CIS VMware ESXi 7.0 Benchmark

v1.6.0 - 08-27-2026

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Internal Only - General

Table of Contents

Terms of Use *1*

Table of Contents *2*

Overview *6*

Important Usage Information 6

Key Stakeholders 6

Apply the Correct Version of a Benchmark 7

Exceptions 7

Remediation 8

Summary 8

Target Technology Details 9

Intended Audience 9

Consensus Guidance 10

Typographical Conventions 11

Recommendation Definitions *12*

Title 12

Assessment Status 12

Automated 12

Manual 12

Profile 12

Description 12

Rationale Statement 12

Impact Statement 13

Audit Procedure 13

Remediation Procedure 13

Default Value 13

References 13

CIS Critical Security Controls® (CIS Controls®) 13

Additional Information 13

Profile Definitions 14

Acknowledgements 15

Recommendations *16*

1 Install 16

1.1 (L1) Ensure ESXi is properly patched (Manual) 17

1.2 (L1) Ensure the Image Profile VIB acceptance level is configured properly (Automated) 19

1.3 (L1) Ensure no unauthorized kernel modules are loaded on the host (Manual) 22

1.4 (L2) Ensure the default value of individual salt per vm is configured (Automated) 24

Internal Only - General

2 Communication 26
2.1 (L1) Ensure NTP time synchronization is configured properly (Automated) 27
2.2 (L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host (Manual) 29
2.3 (L1) Ensure Managed Object Browser (MOB) is disabled (Automated) 31
2.4 (L2) Ensure default self-signed certificate for ESXi communication is not used (Manual) 33
2.5 (L1) Ensure SNMP is configured properly (Manual) 35
2.6 (L1) Ensure dvfilter API is not configured if not used (Manual) 37
2.7 (L1) Ensure expired and revoked SSL certificates are removed from the ESXi server (Manual) 39
2.8 (L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory (Manual) 42
2.9 (L2) Ensure VDS health check is disabled (Manual) 45

3 Logging 47
3.1 (L1) Ensure a centralized location is configured to collect ESXi host core dumps (Automated) 48
3.2 (L1) Ensure persistent logging is configured for all ESXi hosts (Manual) 50
3.3 (L1) Ensure remote logging is configured for ESXi hosts (Automated) 52

4 Access 54
4.1 (L1) Ensure a non-root user account exists for local admin access (Automated) 55
4.2 (L1) Ensure passwords are required to be complex (Manual) 57
4.3 (L1) Ensure the maximum failed login attempts is set to 5 (Automated) 60
4.4 (L1) Ensure account lockout is set to 15 minutes (Automated) 62
4.5 (L1) Ensure previous 5 passwords are prohibited (Manual) 64
4.6 (L1) Ensure Active Directory is used for local user authentication (Manual) 66
4.7 (L1) Ensure only authorized users and groups belong to the esxAdminsGroup group (Manual) 68
4.8 (L1) Ensure the Exception Users list is properly configured (Manual) 70

5 Console 72
5.1 (L1) Ensure the DCUI timeout is set to 600 seconds or less (Automated) 73
5.2 (L1) Ensure the ESXi shell is disabled (Automated) 75
5.3 (L1) Ensure SSH is disabled (Automated) 77
5.4 (L1) Ensure CIM access is limited (Manual) 79
5.5 (L1) Ensure Normal Lockdown mode is enabled (Automated) 81
5.6 (L2) Ensure Strict Lockdown mode is enabled (Automated) 83
5.7 (L2) Ensure the SSH authorized_keys file is empty (Manual) 85
5.8 (L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less (Automated) 87
5.9 (L1) Ensure the shell services timeout is set to 1 hour or less (Automated) 89
5.10 (L1) Ensure DCUI has a trusted users list for lockdown mode (Manual) 91
5.11 (L2) Ensure contents of exposed configuration files have not been modified (Manual) 93

6 Storage 96
6.1 (L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled (Automated) 97
6.2 (L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic (Manual) 100
6.3 (L1) Ensure storage area network (SAN) resources are segregated properly (Manual) 102

7 vNetwork 104
7.1 (L1) Ensure the vSwitch Forged Transmits policy is set to reject (Automated) 105
7.2 (L1) Ensure the vSwitch MAC Address Change policy is set to reject (Automated) 107
7.3 (L1) Ensure the vSwitch Promiscuous Mode policy is set to reject (Automated) 109
7.4 (L1) Ensure port groups are not configured to the value of the native VLAN (Automated) 112
7.5 (L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches (Manual) 114

Internal Only - General

7.6 (L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT) (Automated) 116
7.7 (L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector (Manual) 118
8 Virtual Machines 120
8.1 Communication 121
8.1.1 (L2) Ensure only one remote console connection is permitted to a VM at any time (Automated) 122
8.2 Devices 124
8.2.1 (L1) Ensure unnecessary floppy devices are disconnected (Automated) 125
8.2.2 (L2) Ensure unnecessary CD/DVD devices are disconnected (Automated) 127
8.2.3 (L1) Ensure unnecessary parallel ports are disconnected (Automated) 129
8.2.4 (L1) Ensure unnecessary serial ports are disconnected (Automated) 131
8.2.5 (L1) Ensure unnecessary USB devices are disconnected (Automated) 133
8.2.6 (L1) Ensure unauthorized modification and disconnection of devices is disabled (Automated) 135
8.2.7 (L1) Ensure unauthorized connection of devices is disabled (Automated) 137
8.2.8 (L1) Ensure PCI and PCIe device passthrough is disabled (Automated) 139
8.3 Guest 141
8.3.1 (L1) Ensure unnecessary or superfluous functions inside VMs are disabled (Manual) 142
8.3.2 (L1) Ensure use of the VM console is limited (Manual) 144
8.3.3 (L1) Ensure secure protocols are used for virtual serial port access (Manual) 146
8.3.4 (L1) Ensure standard processes are used for VM deployment (Manual) 148
8.4 Monitor 150
8.4.1 (L1) Ensure access to VMs through the dvfilter network APIs is configured correctly (Manual) 151
8.4.2 (L2) Ensure Autologon is disabled (Automated) 154
8.4.3 (L2) Ensure BIOS BBS is disabled (Automated) 156
8.4.4 (L2) Ensure Guest Host Interaction Protocol Handler is set to disabled (Automated) 158
8.4.5 (L2) Ensure Unity Taskbar is disabled (Automated) 160
8.4.6 (L2) Ensure Unity Active is disabled (Automated) 162
8.4.7 (L2) Ensure Unity Window Contents is disabled (Automated) 164
8.4.8 (L2) Ensure Unity Push Update is disabled (Automated) 166
8.4.9 (L2) Ensure Drag and Drop Version Get is disabled (Automated) 168
8.4.10 (L2) Ensure Drag and Drop Version Set is disabled (Automated) 170
8.4.11 (L2) Ensure Shell Action is disabled (Automated) 172
8.4.12 (L2) Ensure Request Disk Topology is disabled (Automated) 174
8.4.13 (L2) Ensure Trash Folder State is disabled (Automated) 176
8.4.14 (L2) Ensure Guest Host Interaction Tray Icon is disabled (Automated) 178
8.4.15 (L2) Ensure Unity is disabled (Automated) 180
8.4.16 (L2) Ensure Unity Interlock is disabled (Automated) 182
8.4.17 (L2) Ensure GetCreds is disabled (Automated) 184
8.4.18 (L2) Ensure Host Guest File System Server is disabled (Automated) 186
8.4.19 (L2) Ensure Guest Host Interaction Launch Menu is disabled (Automated) 188
8.4.20 (L2) Ensure memSchedFakeSampleStats is disabled (Automated) 190
8.4.21 (L1) Ensure VM Console Copy operations are disabled (Automated) 192
8.4.22 (L1) Ensure VM Console Drag and Drop operations is disabled (Automated) 194
8.4.23 (L1) Ensure VM Console GUI Options is disabled (Automated) 196
8.4.24 (L1) Ensure VM Console Paste operations are disabled (Automated) 198
8.5 Resources 200
8.5.1 (L2) Ensure VM limits are configured correctly (Manual) 201
8.5.2 (L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False" (Automated) 203
8.6 Storage 205
8.6.1 (L2) Ensure nonpersistent disks are limited (Automated) 206

Internal Only - General

8.6.2 (L1) Ensure virtual disk shrinking is disabled (Automated) 208
8.6.3 (L1) Ensure virtual disk wiping is disabled (Automated) 210
8.7 Tools 212
8.7.1 (L1) Ensure the number of VM log files is configured properly (Automated) 213
8.7.2 (L2) Ensure host information is not sent to guests (Automated) 215
8.7.3 (L1) Ensure VM log file size is limited (Automated) 217
Appendix: Summary Table 219
Appendix: CIS Controls v7 IG 1 Mapped Recommendations 226
Appendix: CIS Controls v7 IG 2 Mapped Recommendations 228
Appendix: CIS Controls v7 IG 3 Mapped Recommendations 233
Appendix: CIS Controls v7 Unmapped Recommendations 238
Appendix: CIS Controls v8 IG 1 Mapped Recommendations 239
Appendix: CIS Controls v8 IG 2 Mapped Recommendations 242
Appendix: CIS Controls v8 IG 3 Mapped Recommendations 247
Appendix: CIS Controls v8 Unmapped Recommendations 252
Appendix: Change History 253

Internal Only - General

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Internal Only - General

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Internal Only - General

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Internal Only - General

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for VMware ESXi 7.0. 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 7.0.

Internal Only - General

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. 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://workbench.cisecurity.org/.

Internal Only - General

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, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Internal Only - General

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Internal Only - General

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Internal Only - General

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 (L1) - Corporate/Enterprise Environment (general use)**

  Items in this profile intend to:

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

- **Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)**

  This profile extends the "Level 1 (L1)" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability;
  - may negatively inhibit the utility or performance of the technology; and
  - limit the ability of remote management/access.

  Note: Implementation of Level 2 requires that **both** Level 1 and Level 2 settings are applied.

Internal Only - General

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Randall Mowen

Editors
Robert Plankers
Randall Mowen

Contributors
Tony Wilwerding
Dale McKay
Shawn Kearney
Matthew Reagan
Yevgeniy Steblyanko

Internal Only - General

Recommendations

1 Install

This section contains recommendations for base ESXi install.

Internal Only - General

1.1 (L1) Ensure ESXi is properly patched (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

VMware Lifecycle Manager is a tool which may be utilized 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. VMware also publishes advisories on security patches and offers a way to subscribe to email alerts for them.

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.

Impact:

ESXi servers must be in Maintenance Mode to apply patches. This implies all VMs must be moved or powered off on the ESXi server, so the patching process may necessitate having brief outages.

Audit:

Verify that the patches are up to date. The following PowerCLI snippet will provide a list of all installed patches:

```
Foreach ($VMHost in Get-VMHost ) {
    $EsxCli = Get-EsxCli -VMHost $VMHost -V2
    $EsxCli.software.vib.list.invoke() | Select-Object
@{N="VMHost";E={$VMHost}},*
}
```

You may also manage updates via VMware Lifecycle Manager located under `Menu`, `Lifecycle Manager`.

Remediation:

Employ a process to keep ESXi hosts up to date with patches in accordance with industry standards and internal guidelines. Leverage the VMware Lifecycle Manager to test and apply patches as they become available.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere-lifecycle-manager.doc/GUID-74295A37-E8BB-4EB9-BFBA-47B78F0C570D.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

1.2 (L1) Ensure the Image Profile VIB acceptance level is configured properly (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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. The ESXi Image Profile supports four VIB acceptance levels:

1. VMware Certified - VIBs created, tested, and signed by VMware
2. VMware Accepted - VIBs created by a VMware partner but tested and signed by VMware
3. Partner Supported - VIBs created, tested, and signed by a certified VMware partner
4. Community Supported - VIBs that have not been tested by VMware or a VMware partner

Rationale:

The ESXi Image Profile should only allow signed VIBs because an unsigned VIB represents untested code installed on an ESXi host. Also, use of unsigned VIBs will cause hypervisor Secure Boot to fail to configure. Community Supported VIBs do not have digital signatures. To protect the security and integrity of your ESXi hosts, do not allow unsigned (CommunitySupported) VIBs to be installed on your hosts.

Impact:

Unsigned (Community Supported) VIBs will not be able to be utilized on a host.

Audit:

To verify the host image profile acceptance level perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure`, then under `System` select `Security Profile`.
3. Under `Host Image Profile Acceptance Level` ensure it is set to one of the following - "VMware Certified", "VMware Accepted", or "Partner Supported".

This may also be performed as follows:

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 Accepted", or "Partner Supported".

Internal Only - General

2. Connect to each ESX/ESXi host using the vCLI, and execute the command `esxcli software vib list` to verify the acceptance level for each VIB is either "VMware Certified", "VMware Accepted", 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 verify the host image profile acceptance level perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure`, then under `System` select `Security Profile`.
3. Under `Host Image Profile Acceptance Level` select `Edit`
4. In the dropdown select one of the following - `VMware Certified`, `VMware Accepted`, or `Partner Supported`.

To implement the recommended configuration state, run the following PowerCLI command (in the example code, the level is Partner Supported):

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

Default Value:

Partner Supported

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

Internal Only - General

1.3 (L1) Ensure no unauthorized kernel modules are loaded on the host (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 allow unauthorized kernel modules to be loaded.

Rationale:

VMware provides digital signatures for kernel modules. Untested or malicious kernel modules loaded on the ESXi host can put the host at risk for instability and/or exploitation.

Impact:

This is the default behavior therefor impact is low to none.

Audit:

To list all the loaded kernel modules from the ESXi Shell or vCLI, run: "esxcli system module list".

Review the list for unauthorized modules.

Verifying signatures may assist in identifying unauthorized modules. For each module, verify the signature by running: `esxcli system module get -m <module>`.

Additionally to review signed vs unsigned modules, 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:

Secure the host by disabling unsigned modules and removing the offending VIBs from the host.

Internal Only - General

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

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

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-E9B71B85-FBA3-447C-8A60-DEE2AE1A405A.html
2. http://kb.vmware.com/kb/2042473

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

Internal Only - General

1.4 (L2) Ensure the default value of individual salt per vm is configured (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The concept of salting has been introduced to help address concerns system administrators may have over the security implications of Transparent Page Sharing otherwise known as TPS. As per the original TPS implementation, multiple virtual machines could share pages when the contents of the pages were same. With the new salting settings, the virtual machines can share pages only if the salt value and contents of the pages are identical. A new host config option Mem.ShareForceSalting is introduced to enable or disable salting.

By default, salting is enabled (Mem.ShareForceSalting=2) and each virtual machine has a different salt. This means page sharing does not occur across the virtual machines (inter-VM TPS) and only happens inside a virtual machine (intra VM).

Rationale:

Intra-VM means that TPS will de-duplicate identical pages of memory within a virtual machine, but will not share the pages with any other virtual machines. Ensuring the default setting is in place so that page sharing only occurs inside a virtual machine is the best option here.

Impact:

There is potential in a performance impact regarding this setting, each environment and the impact on it will vary.

Audit:

From the vSphere Web Client:

1. Select a host
2. Click `Configure` then expand `System` then select `Advanced System settings`.
3. Click `Edit` then Filter for `Mem.ShareForceSalting`.
4. Verify that it is set to 2.

Additionally the following PowerCLI command can be used:

```
Get-VMHost | Get-AdvancedSetting -Name Mem.ShareForceSalting
```

Remediation:

From the vSphere Web Client:

Internal Only - General

1. Select a host
2. Click `Configure` then expand `System` then select `Advanced System settings`.
3. Click `Edit` then Filter for `Mem.ShareForceSalting`.
4. Set the value to `2`.
5. Click `OK`.

Additionally, the following PowerCLI command can be used:

```
Get-VMHost | Get-AdvancedSetting -Name Mem.ShareForceSalting | Set-
AdvancedSetting -Value 2
```

References:

1. https://kb.vmware.com/s/article/2097593
2. https://blogs.vmware.com/vsphere/2015/01/assess-the-performance-impact-of-the-security-change-in-transparent-page-sharing-behaviour.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2 Communication

This section contains recommendations related to ESXi communication.

Internal Only - General

2.1 (L1) Ensure NTP time synchronization is configured properly (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Network Time Protocol (NTP) synchronization should be configured correctly and enabled on each VMware ESXi host to ensure accurate time for system event logs. The time sources used by the ESXi hosts should be in sync with an agreed-upon time standard such as Coordinated Universal Time (UTC). There should be at minimum two NTP sources in place, and they should sync whenever possible.

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, it is simpler to track and correlate an intruder's actions when reviewing the relevant log files. Incorrect time settings can also make auditing inaccurate.

Audit:

To confirm NTP synchronization is enabled and properly configured, perform the following from the vSphere Web Client:

1. Select a host
2. Click `Configure` then expand `System` then select `Time Configuration`.
3. Verify that `Time Synchronization` is set to Automatic
4. Verify that the NTP Client is set to `Enabled`
5. Verify that the NTP Service Status is `Running`
6. Verify that appropriate NTP servers are set.

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 enable and properly configure NTP synchronization, perform the following from the vSphere web client:

1. Select a host
2. Click `Configure` then expand `System` then select `Time Configuration`.
3. Select `Edit` next to Network Time Protocol

Internal Only - General

4. Select the `Enable` box, then fill in the appropriate NTP Servers.
5. in the `NTP Service Startup Policy` drop down select `Start and stop with host`.
6. Click `OK`.

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 or the Fully Qualified Domain Name (FQDN) of the internal
NTP server
$NTPServers = "pool.ntp.org", "pool2.ntp.org"
Get-VMHost | Add-VmHostNtpServer $NTPServers
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-2553C86E-7981-4F79-B9FC-A6CECA52F6CC.html

Additional Information:

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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

Internal Only - General

2.2 (L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The ESXi firewall is enabled by default and allows ping (ICMP) and communication with DHCP/DNS clients. Access to services should only be allowed by authorized IP addresses/networks.

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 IP addresses and networks.

Impact:

Connections from IP addresses and ranges that are not explicitly set will be denied. Take care to ensure appropriate IPs/IP address ranges are allowed.

Audit:

To confirm access to services running on an ESXi host is properly restricted, perform the following from the vSphere web client:

1. Select a host
2. Click `Configure` then expand `System` then select `Firewall`.
3. Click `Edit` to view services which are enabled (indicated by a check).
4. For each enabled service, (e.g., ssh, vSphere Web Access, http client) check to ensure that the list of allowed IP addresses specified is correct.

Additionally, the following PowerCLI command may be used:

Internal Only - General

```
# 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 properly restrict access to services running on an ESXi host, perform the following from the vSphere web client:

1. Select a host
2. Click `Configure` then expand `System` then select `Firewall`.
3. Click `Edit` to view services which are enabled (indicated by a check).
4. For each enabled service, (e.g., ssh, vSphere Web Access, http client) provide a list of allowed IP addresses.
5. Click `OK`.

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-8912DD42-C6EA-4299-9B10-5F3AEA52C605.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

Internal Only - General

2.3 (L1) Ensure Managed Object Browser (MOB) is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Managed Object Browser (MOB) is a web-based server application that lets you examine objects that exist on the server side, explore the object model used by the VM kernel to manage the host, and change configurations. It is installed and started automatically when vCenter is installed.

Rationale:

The MOB 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.

Impact:

Some third-party tools may utilize the Managed Object Browser (MOB) meaning that disabling it will cause those tools to malfunction.

Audit:

To confirm whether MOB is enabled, perform the following from the vSphere Web Client:

1. Select a host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Click `Edit` then search for `Config.HostAgent.plugins.solo.enableMob`
4. Verify the value is set to `false`.

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

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

Additionally, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting -Name
Config.HostAgent.plugins.solo.enableMob
```

Remediation:

To disabled MOB, perform the following from the vSphere Web Client:

1. Select a host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.

Internal Only - General

3. Click `Edit` then search for `Config.HostAgent.plugins.solo.enableMob`
4. Set the value to `false`.
5. Click `OK`.

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

Note 2: You must disable MOB from the vSphere interface not via the `vim-cmd` command.

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-0EF83EA7-277C-400B-B697-04BDC9173EA3.html

Additional Information:

Some third-party tools use the MOB to gather information. Use the following command to re-enable the MOB temporarily for third-party tool usage:

To disabled MOB, perform the following from the vSphere Web Client:

1. Select a host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Click `Edit` then search for `Config.HostAgent.plugins.solo.enableMob`
4. Set the value to `true`.
5. Click `OK`.

Note 2: You must enable MOB from the vSphere interface not via the `vim-cmd` command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

Internal Only - General

2.4 (L2) Ensure default self-signed certificate for ESXi communication is not used (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The default certificate is self-signed, not signed by a trusted certificate authority (CA). It should be replaced with a valid certificate issued by a trusted CA. It should be noted that certificates are generated at time of install differing slightly from some self-signed certificate solutions.

Rationale:

Using the default self-signed certificate may increase risk related to man-in-the-middle (MITM) attacks.

Impact:

Replacing the default certificate might cause vCenter Server to stop managing the host. Disconnect and reconnect the host if vCenter Server cannot verify the new certificate.

Audit:

View the details of the SSL certificate presented by the ESXi host and determine if it is issued by a trusted CA:

1. Log in to the ESXi Shell, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
2. Review the contents to see if the certs have been backed up.
3. In the directory `/etc/vmware/ssl`, confirm that it contains orig.rui.crt and orig.rui.key
4. In the directory `/etc/vmware/ssl`, confirm that it contains the newer certs renamed to rui.crt and rui.key

Alternatively, you can put the host into maintenance mode, to review the new certificates.

Remediation:

Backup and replace the details of the SSL certificate presented by the ESXi host and determine if it is issued by a trusted CA:

1. Log in to the ESXi Shell, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
2. In the directory /etc/vmware/ssl, rename the existing certificates using the following commands:

Internal Only - General

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3. Copy the certificates you want to use to /etc/vmware/ssl.
4. Rename the new certificate and key to rui.crt and rui.key.
5. Restart the host after you install the new certificate.

Alternatively, you can put the host into maintenance mode, install the new certificate, use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

```
Leverage VMware's SSL Certificate Automation Tool to install CA-signed SSL
certificates. For more information on this tool, please see
[http://kb.vmware.com/kb/2057340](http://kb.vmware.com/kb/2057340).
```

References:

1. https://kb.vmware.com/s/article/2111219
2. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-AC7E6DD7-F984-4E0F-983A-463031BA5FE7.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

Internal Only - General

2.5 (L1) Ensure SNMP is configured properly (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Simple Network Management Protocol (SNMP) can be used to help manage hosts. Many organizations have other means in place of managing hosts and do not need SNMP enabled. If SNMP is needed, it should be configured properly to reduce the risk of misuse or compromise. For example, ESXi supports SNMPv3, which provides stronger security than SNMPv1 or SNMPv2, including key authentication and encryption. It is also important to configure the destination for SNMP traps.

Rationale:

If SNMP is not properly configured, monitoring data containing sensitive information may be sent to a malicious host and used to help exploit said host.

Audit:

To confirm the proper configuration of SNMP, perform the following from the ESXi Shell or vCLI:

1. Run the following to determine if SNMP is being used:

```
esxcli system snmp get
```

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

Additionally, the following PowerCLI command may be used to view the SNMP configuration:

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

Remediation:

To correct the SNMP configuration, perform the following from the ESXi Shell or vCLI:

1. If SNMP is not needed, disable it by running:

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

2. If SNMP is needed, refer to the vSphere Monitoring and Performance guide, chapter 8 for steps to configure it.

Internal Only - General

Additionally, the following PowerCLI command may be used to implement the configuration:

```
# 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. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-8EF36D7D-59B6-4C74-B1AA-4A9D18AB6250.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.6 (L1) Ensure dvfilter API is not configured if not used (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The dvfilter network API is used by some products (e.g., VMSafe). If it is not in use, it should not be configured to send network information to a VM.

Rationale:

If the dvfilter network API is enabled in the future and it is already configured, an attacker might attempt to connect a VM to it, thereby potentially providing access to the network of other VMs on the host.

Impact:

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

Audit:

If the dvfilter network API 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 `Configure` then expand `System`
2. Click on `Advanced System Settings` then `Edit`.
3. Search for `Net.DVFilterBindIpAddress` in the filter.
4. Verify `Net.DVFilterBindIpAddress` has an empty value.
5. If an appliance is being used, then ensure the value of this parameter is set to the proper IP address.

Additionally, the following PowerCLI command may be used to verify the setting:

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

Remediation:

To remove the configuration for the dvfilter network API, perform the following from the vSphere web client:

1. From the vSphere web client, select the host and click `Configure` then expand `System`
2. Click on `Advanced System Settings` then `Edit`.
3. Search for `Net.DVFilterBindIpAddress` in the filter.

Internal Only - General

4. Set `Net.DVFilterBindIpAddress` has an empty value.
5. If an appliance is being used, make sure the value of this parameter is set to the proper IP address.
6. Enter the proper IP address.
7. Click `OK`.

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

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

Default Value:

Not configured

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

2.7 (L1) Ensure expired and revoked SSL certificates are removed from the ESXi server (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

By default, ESXi hosts do not have Certificate Revocation List (CRL) checking available, so expired and revoked SSL certificates must be checked and removed manually.

Rationale:

Leaving expired and revoked certificates on your vCenter Server system can compromise your environment. Replacing certificates will avoid having users get used to clicking through browser warnings. The warning might be an indication of a man-in-the-middle attack, and only inspection of the certificate and thumbprint can guard against such attacks.

Audit:

To assess if there are expired or revoked SSL certificates on your ESXi server, use the PowerCLI script called out in "verify-ssl-certificates".

Remediation:

Replace expired and revoked certificates with certificates from a trusted CA. Certificates can be replaced in a number of ways:

Replace a Default ESXi Certificate and Key from the ESXi Shell

1. Log in to the ESXi Shell, either directly from the DCUI or from an SSH client, as a user with administrator privileges.
2. In the directory /etc/vmware/ssl, rename the existing certificates using the following commands:

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

3. Copy the certificates that you want to use to /etc/vmware/ssl.
4. Rename the new certificate and key to rui.crt and rui.key.
5. Restart the host after you install the new certificate.

Alternatively, you can put the host into maintenance mode, install the new certificate, use the Direct Console User Interface (DCUI) to restart the management agents, and set the host to exit maintenance mode.

Replace a Default ESI Certificate and Key by Using the vifs Command

Internal Only - General

1. Back up the existing certificates.
2. Generate a certificate request following the instructions from the certificate authority.
3. At the command line, use the vifs command to upload the certificate to the appropriate location on the host.

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

4. Restart the host.

Alternatively, you can put the host into maintenance mode, install the new certificate, and then use the Direct Console User Interface (DCUI) to restart the management agents.

Replace A Default ESI Certificate and Key Using HTTP PUT

1. Back up the existing certificates.
2. In your upload application, process each file as follows:
3. Open the file.
4. Publish the file to one of these locations:

```
Certificates   https://hostname/host/ssl_cert
Keys   https://hostname/host/ssl_key
```

3. The locations /host/ssl_cert and host/ssl_key link to the certificate files in /etc/vmware/ssl.
4. Restart the host.

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-AC7E6DD7-F984-4E0F-983A-463031BA5FE7.html
2. http://en-us.sysadmins.lv/Lists/Posts/Post.aspx?List=332991f0-bfed-4143-9eea-f521167d287c&ID=60

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

Internal Only - General

2.8 (L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

vSphere Authentication Proxy enables ESXi hosts to join a domain without using Active Directory credentials. vSphere Authentication Proxy enhances security for PXE-booted hosts and hosts that are provisioned using Auto Deploy and Host profiles, by removing the need to store Active Directory credentials in the host configuration.

The vSphere Authentication Proxy service binds to an IPv4 address for communication with vCenter Server, and does not support IPv6. The vCenter Server can be on a host machine in an IPv4-only, IPv4/IPv6 mixed-mode, or IPv6-only network environment, but the machine that connects to the vCenter Server through the vSphere Client must have an IPv4 address for the vSphere Authentication Proxy service to work.

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:

If you utilize a host profile to join the domain, before attaching it verify that the profile has been configured to use the proxy server for joining the host to domains by following these steps:

1. In the vSphere Web Client go to `Home` in the menu.
2. Click on `Policies and Profiles` followed by `Host Profiles`.
3. Choose the appropriate host profile
4. Select `Configure` then expand `Security and Services` followed by `Authentication`.
5. Select `Active Directory configuration`.
6. Verify that `JoinDomain Method` is configured to `Use vSphere Authentication Proxy to add the host to the domain`.

There is no way to audit this using web client if you manually chose to join the host to a domain.

Additionally, the following PowerCLI command may be used:

Internal Only - General

```
# Confirm 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.ActiveDirecto
ry.Enabled}}, ` @{N="JoinDomainMethod";E={(($_ | Get-
VMHostProfile).ExtensionData.Config.ApplyProfile.Authentication.ActiveDirecto
ry | Select -ExpandProperty Policy | Where {$_.Id -eq
"JoinDomainMethodPolicy"}).Policyoption.Id}}# Check each host and their
domain membership statusGet-VMHost | Get-VMHostAuthentication | Select
VmHost, Domain, DomainMembershipStatus
```

Remediation:

To properly set the vSphere Authentication Proxy from Web Client directly:

1. Select the host
2. Click on `Configure` then expand `System`, select `Authentication Services`.
3. Click on `Join Domain`
4. Select `Using Proxy Server` radio button.
5. Provide proxy server IP address.

To properly set the vSphere Authentication Proxy via Host Profiles:

1. In the vSphere Web Client go to `Home` in the menu.
2. Click on `Policies and Profiles` followed by `Host Profiles`.
3. Choose the appropriate host profile
4. Select `Configure` followed by `Edit Host Profile...` then expand `Security and Services` followed by `Security Settings`, then `Authentication configuration`.
5. Select `Active Directory configuration`.
6. Set the `JoinDomain Method` is configured to `Use vSphere Authentication Proxy to add the host to the domain`.
7. Click on `Save`.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-084B74BD-40A5-4A4B-A82C-0C9912D580DC.html

Additional Information:

You can install vSphere Authentication Proxy on the same machine as the associated vCenter Server, or on a different machine that has network connection to the vCenter Server. The vSphere Authentication Proxy is not supported with vCenter Server versions earlier than version 5.0.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Internal Only - General

2.9 (L2) Ensure VDS health check is disabled (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The health check support in VDS helps you identify and troubleshoot configuration errors in a vSphere Distributed Switch. It is recommended that health check be turned off by default and confirmed that it is turned off when troubleshooting is finished.

Rationale:

vSphere Distributed switch health check once enabled, collects packets that contain information on host#, vds# port#, which an attacker would find useful.

Audit:

Using the vSphere Web Client for each VDS:

1. Select a VDS
2. Go to `Configure`, expand `Settings` then select `Health Check`.
3. Ensure that `VLAN and MTU` as well as `Teaming and failover` are set to `Disabled`.

Additionally, the following PowerCLI command can be used:

```
$vds = Get-VDSwitch
$vds.ExtensionData.Config.HealthCheckConfig
```

Remediation:

Using the vSphere Web Client for each VDS:

1. Select a VDS
2. Go to `Configure`, expand `Settings` then select `Health Check`.
3. Click on `Edit`.
4. Set `VLAN and MTU` state to `Disabled`.
5. Set `Teaming and failover` state to `Disabled`.
6. Click `OK`.

Additionally, the following PowerCLI command can be used:

Internal Only - General

```
Get-View -ViewType DistributedVirtualSwitch | ?{($_.config.HealthCheckConfig
| ?{$_.enable -notmatch "False"})}| %{$_.UpdateDVSHealthCheckConfig(@((New-
Object Vmware.Vim.VMwareDVSVlanMtuHealthCheckConfig -property
@{enable=0}),(New-Object Vmware.Vim.VMwareDVSTeamingHealthCheckConfig -
property @{enable=0})))}
```

Default Value:

By default, the vSphere Distributed Switch health check is not enabled and configured by default.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-4A6C1E1C-8577-4AE6-8459-EEB942779A82.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

3 Logging

This section contains recommendations related to ESXi's logging capabilities.

Internal Only - General

3.1 (L1) Ensure a centralized location is configured to collect ESXi host core dumps (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The VMware vSphere Network Dump Collector service allows for collecting diagnostic information from a host that experiences a critical fault. This service provides a centralized location for collecting ESXi host core dumps.

Rationale:

When a host crashes, an analysis of the resultant core dump is essential to being able to identify the cause of the crash and determine 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 commands:

```
# 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
```

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

Internal Only - General

3.2 (L1) Ensure persistent logging is configured for all ESXi hosts (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

ESXi can be configured to store log files on an in-memory file system. This occurs when the host's `Syslog.global.LogDir` property is set to a non-persistent location, such as `/scratch.` When this is done, only a single day's worth of logs are stored at any time. Additionally, log files will be reinitialized upon each reboot.

Rationale:

Non-persistent logging presents a security risk because 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:

To verify persistent logging is configured properly, perform the following from the vSphere web client:

1. Select the host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Select `Edit` then enter `Syslog.global.LogDir` in the filter.
4. Ensure `Syslog.global.logDir` field is not empty (null value) or is not set explicitly to a non-persistent datastore or a scratch partition.

If the Syslog.global.logDir parameter is pointing to 'Scratch' location (i.e. empty (null value) or is not set explicitly to a non-persistent datastore or a scratch partition), then ensure that the 'ScratchConfig.CurrentScratchLocation' parameter is also pointing to persistent storage.

Alternatively, the following PowerCLI command may be used:

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

Remediation:

To configure persistent logging properly, perform the following from the vSphere web client:

1. Select the host

Internal Only - General

2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Select `Edit` then enter `Syslog.global.LogDir` in the filter.
4. Set `Syslog.global.logDir` to a persistent location specified as [datastorename] path_to_file where the path is relative to the datastore. For example, [datastore1] /systemlogs.
5. Click `OK`.

Alternatively, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html
2. http://kb.vmware.com/kb/1033696

Additional Information:

Note: `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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

Internal Only - General

3.3 (L1) Ensure remote logging is configured for ESXi hosts (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

By default, ESXI logs are stored on a local scratch volume or ramdisk. To preserve logs, also configure remote logging to a central log host for the ESXI hosts.

Rationale:

Remote logging to a central log host provides a secure, centralized store for ESXi logs. 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 helps prevent log tampering and provides a long-term audit record.

Audit:

To ensure remote logging is configured properly, perform the following from the vSphere web client:

1. Select the host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Select `Edit` then enter `Syslog.global.logHost` in the filter.
4. Verify the `Syslog.global.logHost` is set to the hostname of the central log server.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To configure remote logging properly, perform the following from the vSphere web client:

1. Select the host
2. Click `Configure` then expand `System` then select `Advanced System Settings`.
3. Select `Edit` then enter `Syslog.global.logHost` in the filter.
4. Set the `Syslog.global.logHost` to the hostname or IP address of the central log server.
5. Click `OK`.

Internal Only - General

Alternately, run the following PowerCLI command:

```
# Set Syslog.global.logHost for each host
Get-VMHost | Foreach { Set-AdvancedSetting -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.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9F67DB52-F469-451F-B6C8-DAE8D95976E7.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

Internal Only - General

4 Access

This section contains recommendations related to ESXi access management.

Internal Only - General

4.1 (L1) Ensure a non-root user account exists for local admin access (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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. Use of this shared account should be limited, and named (non-root) user accounts with admin privileges should be used instead.

Rationale:

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. Limit the use of "root", including setting a highly complex password for the account, but do not remove the "root" account.

Audit:

To confirm one or more named user accounts have been established, perform the following for each ESXi host:

1. Connect directly to the ESXi host using the VMware Host Client.
2. Login as root or another authorized user.
3. Select `Manage`, then select the `Security & Users` tab.
4. Select `Users` to view the local users.
5. Ensure at least one user exists that possesses the following:
6. The user has been granted shell access.
7. Select the host then click `Actions` followed by `Permissions` and verify the `Administrator` role has been granted to the user.

Note: You cannot create ESXi users with the vSphere Client. You must directly log in to the host with the VMware Host Client to create ESXi users.

Remediation:

To create one or more named user accounts (local ESXi user accounts), perform the following using the vSphere client (not the vSphere web client) for each ESXi host:

1. Connect directly to the ESXi host using the vSphere Client.
2. Login as root.
3. Select `Manage`, then select the `Security & Users` tab.
4. Select `Users` then click `Add user` to add a new user.
5. Once added now select the Host, then select `Actions` followed by `Permissions`.

Internal Only - General

6. Assign the `Administrator` role to the user.

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.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.hostclient.doc/GUID-0898677F-CE98-41FB-A488-29DF6210CF5D.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

Internal Only - General

4.2 (L1) Ensure passwords are required to be complex (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

ESXi uses the `pam_passwdqc.so` plug-in to set password strength and complexity. Options include setting minimum password length, requiring password characters to come from particular character sets, and restricting the number of consecutive failed logon attempts permitted. The settings should enforce the organization's password policies.

Note that an uppercase character that begins a password does not count toward the number of character classes used, and neither does a number that ends a password.

Rationale:

All passwords for ESXi hosts should be hard to guess to reduce the risk of unauthorized access.

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

Impact:

The remediation requires all passwords to be 14 or more characters long and comprised of at least one character from four distinct character sets.

Audit:

To confirm password complexity requirements are set, 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 N0 is set to `disabled`.
5. Confirm N1 is set to `disabled`.
6. Confirm N2 is set to `disabled`.
7. Confirm N3 is set to `disabled`.
8. Confirm N4 is set to `14` or greater.

or

Internal Only - General

1. Login to the ESXi host
2. Navigate to Host/Manage/System/Advanced settings
3. Locate the following key:

```
Security.PasswordQualityControl
```

verify that 4. Set N0 to `disabled`. 5. Set N1 to `disabled`. 6. Set N2 to `disabled`. 7. Set N3 to `disabled`. 8. Set N4 to `14` or greater.

The string should look like this: retry=3 min=disabled,disabled,disabled,disabled,14

Remediation:

To set the password complexity requirements, perform the following:

1. Login to the ESXi host
2. Navigate to Host/Manage/System/Advanced settings
3. Locate the following key:

```
Security.PasswordQualityControl
```

4. Set N0 to `disabled`.
5. Set N1 to `disabled`.
6. Set N2 to `disabled`.
7. Set N3 to `disabled`.
8. Set N4 to `14` or greater.

The string should look like this: retry=3 min=disabled,disabled,disabled,disabled,14

References:

1. http://www.openwall.com/passwdqc/README.shtml
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43.html
3. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

4.3 (L1) Ensure the maximum failed login attempts is set to 5 (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Authentication should be configured so there is a maximum number of consecutive failed login attempts for each account, at which point the account at risk will be locked out.

Rationale:

Multiple account login failures for the same account could possibly be an attacker trying to brute force guess the password.

Impact:

A users account will be locked after 5 unsuccessful login attempts.

Audit:

To verify the maximum failed login attempts is set properly, perform the following steps:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.AccountLockFailures` in the filter.
5. Verify that the value for this parameter is set to `5`.

Alternately, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures
```

Remediation:

To set the maximum failed login attempts correctly, perform the following steps:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.AccountLockFailures` in the filter.
5. Set the value for this parameter to `5`.

Alternately, use the following PowerCLI command:

Internal Only - General

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-
AdvancedSetting -Value 5
```

References:

1. https://code.vmware.com/apis/196/vsphere#https://vdc-repo.vmware.com/vmwb-repository/dcr-public/6b586ed2-655c-49d9-9029-bc416323cb22/fa0b429a-a695-4c11-b7d2-2cbc284049dc/doc/vim.option.OptionManager.html
2. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

Internal Only - General

4.4 (L1) Ensure account lockout is set to 15 minutes (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

An account is automatically locked after the maximum number of failed consecutive login attempts is reached. The account should be automatically unlocked after 15 minutes, otherwise administrators will need to manually unlock accounts on request by authorized users.

Rationale:

This setting reduces the inconvenience for benign users and the overhead on administrators, while also severely slowing down any brute force password guessing attacks.

Audit:

To verify the account lockout is set to 15 minutes, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.AccountUnlockTime` in the filter.
5. Verify that the value for this parameter is set to 900.

Alternately, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime
```

Remediation:

To set the account lockout to 15 minutes, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.AccountUnlockTime` in the filter.
5. Set the value for this parameter to `900`.

Alternately, use the following PowerCLI command:

Internal Only - General

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime | Set-
AdvancedSetting -Value 900
```

References:

1. https://code.vmware.com/apis/1067/vsphere
2. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

4.5 (L1) Ensure previous 5 passwords are prohibited (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This setting prevents users from utilizing previously used passwords.

Rationale:

Users may attempt to reuse passwords which could lead to a compromised password being used. At least the past 5 passwords should be prevented from use for a user to ensure password re-use is not occurring.

Impact:

Users will be unable to use any of their past 5 passwords.

Audit:

To verify the password history is set to 5, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.PasswordHistory` in the filter.
5. Verify that the value for this parameter is set to `5`.

Alternately, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting Security.PasswordHistory
```

Remediation:

To set the password history 5, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `Security.PasswordHistory` in the filter.
5. Set the value for this parameter is set to `5`.

Alternately, the following PowerCLI command may be used:

Internal Only - General

```
Get-VMHost | Get-AdvancedSetting Security.PasswordHistory | Set-
AdvancedSetting -Value 5
```

Default Value:

None

References:

1. https://www.cisecurity.org/white-papers/cis-password-policy-guide/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

4.6 (L1) Ensure Active Directory is used for local user authentication (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Note: If the AD group "ESX Admins" (default) is created, all users and groups that are members of this group will have full administrative access to all ESXi hosts in the domain.

Rationale:

Joining ESXi hosts to an Active Directory (AD) domain eliminates 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:

To confirm AD is used for local user authentication, perform the following from the vSphere Web Client:

1. Select the host
2. Click on `Configure` then expand `System`.
3. Select `Authentication Services`.
4. Ensure the configuration is in accordance with your organization's Active Directory configuration.

Alternately, execute the following PowerCLI command:

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

Remediation:

To use AD for local user authentication, perform the following from the vSphere Web Client:

1. Select the host
2. Click on `Configure` then expand `System`.
3. Select `Authentication Services`.
4. Click `Join Domain` followed by the appropriate domain and credentials.

Internal Only - General

5. Click OK.

Alternately, 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.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-63D22519-38CC-4A9F-AE85-97A53CB0948A.html
2. https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/securityadvisories/0/24505

Additional Information:

Attention should be given to Broadcom, and AD reported vulnerabilities and security fixes, and applied where appropriate.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Internal Only - General

4.7 (L1) Ensure only authorized users and groups belong to the esxAdminsGroup group (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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 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 or group having membership in the `esxAdminsGroup` group will have full administrative access to all ESXi hosts. Such users may compromise the confidentiality, availability, and integrity of the all ESXi hosts and the respective data and processes they influence.

Audit:

To verify only authorized users and groups belong to `esxAdminsGroup`, go to Active Directory and review the membership of the group name that is defined by the advanced host setting: `Config.HostAgent.plugins.hostsvc.esxAdminsGroup`.

Remediation:

To remove unauthorized users and groups belonging to `esxAdminsGroup`, perform the following steps after coordination between vSphere admins and Active Directory admins:

1. Verify the setting of the `esxAdminsGroup` attribute.
2. View the list of members for that Microsoft Active Directory group.
3. Remove all unauthorized users and groups from that 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`".

Default Value:

"ESX Admins"

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

Internal Only - General

4.8 (L1) Ensure the Exception Users list is properly configured (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Users who are added to the "Exception Users" list do not lose their permissions when the host enters lockdown mode. Usually you may want to add some service accounts, such as a backup agent, to the Exception Users list.

Rationale:

Users who do not require special permissions should not be exempted from lockdown mode because this increases the risk of unauthorized actions being performed, especially if a user account is compromised.

Impact:

If a user is not added to the exception list but should be when host is in lockdown mode they will be unable to perform operations.

Audit:

To verify the membership of the "Exception Users" list, perform the following in the vSphere Web Client:

1. Select the host.
2. Click on `Configure` then expand `System` and select `Security Profile`.
3. Under `Lockdown Mode` view and verify the list of `Exception Users` for accuracy.

Remediation:

To correct the membership of the `Exception Users` list, perform the following in the vSphere Web Client:

1. Select the host.
2. Click on `Configure` then expand `System` and select `Security Profile`.
3. Select `Edit` next to `Lockdown Mode`.
4. Click on `Exception Users`.
5. Add or delete users as appropriate.
6. Click `OK`.

Internal Only - General

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-6CD8C2E3-7925-4706-8271-F42F2BCFF95D.html?hWord=N4IghgNiBcIQ9gYwNYBN4HcB2ACAtvKgKYgC+QA

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

Internal Only - General

5 Console

This section contains recommendations related to ESXi consoles.

Internal Only - General

5.1 (L1) Ensure the DCUI timeout is set to 600 seconds or less (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Direct Console User Interface (DCUI) is used for directly logging into an ESXi host and carrying out host management tasks. This setting terminates an idle DCUI session after the specified number of seconds has elapsed.

Rationale:

Terminating idle DCUI sessions helps avoid unauthorized usage of the DCUI originating from leftover login sessions.

Audit:

To verify the DCUI timeout setting, perform the following steps:

1. From the vSphere Web Client, select the host.
2. Click `Configure`, then under `System` select `Advanced System Settings`.
3. Select `Edit` then enter `UserVars.DcuiTimeOut` in the filter.
4. Verify that the value for this parameter is 600 seconds or less.

Alternately, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut
```

Remediation:

To correct the DCUI timeout setting, perform the following steps:

1. From the vSphere Web Client, select the host.
2. Click `Configure`, then under `System` select `Advanced System Settings`.
3. Select `Edit` then enter `UserVars.DcuiTimeOut` in the filter.
4. Click in the box for the current value, then set the value to 600 seconds or less.

Alternately, use the following PowerCLI command:

Internal Only - General

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut | Set-
AdvancedSetting -Value 600
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.2 (L1) Ensure the ESXi shell is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The ESXi shell is an interactive command line environment available from the Direct Console User Interface (DCUI) or remotely via SSH. The ESXi shell should only be enabled on a host when running diagnostics or troubleshooting.

Rationale:

Activities performed from the ESXi shell bypass vCenter RBAC and audit controls, so the ESXi shell should only be enabled when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere web client or vCLI/PowerCLI.

Audit:

To verify the ESXi shell is disabled, perform the following:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Services`.
3. Click on `ESXi Shell` then click `Edit Startup Policy`.
4. Verify the Startup Policy is set to `Start and Stop Manually`.

Alternately, the following PowerCLI command may be used:

```
# Check if the 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 whenever the ESXi shell is enabled on a host.

Remediation:

To disable the ESXi shell, perform the following:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Services`.
3. Click on `ESXi Shell` then click `Edit Startup Policy`.
4. Set the Startup Policy is set to `Start and Stop Manually`.
5. Click on `OK`.

Alternately, use the following PowerCLI command:

Internal Only - General

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-B5144CE9-F8BB-494D-8F5D-0D5621D65DAE.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-DFA67697-232E-4F7D-860F-96C0819570A8.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

5.3 (L1) Ensure SSH is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The ESXi shell, when enabled, can be accessed directly from the host console through the DCUI or remotely using SSH. Disable Secure Shell (SSH) for each ESXi host to prevent remote access to the ESXi shell, and only enable SSH when needed for troubleshooting or diagnostics.

Rationale:

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.

Impact:

In troubleshooting and assessment scenarios having SSH disabled, which is the default, may prevent connections to the host by tools or via other methods.

Audit:

To verify SSH is disabled, perform the following:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Services`.
3. Click on `SSH` then click `Edit Startup Policy`.
4. Verify the Startup Policy is set to `Start and Stop Manually`.

Alternately, 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 whenever SSH is enabled on a host.

Remediation:

To disable SSH, perform the following:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Services`.
3. Click on `SSH` then click `Edit Startup Policy`.
4. Set the Startup Policy is set to `Start and Stop Manually`.
5. Click `OK`.

Internal Only - General

6. While `ESXi Shell` is still selected click `Stop`.

Alternately, use the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-12E27BF3-3769-4665-8769-DA76C2BC9FFE.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

5.4 (L1) Ensure CIM access is limited (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The Common Information Model (CIM) system provides an interface that enables hardware-level management from remote applications using a set of standard APIs. Provide only the minimum access necessary to applications. Do not provision CIM-based hardware monitoring tools and other third-party applications to run as root or as another administrator account. Instead, create a dedicated service account specific to each CIM application with the minimal access and privileges needed for that application.

Rationale:

If CIM-based hardware monitoring tools or other third-party applications are granted unneeded administrator level access, they could potentially be used to compromise the security of the host.

Impact:

CIM-based hardware monitoring tools or other third-party applications that utilize CIM may not function as expected.

Audit:

To verify CIM access is limited, check for a limited-privileged service account with the following CIM roles applied:

`Host.Config.SystemManagement` `Host.CIM.CIMInteraction`

Alternately, the following PowerCLI command may be used:

```
# List all user accounts on the Host -Host Local connection required-
Get-VMHostAccount
```

Remediation:

To limit CIM access, perform the following:

1. Create a limited-privileged service account for CIM and other third-party applications.
2. This account should access the system via vCenter.
3. Give the account the `CIM Interaction` privilege only. This will enable the account to obtain a CIM ticket, which can then be used to perform both read and write CIM operations on the target host. If an account must connect to the host directly, this account must be granted the full "Administrator" role on the host. This is not recommended unless required by the monitoring software being used.

Internal Only - General

Alternately, run the following PowerCLI command:

```
# Create a new host user account -Host Local connection required-
New-VMHostAccount -ID ServiceUser -Password <password> -UserAccount
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-645EBD81-CF86-44D7-BE77-224EF963D145.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

Internal Only - General

5.5 (L1) Ensure Normal Lockdown mode is enabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Enabling lockdown mode disables direct local access to an ESXi host, requiring the host be managed remotely from vCenter Server.

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 who log in using authorized keys. Also, users in the DCUI.Access list for each host are allowed to override lockdown mode and log in to the DCUI. By default, the "root" user is the only user listed in the DCUI.Access list.

Rationale:

Lockdown mode limits ESXi host access to the vCenter server 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.

Impact:

With lockdown mode enabled the host will only be accessible through vCenter preventing 'local' access.

Audit:

To verify lockdown mode is enabled, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Security Profile`.
3. Verify that `Lockdown Mode` is set to `Normal`.

Alternately, 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:

To enable lockdown mode, perform the following from the vSphere web client:

Internal Only - General

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Security Profile`.
3. Across from `Lockdown Mode` click on `Edit`.
4. Click the radio button for `Normal`.
5. Click `OK`.

Alternately, run the following PowerCLI command:

```
# Enable lockdown mode for each host
(Get-VMHost | Get-View).EnterLockdownMode()
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Internal Only - General

5.6 (L2) Ensure Strict Lockdown mode is enabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Enabling lockdown mode disables direct local access to an ESXi host, requiring the host be managed remotely from vCenter Server.

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 who log in using authorized keys. Also, users in the DCUI.Access list for each host are allowed to override lockdown mode and log in to the DCUI. By default, the "root" user is the only user listed in the DCUI.Access list.

Rationale:

Lockdown mode limits ESXi host access to the vCenter server 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. Additionally strict lockdown move will disabled DCUI - Disabling DCUI prevents all local activity, and thus forces actions to be performed in vCenter Server, where they can be centrally audited and monitored.

Impact:

With lockdown mode enabled the host will only be accessible through vCenter preventing 'local' access. Disabling the DCUI can create a potential "lockout" situation, should the host become isolated from vCenter Server. Recovering from a "lockout" scenario requires reinstalling ESXi. Consider leaving DCUI enabled, and instead enable lockdown mode and limit the users allowed to access the DCUI using the DCUI.Access list.

Audit:

To verify lockdown mode is enabled, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Security Profile`.
3. Verify that `Lockdown Mode` is set to `Strict`.

Alternately, the following PowerCLI command may be used:

Internal Only - General

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

Remediation:

To enable lockdown mode, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Select `Configure` then expand `System` and select `Security Profile`.
3. Across from `Lockdown Mode` click on `Edit`.
4. Click the radio button for `Strict`.
5. Click `OK`.

Alternately, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-88B24613-E8F9-40D2-B838-225F5FF480FF.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

Internal Only - General

5.7 (L2) Ensure the SSH authorized_keys file is empty (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

ESXi hosts come with Secure Shell (SSH), which can be configured to authenticate remote users using public key authentication. For day-to-day operations, the ESXi host should be in lockdown mode with the SSH service disabled. Lockdown mode does not prevent root users from logging in using keys. The presence of a remote user's public key in the `/etc/ssh/keys-root/authorized_keys` file on an ESXi host identifies the user as trusted, meaning the user is granted access to the host without providing a password.

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

Rationale:

Keeping the authorized_keys file empty prevents users from circumventing the intended restrictions of lockdown mode.

Audit:

To verify the `authorized_keys` file does not contain any keys, perform the following:

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

- SSH may need to be enabled first.

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

Remediation:

To remove all keys from the authorized_keys file, perform the following:

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

- SSH may need to be enabled first

2. Edit the `/etc/ssh/keys-root/authorized_keys` file.
3. Remove all keys from the file and save the file.

Default Value:

The file is empty by default.

Internal Only - General

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-392ADDE9-FD3B-49A2-BF64-4ACBB60EB149.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

5.8 (L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The `ESXiShellInteractiveTimeOut` allows you to automatically terminate idle ESXi shell and SSH sessions. The permitted idle time should be 300 seconds or less.

Rationale:

If a user forgets to log out of an ESXi shell or SSH session, the idle session will exist indefinitely, increasing the potential for someone to gain unauthorized privileged access to the host, unless a timeout is set.

Audit:

To verify the timeout is set correctly, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `ESXiShellInteractiveTimeOut` in the filter.
5. Verify that the value for this parameter is set to `300` or less.

Note: A value of 0 disables the ESXiShellInteractiveTimeOut.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To set the timeout to the desired value, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `ESXiShellInteractiveTimeOut` in the filter.
5. Set the value for this parameter is set to the appropriate value (`300` seconds or less).
6. Click `OK`.

Internal Only - General

Note: A value of 0 disables the ESXi ShellInteractiveTimeOut.

Alternately, use the following PowerCLI command:

```
# Set Remove UserVars.ESXiShellInteractiveTimeOut to 300 on all hosts
Get-VMHost | Get-AdvancedSetting -Name 'UserVars.ESXiShellInteractiveTimeOut'
| Set-AdvancedSetting -Value "300"
```

References:

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

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.9 (L1) Ensure the shell services timeout is set to 1 hour or less (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

When the ESXi shell or SSH services are enabled on a host, they will run indefinitely. To avoid this, set the `ESXiShellTimeOut`, which defines a window of time after which the ESXi shell and SSH services will automatically be terminated.

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

Rationale:

This reduces the risk of an inactive ESXi shell or SSH service being misused by an unauthorized party to compromise a host.

Audit:

To verify the timeout is set to one hour or less, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `ESXiShellTimeOut` in the filter.
5. Verify that the value for this parameter is set to `3600` (1 hour) or less.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To set the timeout to the desired value, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `ESXiShellTimeOut` in the filter.
5. Set the value for this parameter is set to `3600` (1 hour) or less
6. Click `OK`.

Internal Only - General

Note: A value of 0 disables the ESXiShellTimeOut.

Alternately, run the following PowerCLI command:

```
# Set UserVars.ESXiShellTimeOut to 3600 on all hosts
Get-VMHost | Get-AdvancedSetting -Name 'UserVars.ESXiShellTimeOut' | Set-
AdvancedSetting -Value "3600"
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-6E1ECA4D-B617-4D42-B40B-71E4C83DEEFB.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-B314F79B-2BDD-4D68-8096-F009B87ACB33.html
3. http://kb.vmware.com/kb/2004746
4. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-94F0C54F-05E3-4E16-8027-0280B9ED1009.html

Additional Information:

This value can be set in minutes via the DCUI. When using the vCenter GUI or PowerShell API, the value is set in seconds.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

Internal Only - General

5.10 (L1) Ensure DCUI has a trusted users list for lockdown mode (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Lockdown mode disables direct host access, requiring admins to manage hosts from vCenter. Set DCUI.Access to a list of highly trusted users who would be able to override lockdown mode and access the DCUI in the event an ESXi host became isolated from vCenter.

NOTE: If you disable lockdown mode using the DCUI, all users with the DCUI.Access privilege will be granted the Administrator role on the host.

Rationale:

The list prevents all admins from becoming locked out and no longer being able to manage the host.

Audit:

To verify a proper trusted users list is set for DCUI, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `DCUI.Access` in the filter.
5. Verify that the `DCUI.Access` attribute is set to a comma-separated list of the users who are allowed to override lockdown mode.

Alternately, the following PowerCLI command may be used:

```
Get-VMHost | Get-AdvancedSetting -Name DCUI.Access
```

Remediation:

To set a trusted users list for DCUI, perform the following from the vSphere web client:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `System`.
3. Select `Advanced System Settings` then click `Edit`.
4. Enter `DCUI.Access` in the filter.
5. Set the `DCUI.Access` attribute is set to a comma-separated list of the users who are allowed to override lockdown mode.

Internal Only - General

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-6779F098-48FE-4E22-B116-A8353D19FF56.html

Additional Information:

Note: 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 user's admin privileges on the host.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●

Internal Only - General

5.11 (L2) Ensure contents of exposed configuration files have not been modified (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Although most configurations on ESXi are controlled via an API, there are a limited set of configuration files that are used directly to govern host behavior. These files are exposed via the vSphere HTTPS-based file transfer API. These files should be monitored for modifications.

WARNING: Do not attempt to monitor files that are NOT exposed via this file transfer API, since this can result in a destabilized system.

Rationale:

Any changes to these files should be correlated with an approved administrative action, such as an authorized configuration change. Tampering with these files could enable unauthorized access to the host configuration and virtual machines.

Audit:

To verify the exposed configuration files have not been modified, perform the following:

1. Open a web browser.
2. Find the ESXi configuration files by browsing to `https://(hostname)/host` (not available if MOB is disabled).
3. Review the contents of those files to confirm no unauthorized modifications have been made.

NOTE: Not all the files listed are modifiable.

Alternately, the configuration files can also be retrieved using the vCLI or PowerCLI.

Remediation:

Restore all modified configuration files to a known good state by restoring backups or using other means.

To help prevent future occurrences, you can back up the host configuration data after configuring or reconfiguring an ESXi host. The vicfg-cfgbackup command is available only for ESXi hosts; it is not available through a vCenter Server system connection. No equivalent ESXCLI command is supported.

Internal Only - General

To help identify future occurrences more quickly, implement a procedure to monitor the files and their contents over time to ensure they are not improperly modified. Be sure not to monitor log files and other files whose content is expected to change regularly due to system activity. Also, account for configuration file changes that are due to authorized administrative activity.

Note: Host Profiles may also be used to track configuration changes on the host; however, Host Profiles do not track all configuration changes.

Additional Information:

During a configuration backup, the serial number is backed up with the configuration. The number is restored when you restore the configuration. The number is not preserved when you run the Recovery CD (ESXi Embedded) or perform a repair operation (ESXi Installable). You can back up and restore configuration information as follows:

1. Back up the configuration by using the vicfg-cfgbackup command.
2. Run the Recovery CD or repair operation
3. Restore the configuration by using the vicfg-cfgbackup command.

When you restore a configuration, you must make sure that all virtual machines on the host are stopped.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

Internal Only - General

Internal Only - General

6 Storage

This section contains recommendations related to ESXi disk and other storage-related settings.

Internal Only - General

6.1 (L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. Bidirectional Challenge-Handshake Authentication Protocol (CHAP), also known as Mutual CHAP, should be enabled to provide bidirectional authentication.

Rationale:

By not authenticating both the iSCSI target and host, there is a potential for a man-in-the-middle attack in which an attacker might impersonate either side of the connection to steal data. Bidirectional authentication can mitigate this risk.

Note: Choosing not to enforce bidirectional authentication can make sense if you create a dedicated network or VLAN to service all your iSCSI devices. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.

Audit:

To verify that bidirectional CHAP authentication is enabled for iSCSI traffic, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Storage`.
3. Select `Storage Adapters` then select the iSCSI Adapter.
4. Under `Properties` verify that the Authentication method is set to `Use bidirectional CHAP`.

Alternately, 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 enable bidirectional CHAP authentication for iSCSI traffic, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Storage`.
3. Select `Storage Adapters` then select the iSCSI Adapter.
4. Under `Properties` click on `Edit` next to `Authentication`.

Internal Only - General

5. Next to `Authentication Method` select `Use bidirectional CHAP` from the dropdown.
6. Specify the outgoing CHAP name.

- Make sure that the name you specify matches the name configured on the storage side.
    - To set the CHAP name to the iSCSI adapter name, select "Use initiator name".
    - To set the CHAP name to anything other than the iSCSI initiator name, deselect "Use initiator name" and type a name in the Name text box.

8. Enter an outgoing CHAP secret to be used as part of authentication. Use the same secret as your storage side secret.
9. Specify incoming CHAP credentials. Make sure your outgoing and incoming secrets do not match.
10. Click `OK`.
11. Click the second to last symbol labeled `Rescan Adapter`.

Alternately, 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
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-2F1E64DB-20BB-4D18-A083-8E65FE380899.html

Additional Information:

Prerequisites- Before setting up CHAP parameters for software or dependent hardware iSCSI, determine whether to configure unidirectional or bidirectional CHAP. Independent hardware iSCSI adapters do not support bidirectional CHAP.

- Verify CHAP parameters configured on the storage side. Parameters that you configure must match the ones on the storage side.
- Required privilege: `Host.Configuration.Storage Partition Configuration`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

Internal Only - General

6.2 (L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Challenge-Handshake Authentication Protocol (CHAP) requires both client and host to know the secret (password) to establish a connection. Each mutual authentication secret should be unique.

Rationale:

If all mutual authentication secrets are unique, compromise of one secret does not allow an attacker to authenticate to other hosts or clients using that same secret.

Audit:

To verify the CHAP secrets are unique, run the following to list all iSCSI adapters and their corresponding CHAP configuration:

```
# 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 change the values of CHAP secrets so they are unique, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Storage`.
3. Select `Storage Adapters` then select the iSCSI Adapter.
4. Under `Properties` click on `Edit` next to `Authentication`.
5. Next to `Authentication Method` specify the authentication method from the dropdown.
    - None
    - Use unidirectional CHAP if required by target
    - Use unidirectional CHAP unless prohibited by target
    - Use unidirectional CHAP
    - Use bidirectional CHAP
6. Specify the outgoing CHAP name.

- Make sure that the name you specify matches the name configured on the storage side.
    - To set the CHAP name to the iSCSI adapter name, select "Use initiator name".

Internal Only - General

- To set the CHAP name to anything other than the iSCSI initiator name, deselect "Use initiator name" and type a name in the Name text box.

8. Enter an outgoing CHAP secret to be used as part of authentication. Use the same secret as your storage side secret.
9. If configuring with bidirectional CHAP, specify incoming CHAP credentials.

- Make sure your outgoing and incoming secrets do not match.

10. If configuring with bidirectional CHAP, specify incoming CHAP credentials.

- Make sure your outgoing and incoming secrets do not match.

11. Click `OK`.
12. Click the second to last symbol labeled `Rescan Adapter`

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-AC65D747-728F-4109-96DD-49B433E2F266.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.storage.doc/GUID-2F1E64DB-20BB-4D18-A083-8E65FE380899.html

Additional Information:

If you change the CHAP parameters, they are used for new iSCSI sessions. For existing sessions, new settings are not used until you log out and log in again.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

Internal Only - General

6.3 (L1) Ensure storage area network (SAN) resources are segregated properly (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Use zoning and logical unit number (LUN) masking to segregate storage area network (SAN) activity.

Zoning provides access control in the SAN topology. Zoning defines which host bus adapters (HBAs) can connect to which targets. The devices outside a zone are not visible to the devices inside the zone when SAN zoning is configured. For example, zones defined for testing should be managed independently within the SAN so they do not interfere with activity in the production zones. Similarly, you can set up different zones for different departments. Zoning must take into account any host groups that have been set up on the SAN device.

LUN masking is a process that makes a LUN available to some hosts and unavailable to other hosts.

Rationale:

Segregating SAN activity can reduce the attack surface for the SAN, prevent non-ESXi systems from accessing SANs, and separate environments, for example, test and production environments.

Audit:

The audit procedures to verify SAN activity is properly segregated are SAN vendor or product-specific.

Remediation:

The remediation procedures to properly segregate SAN activity are SAN vendor or product-specific.

In general, with ESXi hosts, use a single-initiator zoning or a single-initiator-single-target zoning. The latter is a preferred zoning practice. Using the more restrictive zoning prevents problems and misconfigurations that can occur on the SAN.

References:

1. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-6029358F-8EE8-4143-9BB0-16ABB3CA0FE3.html

Internal Only - General

2. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-BFE9046A-2278-4026-809A-ED8F9D8FDACE.html
3. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.storage.doc/GUID-39A4551F-4B03-43A6-BEDF-FAB1528C070D.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.12 Segment Data Processing and Storage Based on Sensitivity Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.		●	●
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●
v7	14.2 Enable Firewall Filtering Between VLANs Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.		●	●

Internal Only - General

7 vNetwork

This section contains recommendations related to configuring vNetwork.

Internal Only - General

7.1 (L1) Ensure the vSwitch Forged Transmits policy is set to reject (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring a standard switch. Set the vSwitch Forged Transmits policy to reject for each vSwitch. Reject Forged Transmit can be set at the vSwitch and/or the Portgroup level. You can override switch-level settings at the Portgroup level.

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. Setting forged transmissions to accept 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.

Impact:

This will prevent VMs from changing their effective MAC address. This will affect applications that require this functionality, such as Microsoft Clustering, which requires systems to effectively share a MAC address. This will 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:

To verify the policy is set to reject forged transmissions, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Verify that `Forged transmits` is set to `Reject` in the dropdown.

Alternately, the following PowerCLI command may be used:

Internal Only - General

```
# 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:

To set the policy to reject forged transmissions, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Set `Forged transmits` to `Reject` in the dropdown.
6. Click on `OK`.

Alternately, the following ESXi shell command may be used:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

7.2 (L1) Ensure the vSwitch MAC Address Change policy is set to reject (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring a standard switch. Ensure the MAC Address Change policy within the vSwitch is set to reject. Reject MAC Changes can be set at the vSwitch and/or the Portgroup level. You can override switch-level settings at the Portgroup level.

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.

Impact:

This will prevent VMs from changing their effective MAC address. It will affect applications that require this functionality, such as Microsoft Clustering, which requires systems to effectively share a MAC address. This will 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:

To verify the policy is set to reject, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Verify that `MAC address changes` is set to `Reject` in the dropdown.

Alternately, the following PowerCLI command may be used:

Internal Only - General

```
# 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:

To set the policy to reject, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Set `MAC address changes` to `Reject` in the dropdown.
6. Click on `OK`.

Alternately, perform the following using the ESXi shell:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

7.3 (L1) Ensure the vSwitch Promiscuous Mode policy is set to reject (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring a standard switch. Ensure the Promiscuous Mode Policy within the vSwitch is set to reject. Promiscuous mode can be set at the vSwitch and/or the Portgroup level. You can override switch-level settings at the Portgroup level.

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. This could enable unauthorized access to the contents of those packets.

Impact:

There might be a legitimate reason to enable promiscuous mode 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:

To verify the policy is set to reject, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Verify that `Promiscuous mode` is set to `Reject` in the dropdown.

Alternately, the following PowerCLI command may be used:

Internal Only - General

```
# 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:

To set the policy to reject, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches` then click `Edit`.
4. Click on `Security`.
5. Set `Promiscuous mode` to `Reject` in the dropdown.
6. Click on `OK`.

Alternately, perform the following via the ESXi shell:

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

Default Value:

Reject

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-891147DD-3E2E-45A1-9B50-7717C3443DD7.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

Internal Only - General

7.4 (L1) Ensure port groups are not configured to the value of the native VLAN (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring pyrtgroups for a standard switch. ESXi does not use the concept of native VLAN, so do not configure port groups to use the native VLAN ID. 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.

Rationale:

Frames with VLAN specified in the port group will have a tag, but frames without a VLAN specified in the port group are not tagged and therefore will end up as belonging to the 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:

To verify the native VLAN ID is not being used for port groups, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.
5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.

Alternately, the following PowerCLI command may be used:

Internal Only - General

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

Remediation:

To stop using the native VLAN ID for port groups, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.
5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.
7. If a VLAN ID change is needed, click the name of the port group in the topology diagram of the virtual switch.
8. Click the `Edit settings` option.
9. In the Properties section, enter an appropriate name in the `Network label` field.
10. In the `VLAN ID` dropdown select or type a new VLAN.
11. Click `OK`.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-3A9D9911-3632-4B81-9D2E-A2F9F2D01180.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

7.5 (L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring pyrtgroups for a standard switch. Ensure that port groups are not configured to VLAN values reserved by upstream physical switches. 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 the documentation for your specific switch.

Rationale:

Using a reserved VLAN might result in a denial of service on the network.

Audit:

To verify port groups are not using reserved VLAN values, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.
5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To change the VLAN values for port groups to non-reserved values, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.

Internal Only - General

5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.
7. If a VLAN ID change is needed, click the name of the port group in the topology diagram of the virtual switch.
8. Click the `Edit settings` option.
9. In the Properties section, enter an appropriate name in the `Network label` field.
10. In the `VLAN ID` dropdown select or type a new VLAN.
11. Click `OK`.

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

7.6 (L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT) (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

This recommendation is intended to address configuring portgroups for a standard switch. Port groups should not be configured to VLAN 4095 or 0 except for Virtual Guest Tagging (VGT). When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest virtual machine without modifying the VLAN tags, leaving it up to the guest to deal with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself.

Rationale:

If VGT is enabled inappropriately, it might cause a denial of service or allow a guest virtual machine to interact with traffic on an unauthorized VLAN.

Audit:

To verify port groups are not set to 4095 unless VGT is required, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.
5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.

Additionally, the following PowerCLI command may be used:

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

Remediation:

To set port groups to values other than 4095 and 0 unless VGT is required, perform the following:

1. From the vSphere Web Client, select the host.
2. Click `Configure` then expand `Networking`.
3. Select `Virtual switches`.
4. Expand the Standard vSwitch.

Internal Only - General

5. View the topology diagram of the switch, which shows the various port groups associated with that switch.
6. For each port group on the vSwitch, verify and record the VLAN IDs used.
7. If a VLAN ID change is needed, click the name of the port group in the topology diagram of the virtual switch.
8. Click the `Edit settings` option.
9. In the Properties section, enter an appropriate name in the `Network label` field.
10. In the `VLAN ID` dropdown select or type a new VLAN.
11. Click `OK`.

References:

1. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/vlans.html#wp1038758

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

7.7 (L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The vSphere VDS can export Netflow information about traffic crossing the VDS. These exports are not encrypted and can contain information about the virtual network making it easier for a Man in the Middle attack to be executed successfully.

NOTE: This is only valid if utilizing VMware vCenter

Rationale:

If Netflow export is required, verify that all VDS Netflow target systems are approved collectors by confirming the IP's are set correctly.

NOTE: This is only valid if utilizing VMware vCenter

Audit:

Using the vSphere Web Client

1. Go to the Networking section of vCenter
2. After selecting each individual switch you will need to perform the following.
3. Go to `Configure` then expand `Settings`.
4. Click on `Netflow`.
5. Verify that `Collector IP address` and `Collector port` are appropriately configured.

Additionally, the following PowerCLI command may be used

```
Get-VDPortgroup | Select Name, VirtualSwitch,
@{Name="NetflowEnabled";Expression={$_.Extensiondata.Config.defaultPortConfig
.ipfixEnabled.Value}} | Where-Object {$_.NetflowEnabled -eq "True"}
```

Remediation:

Using the vSphere Web Client

1. Go to the Networking section of vCenter
2. After selecting each individual switch you will need to perform the following.
3. Go to `Configure` then expand `Settings`.
4. Click on `Netflow`.
5. Click on `Edit`.
6. Enter the `Collector IP address` and `Collector port` as required.

Internal Only - General

7. Click OK.

Additionally, the following PowerCLI command may be used

```
"# Disable Netfow for a VDPortgroup
$DPortgroup = <name of portgroup>
Get-VDPortgroup $DPortGroup | Disable-PGNetflow

#Function for  Disable-PGNetflow
#From: http://www.virtu-al.net/2013/07/23/disabling-netflow-with-powercli/

Function Disable-PGNetflow {
   [CmdletBinding()]
   Param (
      [Parameter(ValueFromPipeline=$true)]
      $DVPG
   )
   Process {
      Foreach ($PG in $DVPG) {
         $spec = New-Object VMware.Vim.DVPortgroupConfigSpec
         $spec.configversion = $PG.Extensiondata.Config.ConfigVersion
         $spec.defaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
         $spec.defaultPortConfig.ipfixEnabled = New-Object
VMware.Vim.BoolPolicy
         $spec.defaultPortConfig.ipfixEnabled.inherited = $false
         $spec.defaultPortConfig.ipfixEnabled.value = $false

         $PGView = Get-View -Id $PG.Id
         $PGView.ReconfigureDVPortgroup_Task($spec)
      }
   }
}
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-FA661AE0-C0B5-4522-951D-A3790DBE70B4.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.networking.doc/GUID-55FCEC92-74B9-4E5F-ACC0-4EA1C36F397A.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	12.8 Deploy NetFlow Collection on Networking Boundary Devices Enable the collection of NetFlow and logging data on all network boundary devices.		●	●

8 Virtual Machines

This section contains recommendations for settings related to guest virtual machines.

Internal Only - General

8.1 Communication

Internal Only - General

8.1.1 (L2) Ensure only one remote console connection is permitted to a VM at any time (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

By default, remote console sessions can be connected to by more than one user at a time. Permit only one remote console connection to a VM at a time. Other attempts will be rejected until the first connection disconnects.

Rationale:

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 can connect to the console and observe the administrator's actions. Also, this could result in an administrator losing console access to a VM. For example, if a jump box is being used for an open console session, and the admin loses a connection to that box, 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:

To verify that only one remote console session is permitted at a time, confirm that `RemoteDisplay.maxConnections` is set to `1`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `RemoteDisplay.maxConnections` is set to `1`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input RemoteDisplay.maxConnections with a value of 1.
5. Click OK, then OK again.

Alternatively, run the following PowerCLI command for VMs that do not specify the setting:

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

Run the following PowerCLI command for VMs that specify the setting but have the wrong value for it:

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

References:

1. http://www.ibenit.com/post/85227299008/security-benchmark-hardening-guide-policies-and-profile
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-27A340F5-DE98-41A8-AC73-01ED4949EEF2.html
3. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-7FED3B17-E2E9-4360-AAC6-B70F9A9AEB84.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.7 Enforce Access Control to Data through Automated Tools Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.			●

Internal Only - General

8.2 Devices

Internal Only - General

8.2.1 (L1) Ensure unnecessary floppy devices are disconnected (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Ensure that no floppy device is connected to a virtual machine unless required. For a floppy device to be disconnected, the floppyX.present parameter should either not be present or have a value of FALSE.

Rationale:

Removing unnecessary hardware devices can reduce the number of potential attack channels and help prevent attacks.

Audit:

To verify floppy drives are not connected, confirm that the following parameter is either NOT present or is set to FALSE: floppyX.present

Alternately, the following PowerCLI command may be used:

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

Remediation:

To disconnect all floppy drives from VMs, run the following PowerCLI command:

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

The VM will need to be powered off for this change to take effect.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-600D24C8-0F77-4D96-B273-A30F256B29D4.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.2 (L2) Ensure unnecessary CD/DVD devices are disconnected (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Ensure that no CD/DVD device is connected to a virtual machine unless required. For a CD/DVD device to be disconnected, the ideX:Y.present parameter should either not be present or have a value of FALSE.

Rationale:

Removing unnecessary hardware devices can reduce the number of potential attack channels and help prevent attacks.

Audit:

To verify CD/DVD drives are not connected, confirm that the following parameter is either NOT present or is set to FALSE: ideX:Y.present

Alternately, the following PowerCLI command may be used:

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

Remediation:

To disconnect all CD/DVD drives from VMs, run the following PowerCLI command:

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

The VM will need to be powered off for this change to take effect.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-600D24C8-0F77-4D96-B273-A30F256B29D4.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.3 (L1) Ensure unnecessary parallel ports are disconnected (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Ensure that no parallel port is connected to a virtual machine unless required. For a parallel port to be disconnected, the parallelX.present parameter should either not be present or have a value of FALSE.

Rationale:

Removing unnecessary hardware devices can reduce the number of potential attack channels and help prevent attacks.

Audit:

To verify parallel ports are not connected, confirm that the following parameter is either NOT present or is set to FALSE: parallelX.present

Alternately, 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 disconnect all parallel ports from VMs, 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
```

The VM will need to be powered off for this change to take effect.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-600D24C8-0F77-4D96-B273-A30F256B29D4.html
2. https://blogs.vmware.com/PowerCLI/2012/05/working-with-vm-devices-in-powercli.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.4 (L1) Ensure unnecessary serial ports are disconnected (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Ensure that no serial port is connected to a virtual machine unless required. For a serial port to be disconnected, the serialX.present parameter should either not be present or have a value of FALSE.

Rationale:

Removing unnecessary hardware devices can reduce the number of potential attack channels and help prevent attacks.

Audit:

To verify serial ports are not connected, confirm that the following parameter is either NOT present or is set to FALSE: serialX.present

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 disconnect all serial ports from VMs, 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
```

The VM will need to be powered off for this change to take effect.

References:

1. https://blogs.vmware.com/PowerCLI/2012/05/working-with-vm-devices-in-powercli.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.5 (L1) Ensure unnecessary USB devices are disconnected (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Ensure that no USB device is connected to a virtual machine unless required. For a USB device to be disconnected, the usb.present parameter should either not be present or have a value of FALSE.

Rationale:

Removing unnecessary hardware devices can reduce the number of potential attack channels and help prevent attacks.

Audit:

To verify USB devices are not connected, confirm that the following parameter is either NOT present or is set to FALSE: usb.present

Alternately, the following PowerCLI command may be used:

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

Remediation:

To disconnect all USB devices from VMs, run the following PowerCLI command:

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

The VM will need to be powered off for this change to take effect.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-7FED3B17-E2E9-4360-AAC6-B70F9A9AEB84.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.6 (L1) Ensure unauthorized modification and disconnection of devices is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In a virtual machine, users and processes without root or administrator privileges can disconnect devices, such as network adapters and CD-ROM drives, and modify device settings within the guest operating system. These actions should be prevented.

Rationale:

Disabling unauthorized modification and disconnection of devices helps prevents unauthorized changes within the guest operating system, which could be used to gain unauthorized access, cause denial of service conditions, and otherwise negatively affect the security of the guest operating system.

Audit:

To verify unauthorized device modifications and disconnections are prevented, access the virtual machine configuration file and verify that `isolation.device.edit.disable` is set to `TRUE`.

Alternately, 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 prevent unauthorized device modifications and disconnections, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-F88A5FED-552B-44F9-A168-C62D9306DBD6.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.7 (L1) Ensure unauthorized connection of devices is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

In a virtual machine, users and processes without root or administrator privileges can connect devices, such as network adapters and CD-ROM drives. This should be prevented.

Rationale:

Disabling unauthorized connection of devices helps prevents unauthorized changes within the guest operating system, which could be used to gain unauthorized access, cause denial of service conditions, and otherwise negatively affect the security of the guest operating system.

Audit:

To verify unauthorized device connections are prevented, access the virtual machine configuration file and verify that `isolation.device.connectable.disable` is set to `TRUE`.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To prevent unauthorized device connections, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-F88A5FED-552B-44F9-A168-C62D9306DBD6.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.2.8 (L1) Ensure PCI and PCIe device passthrough is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Using the VMware DirectPath I/O feature to pass through a PCI or PCIe device to a virtual machine can result in a potential security vulnerability.

Rationale:

The vulnerability can be triggered by buggy or malicious code running in privileged mode in the guest OS, such as a device driver.

Audit:

The following PowerCLI command can be used:

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

Remediation:

The following PowerCLI command can be used:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "pciPassthru*.present" -value ""
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-E5CFB1FB-9216-4C1D-B49A-81AAAC414025.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.3 Guest

Internal Only - General

8.3.1 (L1) Ensure unnecessary or superfluous functions inside VMs are disabled (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Disable all system components that are not needed to support the application or service running on the VM. VMs often don't require as many functions as ordinary physical servers, so when virtualizing, you should evaluate whether a particular function is truly needed.

Rationale:

By disabling unnecessary system components, you reduce the number of potential attack vectors, which reduces the likelihood of compromise.

Audit:

To verify unneeded functions are disabled, check that the following are disabled:

1. Unused services in the operating system. For example, if the system runs a file server, Web services should not be running.
2. Unused physical devices, such as CD/DVD drives, floppy drives, and USB adaptors.
3. Screen savers.
4. X Windows if using a Linux, BSD, or Solaris guest operating system.

Remediation:

To disable unneeded functions, perform whichever of the following steps are applicable:

1. Disable unused services in the operating system.
2. Disconnect unused physical devices, such as CD/DVD drives, floppy drives, and USB adaptors.
3. Turn off any screen savers.
4. If using a Linux, BSD, or Solaris guest operating system, do not run the X Windows system unless it is necessary.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-6BFA8CA7-610F-4E6B-9FC6-D656917B7E7A.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.3.2 (L1) Ensure use of the VM console is limited (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

The VM console enables you to connect to the console of a VM, in effect seeing what a monitor on a physical server would show. The VM console also provides power management and removable device connectivity controls. Instead of the VM console, use native remote management services, such as terminal services and ssh, to interact with VMs. Grant access to the VM console only when needed, and use custom roles to provide fine-grained permissions for those people who do need access. By default, the vCenter roles "Virtual Machine Power User" and "Virtual Machine Administrator" have the "Virtual Machine.Interaction.Console Interaction" privilege.

Rationale:

The VM console could be misused to eavesdrop on VM activity, cause VM outages, and negatively affect the performance of the console, especially if many VM console sessions are open simultaneously.

Audit:

To verify use of the VM console is properly limited, perform the following steps:

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, through the vCenter `Menu` go to `Administration` then `Roles`.
4. Select the role(s) in question and edit via the pencil icon to see which effective privileges are enabled.
5. Verify that only authorized users have a role which allows them a privilege under the Virtual Machine section of the role editor.

Remediation:

To properly limit use of the VM console, perform the following steps:

1. From within vCenter select `Menu` go to `Administration` then `Roles`.
2. Create a custom role then choose the pencil icon to edit the new role.
3. Give the appropriate permissions.
4. View the usage and privileges as required.
5. Remove any default `Admin` or `Power User` roles then assign the new custom roles as needed.

Internal Only - General

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-41E5E52E-A95B-4E81-9724-6AD6800BEF78.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-3D47149A-947D-4608-88B3-E5811129EFA8.html

Additional Information:

You can set this privilege at different levels in the hierarchy. For example, if you set a privilege at the folder level, you can propagate the privilege to one or more objects within the folder. The object listed in the Required On column must have the privilege set, either directly or inherited.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.1 Maintain an Inventory of Authentication Systems Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.		●	●

Internal Only - General

8.3.3 (L1) Ensure secure protocols are used for virtual serial port access (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Serial ports are interfaces for connecting peripherals to the VM. They are often used on physical systems to provide a direct, low-level connection to the console of a server. Virtual serial ports allow VMs to communicate with serial ports over networks. If virtual serial ports are needed, they should be configured to use secure protocols.

Rationale:

If virtual serial ports do not use secure protocols, the communications with those ports could be eavesdropped on, manipulated, or otherwise compromised, giving attackers sensitive information or control to unauthorized parties.

Audit:

To verify that all virtual serial ports use secure protocols, check that all configured protocols are from this list:

- 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
- telnets - telnet over SSL over TCP

Remediation:

To configure all virtual serial ports to use secure protocols, change any protocols that are not secure to one of the following:

- 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
- telnets - telnet over SSL over TCP

References:

1. https://code.vmware.com/apis/968/vsphere
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-462B8B04-29DF-406B-9585-12D2588A6A48.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

8.3.4 (L1) Ensure standard processes are used for VM deployment (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Have a standard process for VM deployment whether this is a VMware template or another means to ensure Operating Systems have the appropriate security controls. Refer to CIS Benchmarks for information in regards to specific Operating System hardening.

Rationale:

By utilizing a standard deployment process and having hardened templates you can ensure that all your virtual machines are created with a known baseline level of security.

Audit:

Verify documentation for the method of standardization for VM deployment. If utilizing templates in VMware confirm they exist, are configured, and documented appropriately.

Remediation:

Create documentation and a standard process for the method for VM deployment. If utilizing templates in VMware create the templates, document the process for using them as well as keeping them up-to-date, then ensure the process is followed accordingly through periodic review.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.vm_admin.doc/GUID-8F7F6533-C7DB-4800-A8D2-DF7016016A80.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-3399BC47-45E8-494B-9B57-E498DD294A47.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	5.2 Maintain Secure Images Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		●	●

Internal Only - General

8.4 Monitor

Internal Only - General

8.4.1 (L1) Ensure access to VMs through the dvfilter network APIs is configured correctly (Manual)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

A VM must be configured explicitly to accept access by the dvfilter network API. Only VMs that need to be accessed by that API should be configured to accept such access.

Rationale:

An attacker might compromise a VM by making use of the dvfilter API.

Audit:

To verify this information utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `ethernet0.filter1.name = dv-filter`1 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.

   - If `dvfilter` access should not be permitted: Verify that the following is NOT listed `ethernet0.filter1.name = dv-filter`.

5. Ensure that the name of the data path kernel is set correctly.

You may also perform the following to determine if dvfilter access should be permitted via the VMX file:

1. Verify that the following is in the VMX file: `ethernet0.filter1.name = dv-filter`1 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.

   - If `dvfilter` access should not be permitted: Verify that the following is not in the VMX file: `ethernet0.filter1.name = dv-filter1`.

2. Ensure that the name of the data path kernel is set correctly.

Internal Only - General

Remediation:

To set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Remove the value from `ethernet0.filter1.name = dv-filter`.

- Parameters are removed when no value is present

5. Click `OK`.

You may also configure a VM to allow dvfilter access via the following method in the VMX file:

1. Configure the following in the 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.

- If `dvfilter` access should not be permitted: Remove the following from its VMX file: `ethernet0.filter1.name = dv-filter1`.

2. Set the name of the data path kernel correctly.

References:

1. http://kb.vmware.com/kb/1714
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

Internal Only - General

8.4.2 (L2) Ensure Autologon is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Autologon should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as autologon, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Audit:

To verify that autologon is disabled if not needed, utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.ghi.autologon.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.ghi.autologon.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

Alternatively you may run the following PowerCLI command:

Internal Only - General

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

Internal Only - General

8.4.3 (L2) Ensure BIOS BBS is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

BIOS BBS should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as BIOS BBS, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Audit:

To verify that BIOS BBS is disabled if not needed, utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.bios.bbs.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.bios.bbs.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To disable BIOS BBS, run the following PowerCLI command:

Internal Only - General

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.4 (L2) Ensure Guest Host Interaction Protocol Handler is set to disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Guest Host Interaction Protocol Handle should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as Guest Host Interaction Protocol Handle, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that Guest Host Interaction Protocol Handle is disabled if not needed, verify that `isolation.tools.ghi.protocolhandler.info.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.ghi.protocolhandler.info.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.

Internal Only - General

3. Click on EDIT CONFIGURATION.
4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.ghi.protocolhandler.info.disable with a value of TRUE.
5. Click OK, then OK again.

To disable Guest Host Interaction Protocol Handle, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.5 (L2) Ensure Unity Taskbar is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity Taskbar feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity Taskbar feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity Taskbar feature is disabled if not needed, verify that `isolation.tools.unity.taskbar.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unity.taskbar.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.unity.taskbar.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Unity Taskbar feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.6 (L2) Ensure Unity Active is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity Active feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity Active feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity Active feature is disabled if not needed verify that `isolation.tools.unityActive.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unityActive.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.unityActive.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Unity Active feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-412EF981-D4F1-430B-9D09-A4679C2D04E7.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.7 (L2) Ensure Unity Window Contents is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity Window Contents feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity Window Contents feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity Window Contents feature is disabled if not needed, verify that `isolation.tools.unity.windowContents.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unity.windowContents.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.unity.windowContents.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Unity Window Contents feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.8 (L2) Ensure Unity Push Update is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity Push Update feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity Push Update feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity Push Update feature is disabled if not needed, verify that `isolation.tools.unity.push.update.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unity.push.update.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.unity.push.update.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Unity Push Update feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.9 (L2) Ensure Drag and Drop Version Get is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Drag and Drop Version Get feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Drag and Drop Version Get feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Drag and Drop Version Get feature is disabled if not needed, verify that `isolation.tools.vmxDnDVersionGet.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.vmxDnDVersionGet.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.vmxDnDVersionGet.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the Drag and Drop Version Get feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.10 (L2) Ensure Drag and Drop Version Set is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Drag and Drop Version Set feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Drag and Drop Version Set feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Drag and Drop Version Set feature is disabled if not needed, verify that `isolation.tools.guestDnDVersionSet.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.guestDnDVersionSet.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.guestDnDVersionSet.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the Drag and Drop Version Set feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.11 (L2) Ensure Shell Action is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Shell Action feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Shell Action feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Shell Action feature is disabled if not needed, verify that `isolation.ghi.host.shellAction.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.ghi.host.shellAction.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.ghi.host.shellAction.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Shell Action feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.12 (L2) Ensure Request Disk Topology is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Request Disk Topology feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Request Disk Topology feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Request Disk Topology feature is disabled if not needed, verify that `isolation.tools.dispTopoRequest.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.dispTopoRequest.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.dispTopoRequest.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the Request Disk Topology feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.13 (L2) Ensure Trash Folder State is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Trash Folder State feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Trash Folder State feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Trash Folder State feature is disabled if not needed, verify that `isolation.tools.trashFolderState.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.trashFolderState.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.trashFolderState.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Trash Folder State feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

Additional Information:

Reference matches, but DOES NOT CONTAIN content.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.14 (L2) Ensure Guest Host Interaction Tray Icon is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Guest Host Interaction Tray Icon feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Guest Host Interaction Tray Icon feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Guest Host Interaction Tray Icon feature is disabled if not needed, verify that `isolation.tools.ghi.trayicon.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.ghi.trayicon.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.ghi.trayicon.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the Guest Host Interaction Tray Icon feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

Additional Information:

Reference matches, but DOES NOT CONTAIN content.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.15 (L2) Ensure Unity is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity feature is disabled if not needed, verify that `isolation.tools.unity.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unity.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.unity.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the Unity feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

Additional Information:

Reference matches, but DOES NOT CONTAIN content.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.16 (L2) Ensure Unity Interlock is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Unity Interlock feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Unity Interlock feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Unity Interlock feature is disabled if not needed, verify that `isolation.tools.unityInterlockOperation.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.unityInterlockOperation.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.unityInterlockOperation.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the Unity Interlock feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.17 (L2) Ensure GetCreds is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The GetCreds feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the GetCreds feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the GetCreds feature is disabled if not needed, verify that `isolation.tools.getCreds.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.getCreds.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.getCreds.disable` with a value of `TRUE`.

Internal Only - General

5. Click OK, then OK again.

To disable the GetCreds feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.18 (L2) Ensure Host Guest File System Server is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Host Guest File System Server should be disabled if it is not needed.

Rationale:

Certain automated operations such as automated tool upgrades use a component in the hypervisor called Host Guest File System (HGFS), and an attacker could potentially use this to transfer files inside the guest OS. These VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features, such as the Host Guest File System Server, are not implemented in ESXi. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

This will cause the VMX process to not respond to commands from the tools process. Setting isolation.tools.hgfsServerSet.disable to TRUE disables the 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.

Audit:

To verify that the Host Guest File System Server is disabled if not needed, verify that `isolation.tools.hgfsServerSet.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.hgfsServerSet.disable` is set to `TRUE`.

Alternately, the following PowerCLI command may be used:

Internal Only - General

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

Remediation:

To set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.hgfsServerSet.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To disable the Host Guest File System Server, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.19 (L2) Ensure Guest Host Interaction Launch Menu is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The Guest Host Interaction Launch Menu feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the Guest Host Interaction Launch Menu feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the Guest Host Interaction Launch Menu feature is disabled if not needed, verify that `isolation.tools.ghi.launchmenu.change` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.ghi.launchmenu.change` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.ghi.launchmenu.change with a value of TRUE.
5. Click OK, then OK again.

To disable the Guest Host Interaction Launch Menu feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.20 (L2) Ensure memSchedFakeSampleStats is disabled (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

The memSchedFakeSampleStats feature should be disabled if it is not needed.

Rationale:

Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features, such as the memSchedFakeSampleStats feature, reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value.

Impact:

Some automated tools and processes may cease to function.

Audit:

To verify that the memSchedFakeSampleStats feature is disabled if not needed, verify that `isolation.tools.memSchedFakeSampleStats.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.memSchedFakeSampleStats.disable` is set to `TRUE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.

Internal Only - General

3. Click on EDIT CONFIGURATION.
4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.memSchedFakeSampleStats.disable with a value of TRUE.
5. Click OK, then OK again.

To disable the memSchedFakeSampleStats feature, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-60E83710-8295-41A2-9C9D-83DEBB6872C2.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.21 (L1) Ensure VM Console Copy operations are disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

VM console copy operations should be disabled.

Rationale:

VM console copy operations are disabled by default (not explicitly specified); however, explicitly disabling this feature enables audit controls to check that this setting is correct.

Audit:

To verify that VM console copy operations are disabled, verify that the `isolation.tools.copy.disable` option is missing or set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.copy.disable` is set to `TRUE` or missing.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.copy.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To explicitly disable VM console copy operations, run the following PowerCLI command:

Internal Only - General

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

Default Value:

Disabled

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-367D02C1-B71F-4AC3-AA05-85033136A667.html
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.22 (L1) Ensure VM Console Drag and Drop operations is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

VM console drag and drop operations should be disabled.

Rationale:

VM console drag and drop operations are disabled by default (not explicitly specified); however, explicitly disabling this feature enables audit controls to check that this setting is correct.

Audit:

To verify that VM console drag and drop operations are disabled, verify that `isolation.tools.dnd.disable` is missing or set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.dnd.disable` is set to `TRUE` or missing.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.dnd.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To explicitly disable VM console drag and drop operations, run the following PowerCLI command:

Internal Only - General

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

Default Value:

Disabled

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-52188148-C579-4F6A-8335-CFBCE0DD2167.html

Additional Information:

Only reference for this element to be found was in the 5.0 documentation portal. It is not found in the 5.1 or 5.5 portal.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.23 (L1) Ensure VM Console GUI Options is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

VM console and paste GUI options should be disabled.

Rationale:

VM console and paste GUI options are disabled by default (not explicitly specified); however, explicitly disabling this feature enables audit controls to check that this setting is correct.

Audit:

To verify that VM console and paste GUI options are disabled, verify that `isolation.tools.setGUIOptions.enable` option is missing or set to `FALSE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.setGUIOptions.enable` is set to `FALSE` or missing.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.setGUIOptions.enable` with a value of `FALSE`.
5. Click `OK`, then `OK` again.

To explicitly disable VM console and paste GUI options, run the following PowerCLI command:

Internal Only - General

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

Default Value:

Disabled

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A

Additional Information:

Only reference for this element to be found was in the 5.0 documentation portal. It is not found in the 5.1 or 5.5 portal.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.4.24 (L1) Ensure VM Console Paste operations are disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

VM console paste operations should be disabled.

Rationale:

VM console paste operations are disabled by default (not explicitly specified); however, explicitly disabling this feature enables audit controls to check that this setting is correct.

Audit:

To verify that VM console paste operations are disabled, verify that `isolation.tools.paste.disable` is missing or set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.paste.disable` is set to `TRUE` or missing.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.paste.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To explicitly disable VM console paste operations, run the following PowerCLI command:

Internal Only - General

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

Default Value:

Disabled

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-367D02C1-B71F-4AC3-AA05-85033136A667.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.5 Resources

Internal Only - General

8.5.1 (L2) Ensure VM limits are configured correctly (Manual)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

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

Rationale:

Without resource management, one virtual machine could consume so much of the host's resources that other virtual machines on the same host could not perform their intended functions.

Audit:

To verify VM limits are configured correctly, confirm that limits with reservations, shares, and/or resource pools are in place to guarantee resources to critical VMs and to constrain resource consumption by VMs 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.

The following PowerCLI command may be used to list resource configurations:

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

Remediation:

To configure VM limits correctly, do all of the following that are applicable:

1. Use shares or reservations to guarantee resources to critical VMs.
2. Use limits to constrain resource consumption by VMs 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.
3. Use resource pools to guarantee resources to a common group of critical VMs.

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-E6262360-9300-4E10-ADE0-D4BED08DB5CA.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

8.5.2 (L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False" (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Due to performance reasons, modern graphic rendering is done within a dedicated graphic processing unit (GPU). Virtual machines can use the host-based GPU for such operations as well. Such dedicated hardware is typically accessed by using complex APIs like OpenGL and DirectX. This hardware-based 3D acceleration should be disabled if it is not needed.

Rationale:

Security flaws within APIs can lead to serious security breaches like memory corruption, denial of service, and remote code execution.

Audit:

To verify that hardware-based 3D acceleration is disabled, verify that `mks.enable3d` is set to `FALSE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `mks.enable3d` is set to `FALSE`.

Alternately, the following PowerCLI command may be used:

```
# List the VMs and their current settings
Get-VM | Get-AdvancedSetting -Name "mks.enable3d"| Select Entity, Name, Value
```

Remediation:

To set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `mks.enable3d` with a value of `FALSE`.
5. Click `OK`, then `OK` again.

To disable hardware-based 3D acceleration, run the following PowerCLI command:

Internal Only - General

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "mks.enable3d" -value $false
```

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-15D965F3-05E3-4E59-9F08-B305FDE672DD.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Internal Only - General

8.6 Storage

Internal Only - General

8.6.1 (L2) Ensure nonpersistent disks are limited (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

By default, VM disks use dependent mode, which means they are affected by snapshots. To avoid this, VM disks can use independent mode instead. Independent mode can be configured as persistent (data is written permanently to the disk) or nonpersistent (all changes made to disk are lost when the system is rebooted). Use of nonpersistent mode should be avoided unless the data is not needed (e.g., already duplicated elsewhere).

Rationale:

From a security standpoint, nonpersistent mode allows successful attackers to remove evidence of their actions or even their presence within a VM by performing a simple shutdown or reboot.

Audit:

To verify nonpersistent mode use is limited, review VM disk types to confirm that nonpersistent mode is only used when the loss of all stored data is not a concern. For all disks where nonpersistent mode is not to be used, scsiX:Y.mode should either be absent or be set to a value other than independent nonpersistent.

Alternately, the following PowerCLI command may be used to review the disk types:

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

Remediation:

To limit the use of nonpersistent mode, run the following PowerCLI command:

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

References:

1. https://code.vmware.com/apis/196/vsphere/doc/vim.vm.device.VirtualDiskOption.DiskMode.html

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.4 Enforce Data Retention Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	●	●	●
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

8.6.2 (L1) Ensure virtual disk shrinking is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

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.

Impact:

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

Audit:

Verify that `isolation.tools.diskShrink.disable` is set to `TRUE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

4. Click on ADD CONFIGURATION PARAMS then input isolation.tools.diskShrink.disable with a value of TRUE.
5. Click OK, then OK again.

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
```

Default Value:

The prescribed state is not the default state.

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8AEAwgPYB2AzhgCYJphYall4BmRahpzGA5uhidzwA1ALIB3MGgR4AKkSIQyIAL5A
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9610FE65-3A78-4982-8C28-5B34FEB264B6.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

8.6.3 (L1) Ensure virtual disk wiping is disabled (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

Wiping a virtual disk reclaims all 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. If virtual disk wiping is done repeatedly, it can cause the virtual disk to become unavailable while wiping occurs. In most datacenter environments, disk wiping is not needed, but normal users and processes--without administrative privileges--can issue disk wipes unless the feature is disabled.

Rationale:

Virtual disk wiping can effectively cause a denial of service.

Audit:

To verify that virtual disk wiping is disabled, verify that `isolation.tools.diskWiper.disable` is set to TRUE.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `isolation.tools.diskWiper.disable` is set to `TRUE`.

Alternately, the following PowerCLI command may be used:

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

Remediation:

To set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `isolation.tools.diskWiper.disable` with a value of `TRUE`.
5. Click `OK`, then `OK` again.

To disable virtual disk wiping, run the following PowerCLI command:

Internal Only - General

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-9610FE65-3A78-4982-8C28-5B34FEB264B6.html
2. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	9.1 Associate Active Ports, Services and Protocols to Asset Inventory Associate active ports, services and protocols to the hardware assets in the asset inventory.		●	●

Internal Only - General

8.7 Tools

Internal Only - General

8.7.1 (L1) Ensure the number of VM log files is configured properly (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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 MB. 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.

Rationale:

Log files should be rotated to preserve log data in case of corruption or destruction of the current log file, and to avoid the likelihood of logging issues caused by an overly large log file.

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.

Audit:

To verify that log files will be created more frequently, verify that `log.keepOld` is set to `10`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `log.keepOld` is set to `10`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.

Internal Only - General

2. Click on the VM Options tab then expand Advanced.
3. Click on EDIT CONFIGURATION.
4. Click on ADD CONFIGURATION PARAMS then input log.keepOld with a value of 10.
5. Click OK, then OK again.

To set the number of log files to be used to 10, run the following PowerCLI command:

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

References:

1. https://docs.vmware.com/en/VMware-Tools/10.3.0/com.vmware.vsphere.vmwaretools.doc/GUID-685722FA-9009-439C-9142-18A9E7C592EA.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

Internal Only - General

8.7.2 (L2) Ensure host information is not sent to guests (Automated)

Profile Applicability:

- Level 2 (L2) - High Security/Sensitive Data Environment (limited functionality)

Description:

Configure VMware Tools to disable host information from being sent to guests unless a particular VM requires this information for performance monitoring purposes.

Rationale:

By enabling a VM to get detailed information about the physical host, an adversary could potentially use this information to inform further attacks on the host.

Audit:

To verify host information is not sent to guests, verify that `tools.guestlib.enableHostInfo` is set to `FALSE`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `tools.guestlib.enableHostInfo` is set to `FALSE`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Click on `ADD CONFIGURATION PARAMS` then input `tools.guestlib.enableHostInfo` with a value of `FALSE`.
5. Click `OK`, then `OK` again.

To prevent host information from being sent to guests, run the following PowerCLI command:

Internal Only - General

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

Default Value:

FALSE

References:

1. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.security.doc/GUID-2CF880DA-2435-4201-9AFB-A16A11951A2D.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

Internal Only - General

8.7.3 (L1) Ensure VM log file size is limited (Automated)

Profile Applicability:

- Level 1 (L1) - Corporate/Enterprise Environment (general use)

Description:

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 MB. If the maximum number of log files already exists, when a new one is created, the oldest log file is deleted.

Rationale:

Virtual machine users and processes can abuse logging either on purpose or inadvertently so that large amounts of data flood the log file. Without restrictions on maximum log file size, over time a log file can consume enough file system space to cause a denial of service.

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.

Audit:

To verify the maximum log file size is limited properly, verify that `log.rotateSize` is set to `1024000`.

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.
3. Click on `EDIT CONFIGURATION`.
4. Verify that `log.rotateSize` is set to `1024000`.

Alternately, 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 set this configuration utilize the vSphere interface as follows:

1. Select the VM then select `Actions` followed by `Edit Settings`.
2. Click on the `VM Options` tab then expand `Advanced`.

Internal Only - General

3. Click on EDIT CONFIGURATION.
4. Click on ADD CONFIGURATION PARAMS then input log.rotateSize with a value of 1024000.
5. Click OK, then OK again.

To properly limit the maximum log file size, run the following PowerCLI command:

```
# Add the setting to all VMs
Get-VM | New-AdvancedSetting -Name "log.rotateSize" -value "1024000"
```

References:

1. http://kb.vmware.com/kb/8182749
2. https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-2DD66869-52C7-42C5-8F5B-145EBD26BBA1.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

Internal Only - General

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Install**		
1.1	(L1) Ensure ESXi is properly patched (Manual)	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly (Automated)	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host (Manual)	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured (Automated)	☐	☐
2	**Communication**		
2.1	(L1) Ensure NTP time synchronization is configured properly (Automated)	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host (Manual)	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled (Automated)	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used (Manual)	☐	☐
2.5	(L1) Ensure SNMP is configured properly (Manual)	☐	☐
2.6	(L1) Ensure dvfilter API is not configured if not used (Manual)	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server (Manual)	☐	☐
2.8	(L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory (Manual)	☐	☐
2.9	(L2) Ensure VDS health check is disabled (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3	**Logging**		
3.1	(L1) Ensure a centralized location is configured to collect ESXi host core dumps (Automated)	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts (Manual)	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts (Automated)	☐	☐
4	**Access**		
4.1	(L1) Ensure a non-root user account exists for local admin access (Automated)	☐	☐
4.2	(L1) Ensure passwords are required to be complex (Manual)	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5 (Automated)	☐	☐
4.4	(L1) Ensure account lockout is set to 15 minutes (Automated)	☐	☐
4.5	(L1) Ensure previous 5 passwords are prohibited (Manual)	☐	☐
4.6	(L1) Ensure Active Directory is used for local user authentication (Manual)	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group (Manual)	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured (Manual)	☐	☐
5	**Console**		
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2	(L1) Ensure the ESXi shell is disabled (Automated)	☐	☐
5.3	(L1) Ensure SSH is disabled (Automated)	☐	☐
5.4	(L1) Ensure CIM access is limited (Manual)	☐	☐
5.5	(L1) Ensure Normal Lockdown mode is enabled (Automated)	☐	☐
5.6	(L2) Ensure Strict Lockdown mode is enabled (Automated)	☐	☐
5.7	(L2) Ensure the SSH authorized_keys file is empty (Manual)	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less (Automated)	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less (Automated)	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode (Manual)	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified (Manual)	☐	☐
6	**Storage**		
6.1	(L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled (Automated)	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic (Manual)	☐	☐
6.3	(L1) Ensure storage area network (SAN) resources are segregated properly (Manual)	☐	☐
7	**vNetwork**		
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject (Automated)	☐	☐
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject (Automated)	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN (Automated)	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches (Manual)	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT) (Automated)	☐	☐
7.7	(L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector (Manual)	☐	☐
8	**Virtual Machines**		
8.1	**Communication**		
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time (Automated)	☐	☐
8.2	**Devices**		
8.2.1	(L1) Ensure unnecessary floppy devices are disconnected (Automated)	☐	☐
8.2.2	(L2) Ensure unnecessary CD/DVD devices are disconnected (Automated)	☐	☐
8.2.3	(L1) Ensure unnecessary parallel ports are disconnected (Automated)	☐	☐
8.2.4	(L1) Ensure unnecessary serial ports are disconnected (Automated)	☐	☐
8.2.5	(L1) Ensure unnecessary USB devices are disconnected (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.2.6	(L1) Ensure unauthorized modification and disconnection of devices is disabled (Automated)	☐	☐
8.2.7	(L1) Ensure unauthorized connection of devices is disabled (Automated)	☐	☐
8.2.8	(L1) Ensure PCI and PCIe device passthrough is disabled (Automated)	☐	☐
8.3	**Guest**		
8.3.1	(L1) Ensure unnecessary or superfluous functions inside VMs are disabled (Manual)	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited (Manual)	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access (Manual)	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment (Manual)	☐	☐
8.4	**Monitor**		
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly (Manual)	☐	☐
8.4.2	(L2) Ensure Autologon is disabled (Automated)	☐	☐
8.4.3	(L2) Ensure BIOS BBS is disabled (Automated)	☐	☐
8.4.4	(L2) Ensure Guest Host Interaction Protocol Handler is set to disabled (Automated)	☐	☐
8.4.5	(L2) Ensure Unity Taskbar is disabled (Automated)	☐	☐
8.4.6	(L2) Ensure Unity Active is disabled (Automated)	☐	☐
8.4.7	(L2) Ensure Unity Window Contents is disabled (Automated)	☐	☐
8.4.8	(L2) Ensure Unity Push Update is disabled (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.4.9	(L2) Ensure Drag and Drop Version Get is disabled (Automated)	☐	☐
8.4.10	(L2) Ensure Drag and Drop Version Set is disabled (Automated)	☐	☐
8.4.11	(L2) Ensure Shell Action is disabled (Automated)	☐	☐
8.4.12	(L2) Ensure Request Disk Topology is disabled (Automated)	☐	☐
8.4.13	(L2) Ensure Trash Folder State is disabled (Automated)	☐	☐
8.4.14	(L2) Ensure Guest Host Interaction Tray Icon is disabled (Automated)	☐	☐
8.4.15	(L2) Ensure Unity is disabled (Automated)	☐	☐
8.4.16	(L2) Ensure Unity Interlock is disabled (Automated)	☐	☐
8.4.17	(L2) Ensure GetCreds is disabled (Automated)	☐	☐
8.4.18	(L2) Ensure Host Guest File System Server is disabled (Automated)	☐	☐
8.4.19	(L2) Ensure Guest Host Interaction Launch Menu is disabled (Automated)	☐	☐
8.4.20	(L2) Ensure memSchedFakeSampleStats is disabled (Automated)	☐	☐
8.4.21	(L1) Ensure VM Console Copy operations are disabled (Automated)	☐	☐
8.4.22	(L1) Ensure VM Console Drag and Drop operations is disabled (Automated)	☐	☐
8.4.23	(L1) Ensure VM Console GUI Options is disabled (Automated)	☐	☐
8.4.24	(L1) Ensure VM Console Paste operations are disabled (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.5	**Resources**		
8.5.1	(L2) Ensure VM limits are configured correctly (Manual)	☐	☐
8.5.2	(L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False" (Automated)	☐	☐
8.6	**Storage**		
8.6.1	(L2) Ensure nonpersistent disks are limited (Automated)	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled (Automated)	☐	☐
8.6.3	(L1) Ensure virtual disk wiping is disabled (Automated)	☐	☐
8.7	**Tools**		
8.7.1	(L1) Ensure the number of VM log files is configured properly (Automated)	☐	☐
8.7.2	(L2) Ensure host information is not sent to guests (Automated)	☐	☐
8.7.3	(L1) Ensure VM log file size is limited (Automated)	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐
5.4	(L1) Ensure CIM access is limited	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.1	(L1) Ensure NTP time synchronization is configured properly	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.5	(L1) Ensure SNMP is configured properly	☐	☐
2.6	(L1) Ensure dvfilter API is not configured if not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
2.8	(L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory	☐	☐
2.9	(L2) Ensure VDS health check is disabled	☐	☐
3.1	(L1) Ensure a centralized location is configured to collect ESXi host core dumps	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.2	(L1) Ensure passwords are required to be complex	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐
4.5	(L1) Ensure previous 5 passwords are prohibited	☐	☐
4.6	(L1) Ensure Active Directory is used for local user authentication	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐
5.2	(L1) Ensure the ESXi shell is disabled	☐	☐
5.3	(L1) Ensure SSH is disabled	☐	☐
5.4	(L1) Ensure CIM access is limited	☐	☐
5.5	(L1) Ensure Normal Lockdown mode is enabled	☐	☐
5.6	(L2) Ensure Strict Lockdown mode is enabled	☐	☐
5.7	(L2) Ensure the SSH authorized_keys file is empty	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
6.1	(L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic	☐	☐
6.3	(L1) Ensure storage area network (SAN) resources are segregated properly	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
7.7	(L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector	☐	☐
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time	☐	☐
8.2.1	(L1) Ensure unnecessary floppy devices are disconnected	☐	☐
8.2.2	(L2) Ensure unnecessary CD/DVD devices are disconnected	☐	☐
8.2.3	(L1) Ensure unnecessary parallel ports are disconnected	☐	☐
8.2.4	(L1) Ensure unnecessary serial ports are disconnected	☐	☐
8.2.5	(L1) Ensure unnecessary USB devices are disconnected	☐	☐
8.2.6	(L1) Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
8.2.7	(L1) Ensure unauthorized connection of devices is disabled	☐	☐
8.2.8	(L1) Ensure PCI and PCIe device passthrough is disabled	☐	☐
8.3.1	(L1) Ensure unnecessary or superfluous functions inside VMs are disabled	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.4.2	(L2) Ensure Autologon is disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.4.3	(L2) Ensure BIOS BBS is disabled	☐	☐
8.4.4	(L2) Ensure Guest Host Interaction Protocol Handler is set to disabled	☐	☐
8.4.5	(L2) Ensure Unity Taskbar is disabled	☐	☐
8.4.6	(L2) Ensure Unity Active is disabled	☐	☐
8.4.7	(L2) Ensure Unity Window Contents is disabled	☐	☐
8.4.8	(L2) Ensure Unity Push Update is disabled	☐	☐
8.4.9	(L2) Ensure Drag and Drop Version Get is disabled	☐	☐
8.4.10	(L2) Ensure Drag and Drop Version Set is disabled	☐	☐
8.4.11	(L2) Ensure Shell Action is disabled	☐	☐
8.4.12	(L2) Ensure Request Disk Topology is disabled	☐	☐
8.4.13	(L2) Ensure Trash Folder State is disabled	☐	☐
8.4.14	(L2) Ensure Guest Host Interaction Tray Icon is disabled	☐	☐
8.4.15	(L2) Ensure Unity is disabled	☐	☐
8.4.16	(L2) Ensure Unity Interlock is disabled	☐	☐
8.4.17	(L2) Ensure GetCreds is disabled	☐	☐
8.4.18	(L2) Ensure Host Guest File System Server is disabled	☐	☐
8.4.19	(L2) Ensure Guest Host Interaction Launch Menu is disabled	☐	☐
8.4.20	(L2) Ensure memSchedFakeSampleStats is disabled	☐	☐
8.4.21	(L1) Ensure VM Console Copy operations are disabled	☐	☐
8.4.22	(L1) Ensure VM Console Drag and Drop operations is disabled	☐	☐
8.4.23	(L1) Ensure VM Console GUI Options is disabled	☐	☐
8.4.24	(L1) Ensure VM Console Paste operations are disabled	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.5.2	(L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False"	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐
8.6.3	(L1) Ensure virtual disk wiping is disabled	☐	☐
8.7.1	(L1) Ensure the number of VM log files is configured properly	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.7.3	(L1) Ensure VM log file size is limited	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.1	(L1) Ensure NTP time synchronization is configured properly	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.5	(L1) Ensure SNMP is configured properly	☐	☐
2.6	(L1) Ensure dvfilter API is not configured if not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
2.8	(L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory	☐	☐
2.9	(L2) Ensure VDS health check is disabled	☐	☐
3.1	(L1) Ensure a centralized location is configured to collect ESXi host core dumps	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.2	(L1) Ensure passwords are required to be complex	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐
4.5	(L1) Ensure previous 5 passwords are prohibited	☐	☐
4.6	(L1) Ensure Active Directory is used for local user authentication	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐
5.2	(L1) Ensure the ESXi shell is disabled	☐	☐
5.3	(L1) Ensure SSH is disabled	☐	☐
5.4	(L1) Ensure CIM access is limited	☐	☐
5.5	(L1) Ensure Normal Lockdown mode is enabled	☐	☐
5.6	(L2) Ensure Strict Lockdown mode is enabled	☐	☐
5.7	(L2) Ensure the SSH authorized_keys file is empty	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
6.1	(L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic	☐	☐
6.3	(L1) Ensure storage area network (SAN) resources are segregated properly	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
7.7	(L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector	☐	☐
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time	☐	☐
8.2.1	(L1) Ensure unnecessary floppy devices are disconnected	☐	☐
8.2.2	(L2) Ensure unnecessary CD/DVD devices are disconnected	☐	☐
8.2.3	(L1) Ensure unnecessary parallel ports are disconnected	☐	☐
8.2.4	(L1) Ensure unnecessary serial ports are disconnected	☐	☐
8.2.5	(L1) Ensure unnecessary USB devices are disconnected	☐	☐
8.2.6	(L1) Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
8.2.7	(L1) Ensure unauthorized connection of devices is disabled	☐	☐
8.2.8	(L1) Ensure PCI and PCIe device passthrough is disabled	☐	☐
8.3.1	(L1) Ensure unnecessary or superfluous functions inside VMs are disabled	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.4.2	(L2) Ensure Autologon is disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.4.3	(L2) Ensure BIOS BBS is disabled	☐	☐
8.4.4	(L2) Ensure Guest Host Interaction Protocol Handler is set to disabled	☐	☐
8.4.5	(L2) Ensure Unity Taskbar is disabled	☐	☐
8.4.6	(L2) Ensure Unity Active is disabled	☐	☐
8.4.7	(L2) Ensure Unity Window Contents is disabled	☐	☐
8.4.8	(L2) Ensure Unity Push Update is disabled	☐	☐
8.4.9	(L2) Ensure Drag and Drop Version Get is disabled	☐	☐
8.4.10	(L2) Ensure Drag and Drop Version Set is disabled	☐	☐
8.4.11	(L2) Ensure Shell Action is disabled	☐	☐
8.4.12	(L2) Ensure Request Disk Topology is disabled	☐	☐
8.4.13	(L2) Ensure Trash Folder State is disabled	☐	☐
8.4.14	(L2) Ensure Guest Host Interaction Tray Icon is disabled	☐	☐
8.4.15	(L2) Ensure Unity is disabled	☐	☐
8.4.16	(L2) Ensure Unity Interlock is disabled	☐	☐
8.4.17	(L2) Ensure GetCreds is disabled	☐	☐
8.4.18	(L2) Ensure Host Guest File System Server is disabled	☐	☐
8.4.19	(L2) Ensure Guest Host Interaction Launch Menu is disabled	☐	☐
8.4.20	(L2) Ensure memSchedFakeSampleStats is disabled	☐	☐
8.4.21	(L1) Ensure VM Console Copy operations are disabled	☐	☐
8.4.22	(L1) Ensure VM Console Drag and Drop operations is disabled	☐	☐
8.4.23	(L1) Ensure VM Console GUI Options is disabled	☐	☐
8.4.24	(L1) Ensure VM Console Paste operations are disabled	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.5.2	(L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False"	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐
8.6.3	(L1) Ensure virtual disk wiping is disabled	☐	☐
8.7.1	(L1) Ensure the number of VM log files is configured properly	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.7.2	(L2) Ensure host information is not sent to guests	☐	☐
8.7.3	(L1) Ensure VM log file size is limited	☐	☐

Internal Only - General

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.2	(L1) Ensure passwords are required to be complex	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5	☐	☐
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐
4.5	(L1) Ensure previous 5 passwords are prohibited	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.4.2	(L2) Ensure Autologon is disabled	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.6.3	(L1) Ensure virtual disk wiping is disabled	☐	☐
8.7.1	(L1) Ensure the number of VM log files is configured properly	☐	☐
8.7.2	(L2) Ensure host information is not sent to guests	☐	☐
8.7.3	(L1) Ensure VM log file size is limited	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.1	(L1) Ensure NTP time synchronization is configured properly	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.5	(L1) Ensure SNMP is configured properly	☐	☐
2.6	(L1) Ensure dvfilter API is not configured if not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
2.8	(L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory	☐	☐
3.1	(L1) Ensure a centralized location is configured to collect ESXi host core dumps	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.2	(L1) Ensure passwords are required to be complex	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5	☐	☐
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
4.5	(L1) Ensure previous 5 passwords are prohibited	☐	☐
4.6	(L1) Ensure Active Directory is used for local user authentication	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐
5.2	(L1) Ensure the ESXi shell is disabled	☐	☐
5.3	(L1) Ensure SSH is disabled	☐	☐
5.4	(L1) Ensure CIM access is limited	☐	☐
5.5	(L1) Ensure Normal Lockdown mode is enabled	☐	☐
5.6	(L2) Ensure Strict Lockdown mode is enabled	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
6.1	(L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic	☐	☐
6.3	(L1) Ensure storage area network (SAN) resources are segregated properly	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
7.7	(L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector	☐	☐
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time	☐	☐
8.2.1	(L1) Ensure unnecessary floppy devices are disconnected	☐	☐
8.2.2	(L2) Ensure unnecessary CD/DVD devices are disconnected	☐	☐
8.2.3	(L1) Ensure unnecessary parallel ports are disconnected	☐	☐
8.2.4	(L1) Ensure unnecessary serial ports are disconnected	☐	☐
8.2.5	(L1) Ensure unnecessary USB devices are disconnected	☐	☐
8.2.6	(L1) Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
8.2.7	(L1) Ensure unauthorized connection of devices is disabled	☐	☐
8.2.8	(L1) Ensure PCI and PCIe device passthrough is disabled	☐	☐
8.3.1	(L1) Ensure unnecessary or superfluous functions inside VMs are disabled	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.4.2	(L2) Ensure Autologon is disabled	☐	☐
8.4.3	(L2) Ensure BIOS BBS is disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.4.4	(L2) Ensure Guest Host Interaction Protocol Handler is set to disabled	☐	☐
8.4.5	(L2) Ensure Unity Taskbar is disabled	☐	☐
8.4.6	(L2) Ensure Unity Active is disabled	☐	☐
8.4.7	(L2) Ensure Unity Window Contents is disabled	☐	☐
8.4.8	(L2) Ensure Unity Push Update is disabled	☐	☐
8.4.9	(L2) Ensure Drag and Drop Version Get is disabled	☐	☐
8.4.10	(L2) Ensure Drag and Drop Version Set is disabled	☐	☐
8.4.11	(L2) Ensure Shell Action is disabled	☐	☐
8.4.12	(L2) Ensure Request Disk Topology is disabled	☐	☐
8.4.13	(L2) Ensure Trash Folder State is disabled	☐	☐
8.4.14	(L2) Ensure Guest Host Interaction Tray Icon is disabled	☐	☐
8.4.15	(L2) Ensure Unity is disabled	☐	☐
8.4.16	(L2) Ensure Unity Interlock is disabled	☐	☐
8.4.17	(L2) Ensure GetCreds is disabled	☐	☐
8.4.18	(L2) Ensure Host Guest File System Server is disabled	☐	☐
8.4.19	(L2) Ensure Guest Host Interaction Launch Menu is disabled	☐	☐
8.4.20	(L2) Ensure memSchedFakeSampleStats is disabled	☐	☐
8.4.21	(L1) Ensure VM Console Copy operations are disabled	☐	☐
8.4.22	(L1) Ensure VM Console Drag and Drop operations is disabled	☐	☐
8.4.23	(L1) Ensure VM Console GUI Options is disabled	☐	☐
8.4.24	(L1) Ensure VM Console Paste operations are disabled	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.5.2	(L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False"	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐
8.6.3	(L1) Ensure virtual disk wiping is disabled	☐	☐
8.7.1	(L1) Ensure the number of VM log files is configured properly	☐	☐
8.7.2	(L2) Ensure host information is not sent to guests	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.7.3	(L1) Ensure VM log file size is limited	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	(L1) Ensure ESXi is properly patched	☐	☐
1.2	(L1) Ensure the Image Profile VIB acceptance level is configured properly	☐	☐
1.3	(L1) Ensure no unauthorized kernel modules are loaded on the host	☐	☐
1.4	(L2) Ensure the default value of individual salt per vm is configured	☐	☐
2.1	(L1) Ensure NTP time synchronization is configured properly	☐	☐
2.2	(L1) Ensure the ESXi host firewall is configured to restrict access to services running on the host	☐	☐
2.3	(L1) Ensure Managed Object Browser (MOB) is disabled	☐	☐
2.4	(L2) Ensure default self-signed certificate for ESXi communication is not used	☐	☐
2.5	(L1) Ensure SNMP is configured properly	☐	☐
2.6	(L1) Ensure dvfilter API is not configured if not used	☐	☐
2.7	(L1) Ensure expired and revoked SSL certificates are removed from the ESXi server	☐	☐
2.8	(L1) Ensure vSphere Authentication Proxy is used when adding hosts to Active Directory	☐	☐
2.9	(L2) Ensure VDS health check is disabled	☐	☐
3.1	(L1) Ensure a centralized location is configured to collect ESXi host core dumps	☐	☐
3.2	(L1) Ensure persistent logging is configured for all ESXi hosts	☐	☐
3.3	(L1) Ensure remote logging is configured for ESXi hosts	☐	☐
4.1	(L1) Ensure a non-root user account exists for local admin access	☐	☐
4.2	(L1) Ensure passwords are required to be complex	☐	☐
4.3	(L1) Ensure the maximum failed login attempts is set to 5	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
4.4	(L1) Ensure account lockout is set to 15 minutes	☐	☐
4.5	(L1) Ensure previous 5 passwords are prohibited	☐	☐
4.6	(L1) Ensure Active Directory is used for local user authentication	☐	☐
4.7	(L1) Ensure only authorized users and groups belong to the esxAdminsGroup group	☐	☐
4.8	(L1) Ensure the Exception Users list is properly configured	☐	☐
5.1	(L1) Ensure the DCUI timeout is set to 600 seconds or less	☐	☐
5.2	(L1) Ensure the ESXi shell is disabled	☐	☐
5.3	(L1) Ensure SSH is disabled	☐	☐
5.4	(L1) Ensure CIM access is limited	☐	☐
5.5	(L1) Ensure Normal Lockdown mode is enabled	☐	☐
5.6	(L2) Ensure Strict Lockdown mode is enabled	☐	☐
5.7	(L2) Ensure the SSH authorized_keys file is empty	☐	☐
5.8	(L1) Ensure idle ESXi shell and SSH sessions time out after 300 seconds or less	☐	☐
5.9	(L1) Ensure the shell services timeout is set to 1 hour or less	☐	☐
5.10	(L1) Ensure DCUI has a trusted users list for lockdown mode	☐	☐
5.11	(L2) Ensure contents of exposed configuration files have not been modified	☐	☐
6.1	(L1) Ensure bidirectional CHAP authentication for iSCSI traffic is enabled	☐	☐
6.2	(L2) Ensure the uniqueness of CHAP authentication secrets for iSCSI traffic	☐	☐
6.3	(L1) Ensure storage area network (SAN) resources are segregated properly	☐	☐
7.1	(L1) Ensure the vSwitch Forged Transmits policy is set to reject	☐	☐
7.2	(L1) Ensure the vSwitch MAC Address Change policy is set to reject	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.3	(L1) Ensure the vSwitch Promiscuous Mode policy is set to reject	☐	☐
7.4	(L1) Ensure port groups are not configured to the value of the native VLAN	☐	☐
7.5	(L1) Ensure port groups are not configured to VLAN values reserved by upstream physical switches	☐	☐
7.6	(L1) Ensure port groups are not configured to VLAN 4095 and 0 except for Virtual Guest Tagging (VGT)	☐	☐
7.7	(L1) Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector	☐	☐
8.1.1	(L2) Ensure only one remote console connection is permitted to a VM at any time	☐	☐
8.2.1	(L1) Ensure unnecessary floppy devices are disconnected	☐	☐
8.2.2	(L2) Ensure unnecessary CD/DVD devices are disconnected	☐	☐
8.2.3	(L1) Ensure unnecessary parallel ports are disconnected	☐	☐
8.2.4	(L1) Ensure unnecessary serial ports are disconnected	☐	☐
8.2.5	(L1) Ensure unnecessary USB devices are disconnected	☐	☐
8.2.6	(L1) Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
8.2.7	(L1) Ensure unauthorized connection of devices is disabled	☐	☐
8.2.8	(L1) Ensure PCI and PCIe device passthrough is disabled	☐	☐
8.3.1	(L1) Ensure unnecessary or superfluous functions inside VMs are disabled	☐	☐
8.3.2	(L1) Ensure use of the VM console is limited	☐	☐
8.3.3	(L1) Ensure secure protocols are used for virtual serial port access	☐	☐
8.3.4	(L1) Ensure standard processes are used for VM deployment	☐	☐
8.4.1	(L1) Ensure access to VMs through the dvfilter network APIs is configured correctly	☐	☐
8.4.2	(L2) Ensure Autologon is disabled	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.4.3	(L2) Ensure BIOS BBS is disabled	☐	☐
8.4.4	(L2) Ensure Guest Host Interaction Protocol Handler is set to disabled	☐	☐
8.4.5	(L2) Ensure Unity Taskbar is disabled	☐	☐
8.4.6	(L2) Ensure Unity Active is disabled	☐	☐
8.4.7	(L2) Ensure Unity Window Contents is disabled	☐	☐
8.4.8	(L2) Ensure Unity Push Update is disabled	☐	☐
8.4.9	(L2) Ensure Drag and Drop Version Get is disabled	☐	☐
8.4.10	(L2) Ensure Drag and Drop Version Set is disabled	☐	☐
8.4.11	(L2) Ensure Shell Action is disabled	☐	☐
8.4.12	(L2) Ensure Request Disk Topology is disabled	☐	☐
8.4.13	(L2) Ensure Trash Folder State is disabled	☐	☐
8.4.14	(L2) Ensure Guest Host Interaction Tray Icon is disabled	☐	☐
8.4.15	(L2) Ensure Unity is disabled	☐	☐
8.4.16	(L2) Ensure Unity Interlock is disabled	☐	☐
8.4.17	(L2) Ensure GetCreds is disabled	☐	☐
8.4.18	(L2) Ensure Host Guest File System Server is disabled	☐	☐
8.4.19	(L2) Ensure Guest Host Interaction Launch Menu is disabled	☐	☐
8.4.20	(L2) Ensure memSchedFakeSampleStats is disabled	☐	☐
8.4.21	(L1) Ensure VM Console Copy operations are disabled	☐	☐
8.4.22	(L1) Ensure VM Console Drag and Drop operations is disabled	☐	☐
8.4.23	(L1) Ensure VM Console GUI Options is disabled	☐	☐
8.4.24	(L1) Ensure VM Console Paste operations are disabled	☐	☐
8.5.1	(L2) Ensure VM limits are configured correctly	☐	☐
8.5.2	(L2) Ensure hardware-based 3D acceleration is disabled and mks.enable3d is set to "False"	☐	☐
8.6.1	(L2) Ensure nonpersistent disks are limited	☐	☐
8.6.2	(L1) Ensure virtual disk shrinking is disabled	☐	☐
8.6.3	(L1) Ensure virtual disk wiping is disabled	☐	☐
8.7.1	(L1) Ensure the number of VM log files is configured properly	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.7.2	(L2) Ensure host information is not sent to guests	☐	☐
8.7.3	(L1) Ensure VM log file size is limited	☐	☐

Internal Only - General

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Internal Only - General

Appendix: Change History

Date	Version	Changes for this version
8/31/2026	1.6.0	Added support for the latest ESXi Version 7 Update 3w
8/31/2026	1.6.0	Add recommendation URLs.
8/31/2026	1.6.0	Added comments to harden AD appropriately Ticket #28446
8/31/2026	1.6.0	Updated recommendation 5.9 setting 0 to “fail” Ticket # 25830
5/14/2025	1.5.0	All Recommendations validated against ESXi v7.0 update 3v.
5/5/2025	1.5.0	Ticket # 24665 Updated URL references
5/4/2025	1.5.0	Ticket # 24666 Updated URL references
4/23/2024	1.4.0	All Recommendations validated against ESXi v7.0 update 3q.
4/2/2024	1.4.0	Ticket # 20552 Edited recommendation 8.6.1
4/2/2024	1.4.0	Ticket # 20520 Edited recommendation 7.1
8/30/2023	1.3.0	All Recommendations validated against ESXi v7.0 update 3n.
8/29/2023	1.3.0	Updated PowerShell scripts

Internal Only - General

Internal Only - General