set to the correct value.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "vmsafe.agentAddress" | Select Entity, Name, Value
```

Remediation:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and verify that `vmsafe.agentAddress` is not present.

If it is being protected by a VMsafe CPU/Memory product then make sure this is set to the correct value

Impact:

Incorrectly configuring this option can negatively impact functionality of tools that use VMsafe API.

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/1714
2. http://www.vmware.com/files/xls/hardeningguide-vsphere5-1-ga-release-public.xlsx

8.4.3 Control VMsafe Agent Port (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure the `vmsafe.agentPort` option in the virtual machine configuration file correctly.

Rationale:

The VMsafe CPU/memory API allows a security virtual machine to inspect and modify the contents of the memory and CPU registers on other VMs, for the purpose of detecting and preventing malware attacks. However, an attacker might compromise the VM by making use of this introspection channel; therefore you should monitor for unauthorized usage of this API. A VM must be configured explicitly to accept access by the VMsafe CPU/memory API.

This involves three parameters to perform the following:

1. Enable the API
2. Set the IP address used by the security virtual appliance on the introspection vSwitch
3. Set the port number for that IP address.

If the VM is being protected by such a product, then make sure the latter two parameters are set correctly. This should be done only for specific VMs for which you want this protection.

Audit:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and verify that vmsafe.agentPort is not present. If it is being protect by a VMsafe CPU/Memory product, make sure this is set to the correct value

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "vmsafe.agentPort"| Select Entity, Name, Value
```

Remediation:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and verify that `vmsafe.agentPort` is not present.

If it is being protect by a VMsafe CPU/Memory product, make sure vmsafe.agentPort is set to the correct value.

Impact:

Incorrectly configuring this option can negatively impact functionality of tools that use VMsafe API.

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/1714
2. http://www.vmware.com/files/xls/hardeningguide-vsphere5-1-ga-release-public.xlsx

8.4.4 Control VMsafe Agent Configuration (Not Scored)

Profile Applicability:

- Level 1

Description:

Configure the `vmsafe.enable` option in the virtual machine configuration file correctly.

Rationale:

The VMsafe CPU/memory API allows a security virtual machine to inspect and modify the contents of the memory and CPU registers on other VMs, for the purpose of detecting and preventing malware attacks. However, an attacker might compromise the VM by making use of this introspection channel; therefore you should monitor for unauthorized usage of this API. A VM must be configured explicitly to accept access by the VMsafe CPU/memory API.

This involves three parameters to perform the following:

1. Enable the API

2. Set the IP address used by the security virtual appliance on the introspection vSwitch
3. Set the port number for that IP address.

If the VM is being protected by such a product, then make sure the latter two parameters are set correctly. This should be done only for specific VMs for which you want this protection.

Audit:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and verify that vmsafe.enable is either not present, or set to FALSE.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "vmsafe.enable"| Select Entity, Name, Value
```

Remediation:

If the VM is not being protected by a VMsafe CPU/memory product, then check virtual machine configuration file and set `vmsafe.enable` to `FALSE`.

Impact:

Incorrectly configuring this option can negatively impact functionality of tools that use vmsafe API.

Default Value:

The prescribed state is the default state.

References:

1. http://kb.vmware.com/kb/1714
2. http://www.vmware.com/files/xls/hardeningguide-vsphere5-1-ga-release-public.xlsx

8.4.5 Disable Autologon (Scored)

Profile Applicability:

- Level 2

Description:

Disable unneeded autologon to reduce the potential for vulnerabilities.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.ghi.autologon.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable" -value
$true
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.6 Disable BIOS BBS (Scored)

Profile Applicability:

- Level 2

Description:

Disable BIOS BBS to reduce the potential for vulnerabilities.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.bios.bbs.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.bios.bbs.disable"| Select Entity, Name,
Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.bios.bbs.disable" -value $true
```

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.7 Disable Guest Host Interaction Protocol Handler (Scored)

Profile Applicability:

- Level 2

Description:

Disable Guest Host Interaction Protocol Handle to reduce opportunity for vulnerabilities.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.ghi.protocolhandler.info.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable"
| Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable"
-value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.8 Disable Unity Taskbar (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity Taskbar feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unity.taskbar.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" | Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.9 Disable Unity Active (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity Active feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unityActive.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unityActive.disable" | Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unityActive.disable" -value $True
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.10 Disable Unity Window Contents (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity Window Contents feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unity.windowContents.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" |
Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" -
value $True
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.11 Disable Unity Push Update (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity Push Update features

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unity.push.update.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" |
Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.12 Disable Drag and Drop Version Get (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Drag and Drop Version Get feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.vmxDnDVersionGet.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.13 Disable Drag and Drop Version Set (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Drag and Drop Version Set feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters

that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.guestDnDVersionSet.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable"|
Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.14 Disable Shell Action (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Shell Action feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.ghi.host.shellAction.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" | Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.15 Disable Request Disk Topology (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Request Disk Topology feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.dispTopoRequest.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.16 Disable Trash Folder State (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Trash Folder State feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.trashFolderState.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.trashFolderState.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.trashFolderState.disable" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.17 Disable Guest Host Interaction Tray Icon (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Guest Host Interaction Tray Icon feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.ghi.trayicon.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable" -value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.18 Disable Unity (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unity.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unity.disable"| Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.disable" -value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.19 Disable Unity Interlock (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Unity Interlock feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.unityInterlockOperation.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable"|
Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable" -
value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.20 Disable GetCreds (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed GetCreds feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.getCreds.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.getCreds.disable"| Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.getCreds.disable" -value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.21 Disable Host Guest File System Server (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Host Guest File System Server feature.

Rationale:

Certain automated operations such as automated tools upgrades use a component into the hypervisor called Host Guest File System (HGFS) and an attacker could potentially use this to transfer files inside the guest OS.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.hgfsServerSet.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.hgfsServerSet.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.hgfsServerSet.disable" -value
$true
```

Impact:

Setting isolation.tools.hgfsServerSet.disable to true disables registration of the guest's HGFS server with the host. APIs that use HGFS to transfer files to and from the guest operating system, such as some VIX commands or the VMware Tools auto-upgrade utility, will not function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.22 Disable Guest Host Interaction Launch Menu (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed Guest Host Interaction Launch Menu feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESXi, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.ghi.launchmenu.change` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" | Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" -value
$true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.23 Disable memSchedFakeSampleStats (Scored)

Profile Applicability:

- Level 2

Description:

Disable unexposed memSchedFakeSampleStats feature.

Rationale:

Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities. Disabling these features reduces the number of vectors through which a guest can attempt to influence the host, and thus may help prevent successful exploits.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.memSchedFakeSampleStats.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable" |
Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable" -
value $true
```

Impact:

Some automated tools and process may cease to function.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

8.4.24 Disable VM Monitor Control (Scored)

Profile Applicability:

- Level 2

Description:

Disable VM Monitor Control.

Rationale:

When Virtual Machines are running on a hypervisor they are "aware" that they are running in a virtual environment and this and this information is available to tools inside the guest OS. This can give attackers information about the platform that they are running on that they may not get from a normal physical server. This option completely disables all hooks for a virtual machine and the guest OS will not be aware that it is running in a virtual environment at all.

Audit:

Check virtual machine configuration file and verify that `isolation.monitor.control.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.monitor.control.disable"| Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.monitor.control.disable" -value $true
```

Impact:

This configuration option may cause unexpected results, the virtual machine will be completely unaware that it is running in a virtualized setting. VMware tools will not install or function.

Default Value:

The prescribed state is not the default state.

References:

1. http://www.vmware.com/files/xls/hardeningguide-vsphere5-1-ga-release-public.xlsx

8.4.25 Disable VM Console Copy operations (Scored)

Profile Applicability:

- Level 1

Description:

Disable VM console copy and paste operations.

Rationale:

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this feature is enabled, you can copy and paste rich text and, depending on the VMware product, graphics and files from your clipboard to the guest operating system in a virtual machine. That is, as soon as the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running.

Audit:

Check virtual machine configuration and verify that `isolation.tools.copy.disable` option is missing or set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.copy.disable" | Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.copy.disable" -value $true
```

Impact:

This is the default setting so functionality remains the same.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.26 Disable VM Console Drag and Drop operations (Scored)

Profile Applicability:

- Level 1

Description:

Disable VM Console Drag and Drop operations.

Rationale:

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this feature is enabled, you can copy and paste rich text and, depending on the VMware product, graphics and files from your clipboard to the guest operating system in a virtual machine. That is, as soon as the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running.

Audit:

Check virtual machine configuration and verify that `isolation.tools.dnd.disable` is missing or set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.dnd.disable" | Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.dnd.disable" -value $true
```

Impact:

This is the default setting so functionality remains the same.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-50/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.27 Disable VM Console and Paste GUI Options (Scored)

Profile Applicability:

- Level 1

Description:

Disable VM Console and Paste GUI Options.

Rationale:

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this feature is enabled, you can copy and paste rich text and, depending on the VMware product, graphics and files from your clipboard to the guest operating system in a virtual machine. That is, as soon as the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running.

Audit:

Check virtual machine configuration and verify that `isolation.tools.setGUIOptions.enable` option is missing or set to `FALSE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.setGUIOptions.enable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.setGUIOptions.enable" -value
$false
```

Impact:

This is the default setting so functionality remains the same.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-50/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.4.28 Disable VM Console Paste operations (Scored)

Profile Applicability:

- Level 1

Description:

Disable VM Console Paste operations.

Rationale:

By default, the ability to copy and paste text, graphics, and files is disabled, as is the ability to drag and drop files. When this feature is enabled, you can copy and paste rich text and, depending on the VMware product, graphics and files from your clipboard to the guest

operating system in a virtual machine. That is, as soon as the console window of a virtual machine gains focus, nonprivileged users and processes running in the virtual machine can access the clipboard on the computer where the console window is running.

Audit:

Check virtual machine configuration and verify that `isolation.tools.paste.disable` is missing or set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.paste.disable"| Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.paste.disable" -value $true
```

Impact:

This is the default setting so functionality remains the same.

Default Value:

The prescribed state is the default state.

References:

1. http://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.5 Resources

8.5.1 Prevent virtual machines from taking over resources (Not Scored)

Profile Applicability:

- Level 2

Description:

Use limits, shares, and reservations to prevent virtual machines from taking over resources.

Rationale:

By default, all virtual machines on an ESXi host share the resources equally. By using the resource management capabilities of ESXi, such as shares and limits, you can control the server resources that a virtual machine consumes. 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.

Audit:

Use shares or reservations to guarantee resources to critical VMs. Use limits to constrain resource consumption by virtual machines that have a greater risk of being exploited or attacked, or that run applications that are known to have the potential to greatly consume resources.

Additionally, the following PowerCLI command may be used:

```
# List all Resource shares on all VMs
Get-VM | Get-VMResourceConfiguration
```

Remediation:

- Use shares or reservations to guarantee resources to critical VMs.
- Use limits to constrain resource consumption by virtual machines that have a greater risk of being exploited or attacked, or that run applications that are known to have the potential to greatly consume resources.

References:

1. http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-resource-management-guide.pdf

8.6 Storage

8.6.1 Avoid using nonpersistent disks (Scored)

Profile Applicability:

- Level 1

Description:

Virtual Machine Disks are created as Dependent by default and are affected by snapshots.

To ensure a virtual machine disk is not affected by snapshots the disk mode can be set to Independent.

Disks set to Independent mode can be Independent Persistent or Independent Nonpersistent.

Disks with Independent persistent mode have their data written permanently to the disk.

Independent Nonpersistent disks lose any changes made to the disk when the system is rebooted and can mask any trace of an attack on the system.

Rationale:

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 production virtual machines should be configured as follows:

1. Independent setting not enabled
2. Independent persistent
3. Independent nonpersistent with remote logging

Without a persistent record of activity on a VM, administrators might never know whether they have been attacked or hacked.

Audit:

If remote logging of events and activity is not configured for the guest, scsiX:Y.mode should be either:

1. Not present. This is the default.
2. Not set to independent nonpersistent

Additionally, the following PowerCLI command may be used:

```
#List the VM's and their disk types
Get-VM | Get-HardDisk | Select Parent, Name, Filename, DiskType, Persistence
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
#Alter the parameters for the following cmdlet to set the VM Disk Type:
Get-VM | Get-HardDisk | Set-HardDisk
```

Impact:

Won't be able to make use of nonpersistent mode, which allows rollback to a known state when rebooting the VM.

Default Value:

The default mode is the correct mode.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.wssdk.apiref.doc/vim.vm.device.VirtualDiskOption.DiskMode.html
2. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vm_admin.doc/GUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

8.6.2 Disable virtual disk shrinking (Scored)

Profile Applicability:

- Level 2

Description:

If Virtual disk shrinking is done repeatedly it will cause the virtual disk to become unavailable resulting in a denial of service. You can prevent virtual disk shrinking by disabling it.

Rationale:

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. Repeated disk shrinking can make a virtual disk unavailable. This capability is available to nonadministrative users in the guest.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.diskShrink.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.diskShrink.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.diskShrink.disable" -value $true
```

Impact:

Inability to shrink virtual machine disks in the event that a datastore runs out of space.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-C7D50832-CDBF-4E64-B5C0-57DF4A94B892.html

8.7 Tools

8.7.1 Disable VMware Tools auto install (Scored)

Profile Applicability:

- Level 1

Description:

When installing VMware tools, it can sometimes require a reboot to finalize the installation. If you choose the auto install option it will reboot the system without notice if one is required.

Rationale:

VMware Tools auto install can initiate an automatic reboot, disabling this option will prevent tools from being installed automatically and prevent automatic machine reboots.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.autoinstall.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.autoInstall.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.autoInstall.disable" -value $true
```

Impact:

This option disables tools auto install via the hypervisor. It is recommended that VMware tools installs and upgrades be handled through other means (For example: a devops tool such as ansible, chef, puppet, or saltstack).

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-65BCA561-5A03-4D17-A663-46A0C50CE6A7.html

8.7.2 Disable VIX messages from the VM (Scored)

Profile Applicability:

- Level 1

Description:

If you do not make use of custom VIX programming in your environment then you should disable this feature to reduce the potential for vulnerabilities.

Rationale:

The VIX API is a library for writing scripts and programs to manipulate virtual machines. If you do not make use of custom VIX programming in your environment, then you should disable certain features to reduce the potential for vulnerabilities. The ability to send messages from the VM to the host is one of these features.

Note: Disabling this feature does NOT adversely affect the functioning of VIX operations that originate outside the guest, so certain VMware and 3rd party solutions that rely upon this capability should continue to work. This is a deprecated interface. Ensure that any deprecated interface is turned off for audit purposes.

Audit:

Check virtual machine configuration file and verify that `isolation.tools.vixMessage.disable` is set to `TRUE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "isolation.tools.vixMessage.disable"| Select
Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "isolation.tools.vixMessage.disable" -value $true
```

Impact:

Guest will no longer be able to send messages via VIX API.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vddk.pg.doc/vddkTasks.8.7.html

8.7.3 Do not send host information to guests (Scored)

Profile Applicability:

- Level 1

Description:

Configure VMware Tools to disable host info from being sent to guests.

Rationale:

If set to `TRUE` a VM can obtain detailed information about the physical host. The default value for the parameter is `FALSE`. This setting should not be `TRUE` unless a particular VM requires this information for performance monitoring. An adversary potentially can use this information to inform further attacks on the host.

Audit:

Check virtual machine configuration file and verify that `tools.guestlib.enableHostInfo` is set to `FALSE`.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "tools.guestlib.enableHostInfo"| Select Entity,
Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "tools.guestlib.enableHostInfo" -value $false
```

Impact:

Unable to retrieve performance information about the host from inside the guest, there are times when this can be useful for troubleshooting.

Default Value:

The prescribed state is the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.security.doc/GUID-2CF880DA-2435-4201-9AFB-A16A11951A2D.html

8.7.4 Limit number of VM log files (Scored)

Profile Applicability:

- Level 1

Description:

Configure VM settings to prevent uncontrolled logging.

Rationale:

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. Uncontrolled logging can lead to denial of service due to the datastore's being filled.

Audit:

Check virtual machine configuration file and verify that log.keepOld is set to 10.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "log.keepOld"| Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "log.keepOld" -value "10"
```

Impact:

A more extreme strategy is to disable logging altogether for the virtual machine. Disabling logging makes troubleshooting challenging and support difficult. Do not consider disabling logging unless the log file rotation approach proves insufficient.

Default Value:

The prescribed state is not the default state.

References:

1. https://pubs.vmware.com/vsphere-51/topic/com.vmware.vmtools.install.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

8.7.5 Limit VM log file size (Scored)

Profile Applicability:

- Level 1

Description:

Configure VM settings to prevent uncontrolled logging.

Rationale:

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. Uncontrolled logging can lead to denial of service due to the datastore's being filled.

Audit:

Check virtual machine configuration file and verify that log.rotateSize is set to 100000.

Additionally, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "log.rotateSize"| Select Entity, Name, Value
```

Remediation:

To implement the recommended configuration state, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "log.rotateSize" -value "100000"
```

Impact:

A more extreme strategy is to disable logging altogether for the virtual machine. Disabling logging makes troubleshooting challenging and support difficult. Do not consider disabling logging unless the log file rotation approach proves insufficient.

Default Value:

The prescribed state is not the default state.

References:

1. http://kb.vmware.com/kb/8182749

Appendix: Change History

Date	Version	Changes for this version
2014-06-10	1.0.0	Initial Public Release
2014-06-23	1.0.1	Fixed numbering in section 1