CIS VMware ESXi 8.0 Benchmark

v1.4.0 - 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 *7*

Important Usage Information **7**

Key Stakeholders **7**

Apply the Correct Version of a Benchmark **8**

Exceptions **8**

Remediation **9**

Summary **9**

Target Technology Details **10**

Intended Audience **10**

Consensus Guidance **11**

Typographical Conventions **12**

Recommendation Definitions *13*

Title **13**

Assessment Status **13**

Automated **13**

Manual **13**

Profile **13**

Description **13**

Rationale Statement **13**

Impact Statement **14**

Audit Procedure **14**

Remediation Procedure **14**

Default Value **14**

References **14**

CIS Critical Security Controls® (CIS Controls®) **14**

Additional Information **14**

Profile Definitions **15**

Acknowledgements ..... Error! Bookmark not defined.

Recommendations *17*

1 Hardware **17**

1.1 Host hardware must have auditable, authentic, and up to date system & device firmware (Manual) 18

1.2 Host hardware must enable UEFI Secure Boot (Manual) 21

1.3 Host hardware must enable Intel TXT, if available (Manual) 23

Internal Only - General

1.4 Host hardware must enable and configure a TPM 2.0 (Manual) 25
1.5 Host integrated hardware management controller must be secure (Manual) 27
1.6 Host integrated hardware management controller must enable time synchronization (Manual) 29
1.7 Host integrated hardware management controller must enable remote logging of events (Manual) 31
1.8 Host integrated hardware management controller must secure authentication (Manual) 33
1.9 Host hardware must enable AMD SEV-ES, if available (Manual) 35
1.10 Host hardware must enable Intel SGX, if available (Manual) 37
1.11 Host hardware must secure unused external hardware ports (Manual) 39
1.12 Host integrated hardware management controller must deactivate internal networking (Manual) 41

2 Base 43
2.1 Host must run software that has not reached End of General Support status (Manual) 44
2.2 Host must have all software updates installed (Manual) 46
2.3 Host must enable Secure Boot enforcement (Manual) 48
2.4 (Host image profile acceptance level must be PartnerSupported or higher (Automated) 50
2.5 Host must only run binaries delivered via signed VIB (Manual) 53
2.6 Host must have reliable time synchronization sources (Automated) 55
2.7 Host must have time synchronization services enabled and running (Manual) 58
2.8 Host must require TPM-based configuration encryption (Manual) 60
2.9 Host must not suppress warnings about unmitigated hyperthreading vulnerabilities (Manual) 62
2.10 Host must restrict inter-VM transparent page sharing (Automated) 64
2.11 Host must use sufficient entropy for cryptographic operations (Manual) 66
2.12 Host must enable volatile key destruction (Manual) 68

3 Management 70
3.1 Host should deactivate SSH (Automated) 71
3.2 Host must deactivate the ESXi shell (Automated) 73
3.3 Host must deactivate the ESXi Managed Object Browser (MOB) (Automated) 75
3.4 Host must deactivate SLP (Manual) 77
3.5 Host must deactivate CIM (Manual) 79
3.6 Host should deactivate SNMP (Manual) 81
3.7 Host must automatically terminate idle DCUI sessions (Automated) 83
3.8 Host must automatically terminate idle shells (Automated) 85
3.9 Host must automatically deactivate shell services (Automated) 87
3.10 Host must not suppress warnings that the shell is enabled (Manual) 89
3.11 Host must enforce password complexity (Manual) 91
3.12 Host must lock an account after a specified number of failed login attempts (Automated) 93
3.13 Host must unlock accounts after a specified timeout period (Automated) 95
3.14 Host must configure the password history setting to restrict the reuse of passwords (Manual) 97
3.15 Host must be configured with an appropriate maximum password age (Manual) 99
3.16 Host must configure a session timeout for the API (Manual) 101
3.17 Host must automatically terminate idle host client sessions (Manual) 103
3.18 Host must have an accurate DCUI.Access list (Manual) 105
3.19 Host must have an accurate Exception Users list (Manual) 107
3.20 Host must enable lockdown mode (Automated) 109
3.21 Host should enable strict lockdown mode (Automated) 111
3.22 Host must deny shell access for the dcui account (Manual) 113
3.23 Host must deny shell access for the vpxuser account (Manual) 115
3.24 Host must display a login banner for the DCUI and Host Client (Manual) 117
3.25 Host must display a login banner for SSH connections (Manual) 119
3.26 Host must enable the highest version of TLS supported (Manual) 121

Internal Only - General

4 Logging 123
4.1 Host must configure a persistent log location for all locally stored system logs (Manual) 124
4.2 Host must transmit system logs to a remote log collector (Automated) 127
4.3 Host must log sufficient information for events (Manual) 130
4.4 Host must set the logging informational level to info (Manual) 132
4.5 Host must deactivate log filtering (Manual) 134
4.6 Host must enable audit record logging (Manual) 136
4.7 Host must configure a persistent log location for all locally stored audit records (Manual) 138
4.8 Host must store one week of audit records (Manual) 140
4.9 Host must transmit audit records to a remote log collector (Manual) 142
4.10 Host must verify certificates for TLS remote logging endpoints (Manual) 144
4.11 Host must use strict x509 verification for TLS-enabled remote logging endpoints (Manual) 146

5 Network 148
5.1 Host firewall must only allow traffic from authorized networks (Manual) 149
5.2 Host must block network traffic by default (Manual) 151
5.3 Host must restrict use of the dvFilter network API (Manual) 153
5.4 Host must filter Bridge Protocol Data Unit (BPDU) packets (Manual) 155
5.5 Host should deactivate virtual hardware management network interfaces (Manual) 157
5.6 Host should reject forged transmits on standard virtual switches and port groups (Automated) 159
5.7 Host should reject MAC address changes on standard virtual switches and port groups (Automated) 161
5.8 Host should reject promiscuous mode requests on standard virtual switches and port groups (Automated) 163
5.9 Host must restrict access to a default or native VLAN on standard virtual switches (Automated) 166
5.10 Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches (Automated) 168
5.11 Host must isolate management communications (Manual) 170

6 Features 171
6.1 CIM 172
6.1.1 Host CIM services, if enabled, must limit access (Manual) 173
6.2 Core Storage 175
6.2.1 Host must isolate storage communications (Manual) 176
6.2.2 Host must ensure all datastores have unique names (Manual) 178
6.3 iSCSI 180
6.3.1 Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication (Automated) 181
6.3.2 Host iSCSI client, if enabled, must employ unique CHAP authentication secrets (Manual) 184
6.4 SNMP 187
6.4.1 Host SNMP services, if enabled, must limit access (Manual) 188
6.5 SSH 190
6.5.1 Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers (Manual) 191
6.5.2 Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules (Manual) 193
6.5.3 Host SSH daemon, if enabled, must not allow use of gateway ports (Manual) 195
6.5.4 Host SSH daemon, if enabled, must not allow host-based authentication (Manual) 197
6.5.5 Host SSH daemon, if enabled, must set a timeout count on idle sessions (Manual) 199
6.5.6 Host SSH daemon, if enabled, must set a timeout interval on idle sessions (Manual) 201
6.5.7 Host SSH daemon, if enabled, must display the system login banner before granting access (Manual) 203

Internal Only - General

6.5.8 Host SSH daemon, if enabled, must ignore .rhosts files (Manual) 205
6.5.9 Host SSH daemon, if enabled, must disable stream local forwarding (Manual) 207
6.5.10 Host SSH daemon, if enabled, must disable TCP forwarding (Manual) 209
6.5.11 Host SSH daemon, if enabled, must not permit tunnels (Manual) 211
6.5.12 Host SSH daemon, if enabled, must not permit user environment settings (Manual) 213

7 Virtual Machine 215

7.1 Virtual machines must enable Secure Boot (Manual) 216
7.2 Virtual machines must require encryption for vMotion (Manual) 218
7.3 Virtual machines must require encryption for Fault Tolerance (Manual) 220
7.4 Virtual machines should deactivate 3D graphics features when not required (Automated) 222
7.5 Virtual machines must be configured to lock when the last console connection is closed (Manual) 224
7.6 Virtual machines must limit console sharing. (Automated) 226
7.7 Virtual machines must limit PCI/PCIe device passthrough functionality (Automated) 228
7.8 Ensure unauthorized modification and disconnection of devices is disabled (Automated) 230
7.9 Virtual machines must prevent unauthorized connection of devices (Automated) 232
7.10 Virtual machines must remove unnecessary audio devices (Manual) 234
7.11 Virtual machines must remove unnecessary AHCI devices (Manual) 236
7.12 Virtual machines must remove unnecessary USB/XHCI devices (Automated) 238
7.13 Virtual machines must remove unnecessary serial port devices (Automated) 240
7.14 Virtual machines must remove unnecessary parallel port devices (Automated) 242
7.15 Virtual machines must remove unnecessary CD/DVD devices (Automated) 244
7.16 Virtual machines must remove unnecessary floppy devices (Automated) 246
7.17 Virtual machines must deactivate console drag and drop operations (Automated) 248
7.18 Virtual machines must deactivate console copy operations (Automated) 250
7.19 Virtual machines must deactivate console paste operations (Automated) 252
7.20 Virtual machines must limit access through the "dvfilter" network API (Manual) 254
7.21 Virtual machines must deactivate virtual disk shrinking operations (Automated) 257
7.22 Virtual machines must deactivate virtual disk wiping operations (Automated) 259
7.23 Virtual machines must restrict sharing of memory pages with other VMs (Manual) 261
7.24 Virtual machines must not be able to obtain host information from the hypervisor (Automated) 263
7.25 Virtual machines must enable diagnostic logging (Manual) 265
7.26 Virtual machines must limit the number of retained diagnostic logs (Automated) 267
7.27 Virtual machines must limit the size of diagnostic logs (Automated) 269
7.28 Virtual machines must limit informational messages from the virtual machine to the VMX file (Manual) 271
7.29 Virtual machines should have virtual machine hardware version 19 or newer (Manual) 273

8 VMware Tools 275

8.1 VMware Tools must be a version that has not reached End of General Support status (Manual) 276
8.2 VMware Tools must have all software updates installed (Manual) 278
8.3 VMware Tools should configure automatic upgrades as appropriate for the environment (Manual) 280
8.4 VMware Tools on deployed virtual machines must prevent being recustomized (Manual) 282
8.5 VMware Tools must limit the automatic addition of features (Manual) 284
8.6 VMware Tools must limit the automatic removal of features (Manual) 286
8.7 VMware Tools must deactivate GlobalConf unless required (Manual) 288
8.8 VMware Tools must deactivate ContainerInfo unless required (Manual) 290
8.9 VMware Tools must deactivate Appinfo information gathering unless required (Manual) 292
8.10 VMware Tools must deactivate Guest Store Upgrade operations unless required (Manual) 294

Internal Only - General

8.11 VMware Tools must deactivate Service Discovery unless required (Manual).....296
8.12 VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools (Manual).....298
8.13 VMware Tools must enable VMware Tools logging (Manual).....300
8.14 VMware Tools must send VMware Tools logs to the system log service (Manual).....301
8.15 VMware Tools must deactivate Guest Operations unless required (Manual).....303
Appendix: Summary Table..... 305
Appendix: CIS Controls v7 IG 1 Mapped Recommendations..... 315
Appendix: CIS Controls v7 IG 2 Mapped Recommendations..... 318
Appendix: CIS Controls v7 IG 3 Mapped Recommendations..... 325
Appendix: CIS Controls v7 Unmapped Recommendations..... 332
Appendix: CIS Controls v8 IG 1 Mapped Recommendations..... 333
Appendix: CIS Controls v8 IG 2 Mapped Recommendations..... 337
Appendix: CIS Controls v8 IG 3 Mapped Recommendations..... 344
Appendix: CIS Controls v8 Unmapped Recommendations..... 351
Appendix: Change History..... Error! Bookmark not defined.

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 8.0. 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 8.

The scope of this document does not extend to VMware vCenter 8, VMware vSphere 8, features and functions which are enabled when ESXi 8 is managed via VMware vCenter, or engineered solutions that incorporate ESXi 8.

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
Bob Plankers
Randall Mowen

Contributors
Tony Wilwerding
Matthew Reagan
Shawn Kearney

Internal Only - General

Recommendations

1 Hardware

This section contains recommendations for configuring server hardware to support the security features present in VMware ESXi.

Internal Only - General

1.1 Host hardware must have auditable, authentic, and up to date system & device firmware (Manual)

Profile Applicability:

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

Description:

Hardware firmware is not immune to serious issues affecting confidentiality, integrity, or availability. Vulnerable system management controllers & management engines can provide places for attackers to establish persistence, in order to re-infect and re-compromise hosts after reboots and updates.

Ensure that the latest firmware updates are applied to all components of your systems and that the firmware is authentic and supplied by your hardware manufacturer.

Rationale:

To ensure the integrity, security, and optimal performance of server hardware, it is essential to maintain system and device firmware that is verifiable, genuine, and current.

Impact:

If you are a vSAN customer please ensure that storage device & controller firmware versions are certified.

Audit:

The preferred approach is to utilize a vendor-supported, VMware-compatible firmware and driver combination. Leverage Broadcom's Lifecycle Manager hardware compatibility checks or similar tools if available.

If that is not available, manually inventory:

- System BIOS/UEFI
- BMC / iDRAC / iLO firmware
- TPM firmware
- RAID/storage controller firmware
- HBA firmware
- NIC firmware
- Fibre Channel adapter firmware
- NVMe / storage-device firmware where applicable
- GPU firmware where applicable

compare those results with the currently supported and recommended baseline as well as VMware Compatibility Guide for ESXi.

Internal Only - General

Remediation:

Proposed remediation guidelines:

1. Verify the exact server model and hardware components.
2. Obtain firmware only from the OEM/vendor:
    - Dell
    - HPE
    - Lenovo
    - Cisco
    - etc.
3. Verify that the proposed firmware and associated ESXi

   driver are supported for your ESXi 8 release.

4. Place the ESXi host in maintenance mode.
5. Apply firmware through the vendor-supported mechanism (for example):
    - Dell iDRAC / OpenManage
    - HPE iLO / SPP
    - Lenovo XClarity
    - Cisco UCS Manager
    - Vendor bootable firmware package
    - Vendor Hardware Support Manager
6. Reboot the physical host if required.
7. Re-run the firmware inventory.
8. Confirm device/driver/firmware compatibility.
9. Exit maintenance mode.

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.	●	●	●
v8	16.5 Use Up-to-Date and Trusted Third-Party Software Components Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●
v7	18.4 Only Use Up-to-date And Trusted Third-Party Components Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

Internal Only - General

1.2 Host hardware must enable UEFI Secure Boot (Manual)

Profile Applicability:

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

Description:

UEFI Secure Boot is a security feature of the Unified Extensible Firmware Interface (UEFI) specification. Its primary purpose is to ensure that only signed and trusted boot loaders and operating system kernels are allowed to execute during the system startup. This helps protect systems from malware and unauthorized software that might try to run before the operating system loads. By verifying the digital signatures of bootable applications and drivers, Secure Boot prevents potentially harmful code from compromising the boot process.

Rationale:

Enabling UEFI Secure Boot on the ESXi host hardware helps prevent malware and untrusted configurations.

Impact:

Enabling this after installation may render the host unbootable. Refer to the vSphere documentation for more information about enabling Secure Boot.

Audit:

From the ESXi Shell run the command:
`/usr/lib/vmware/secureboot/bin/secureBoot.py -s`

Expected return is "Enabled"

Alternatively, check if the host booted with UEFI by running the command: `vsish -e get /hardware/firmwareType`

Expected Return is "UEFI"

If these audits do not return compliant results review the remeidation section to resolve.

Remediation:

You must enable the physical server's UEFI Secure Boot in the server BIOS/UEFI.

1. Put the non-compliant Host into maintenance mode:

   ```
   vim-cmd hostsvc/maintenance_mode_enter
   ```

2. Verify Secure Boot compatibility:

   ```
   /usr/lib/vmware/secureboot/bin/secureBoot.py -c
   ```


Internal Only - General

3. Restart the ESXi host with the `reboot` command.
4. on the ESXI physical host BIOS/UEFI configuration, ensure that "boot mode" is UEFI
5. Under Boot or Security menus, look for "Secure Boot" and set it to "Enabled".
6. Save all modified firmware changes and reboot the ESXi host.
7. Verify results.

References:

1. https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-security/securing-esxi-hosts/uefi-secure-boot-for-esxi-hosts.html?utm_source=chatgpt.com
2. https://knowledge.broadcom.com/external/article/434297
3. https://knowledge.broadcom.com/external/article?articleNumber=393506

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.5 Use Up-to-Date and Trusted Third-Party Software Components Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		●	●
v7	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●
v7	18.4 Only Use Up-to-date And Trusted Third-Party Components Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●

Internal Only - General

1.3 Host hardware must enable Intel TXT, if available (Manual)

Profile Applicability:

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

Description:

Intel Xeon Scalable Processor platforms have Trusted Execution Technology, or TXT, that help harden systems against malware, rootkits, BIOS & firmware attacks, and more. When enabled, ESXi will take advantage of security benefits offered by this technology.

Rationale:

Enabling Intel TXT (Trusted Execution Technology) on host hardware, when available, provides a hardware-based foundation for security.

Impact:

In early implementations, operations such as firmware updates and abrupt system shutdowns may activate attestation alarms in vCenter Server or cause boot failures. Typically, a cold system restart offers a temporary fix, while a system firmware update provides a permanent solution. Refer to KB 78243.

Audit:

1. Execute: `esxcli hardware trustedboot get`
2. For hardware that supports Intel Trusted Execution Technology, verify:

   Drtm Enabled: true Tpm Present: true

Note: If Drtm Enabled is false, determine whether Intel TXT is supported by the host hardware and firmware. If TXT is supported but not enabled, the host is not compliant.

Remediation:

Place the ESXi host into maintenance mode and reboot the physical server. Enter the system BIOS/UEFI configuration and enable TPM 2.0 and Intel Trusted Execution Technology (TXT), where supported. Save the firmware configuration and perform a full reboot.

References:

1. The strongest Broadcom references for this specific control are KB 425234 for Intel TXT behavior on ESXi 8.x and KB 393506 for enabling TPM/TXT and validating trusted boot.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

1.4 Host hardware must enable and configure a TPM 2.0 (Manual)

Profile Applicability:

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

Description:

ESXi can use Trusted Platform Modules (TPM) 2.0 to enable advanced security features that prevent malware, remove dependencies, and secure hardware lifecycle operations.

Rationale:

Enabling and configuring TPM 2.0 on host hardware ensures enhanced security by providing hardware-level cryptographic operations and secure storage for sensitive data and keys.

Impact:

No impact noted.

Audit:

1. Execute `esxcli hardware trustedboot get`
2. Verify a TPM is present and trusted boot information is returned.
3. Run `esxcli system settings encryption get` and verify the command completes without TPM communication errors.
4. In vCenter, verify the host has no TPM attestation alarm.

Remediation:

1. Place the host in maintenance mode.
2. reboot into BIOS/UEFI.
3. Enable and activate the TPM
4. Select TPM 2.0 mode, and ensure UEFI/Secure Boot prerequisites required by the server vendor are enabled.
5. Save changes.
6. reboot with command `reboot`
7. Verify again with esxcli hardware trustedboot get and esxcli system settings encryption get.

References:

1. https://knowledge.broadcom.com/external/article?articleNumber=393506
2. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html

Internal Only - General

3. https://developer.broadcom.com/tools/esxcli/latest/

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	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

Internal Only - General

1.5 Host integrated hardware management controller must be secure (Manual)

Profile Applicability:

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

Description:

Many servers have integrated hardware management controllers that can be extremely helpful when monitoring and updating hardware, settings, and firmware. These controllers should be checked to ensure that ALL unused functionality is disabled, ALL unused access methods are disabled, passwords and password controls are set, and firewalling and access control is in place so that the only access is from authorized access workstations for the virtualization administration team.

All "first boot" configuration options should be disabled, especially ones that reconfigure the system from USB devices that are inserted. Disable or protect USB ports attached to the management controllers. Where possible, USB ports should be set to only permit keyboards.

Default passwords for accounts should be changed.

External information displays should be secured to prevent information leakage. Power and information buttons should be secured against unauthorized use.

Many hardware management controllers provide mechanisms for alerting when hardware faults & configuration changes occur. You should consider those if you are not using another method for hardware monitoring.

Rationale:

Impact:

Disablement of connection methods may mean that future monitoring and management efforts require changes to the hardware management controller configurations across your fleet of servers.

Most hardware management controllers have CLI and API management methods that can be scripted and used from a management workstation, in lieu of additional management software or applications. Learning these techniques saves time, avoids the additional effort of installing and maintaining additional tools, and allows for timely changes to configurations.

Audit:

1. Verify whether the ESXi host exposes a BMC interface:

```
esxcli hardware ipmi bmc get
```


Internal Only - General

2. Find the hardware management controller and review:

• Firmware is current and vendor-supported. • Default accounts and default passwords are not in use. • Administrative accounts are individually assigned. • Strong password/authentication policy is configured. • MFA is enabled where supported. • HTTPS/TLS is used for web management. • Weak or obsolete protocols are disabled. • SSH/IPMI access is disabled unless operationally required. • Management access is restricted to authorized management networks. • Remote console and virtual-media access are limited to authorized administrators. • Unused services and interfaces are disabled. • Security/event logging is enabled. • Certificates are valid and trusted where supported.

The expected compliant result: the BMC is running supported firmware, administrative access is strongly authenticated, unnecessary services are disabled, management traffic is isolated/restricted, and there are no default or shared administrative credentials.

Remediation:

Configure the controller according to the organization's secure-management baseline.

References:

1. https://knowledge.broadcom.com/external/article/424026/security-hardening-for-esxi-and-vcenter.html?utm_source=chatgpt.com

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	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

Internal Only - General

1.6 Host integrated hardware management controller must enable time synchronization (Manual)

Profile Applicability:

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

Description:

Cryptography, audit logging, cluster operations, and incident response/forensics depend deeply on synchronized time. This recommendation extends to all devices in infrastructure. The recommendation for NTP is to have at least four sources.

Rationale:

Ensuring the host integrated hardware management controller enables time synchronization provides a consistent and accurate timestamp for logs and events, which is crucial for auditing, troubleshooting, and identifying security incidents.

Impact:

No impact noted.

Audit:

1. Verify that NTP or another approved time synchronization mechanism is enabled
2. Verify that the ESXi host uses reliable time synchronization

```
esxcli system ntp get
```

Remediation:

1. Enable NTP or the vendor-supported automatic time synchronization service.
2. Enter the organization's approved NTP servers.
3. Configure multiple authoritative NTP sources where supported.
4. Configure the appropriate time zone.
5. Save/apply the configuration.

References:

1. https://knowledge.broadcom.com/external/article/317537/configuring-network-time-protocol-ntp-on.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	5.4 Deploy System Configuration Management Tools Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		●	●

Internal Only - General

1.7 Host integrated hardware management controller must enable remote logging of events (Manual)

Profile Applicability:

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

Description:

The host's integrated hardware management controller provides critical out-of-band server oversight. For enhanced security, it is essential to configure this controller to log events remotely. This practice ensures that hardware-related logs are sent to an off-site location, protecting them from potential tampering and offering a centralized record of server health and activities.

Rationale:

Enabling remote logging of events on the integrated hardware management controller ensures that all hardware-level activities are securely recorded off-site, providing traceability, mitigating data tampering risks, and facilitating incident response.

Impact:

No impact noted.

Audit:

Access the hardware management controller and verify that remote event logging/syslog forwarding is enabled and configured to send hardware, security, authentication, and management events to an approved centralized log collector.

Remediation:

Locate the controller's Syslog, Remote Logging, Event Forwarding, or equivalent configuration and:

1. Enable remote event logging.
2. Configure the hostname or IP address of the approved centralized log collector.
3. Configure the appropriate port and protocol.
4. Use TLS or another protected transport where supported.
5. Select the required event categories, including hardware, security, authentication, firmware, and administrative events.
6. Save the configuration.

Internal Only - General

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.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

Internal Only - General

1.8 Host integrated hardware management controller must secure authentication (Manual)

Profile Applicability:

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

Description:

Connections to centralized authentication sources, like Active Directory, should be disabled or carefully considered as attack vectors and dependency loops (for authentication, authorization, DNS, DHCP, and time). Consider managing local accounts on these devices through the APIs and CLI interfaces provided. If Active Directory must be used for authentication do authorization locally so that an attacker with access to Active Directory cannot promote themselves through group membership.

Rationale:

To prevent unauthorized access and potential malicious control of server hardware functions, it's essential to ensure that the integrated hardware management controller utilizes secure authentication mechanisms.

Impact:

Not connecting hardware management controllers to centralized authentication & authorization sources entails additional management. Most hardware management controllers have CLI toolkits or APIs to automate management of user accounts and/or authorization levels.

Audit:

1. Access the hardware management controller and verify that:

• Default credentials are not in use. • Each administrator has an individually assigned account. • Shared administrative accounts are avoided. • Strong password requirements are enforced. • Multi-factor authentication is enabled where supported. • Directory-based authentication such as LDAP/AD is used where supported. • Anonymous or unauthenticated access is disabled. • Unused local accounts are disabled or removed. • Account lockout / throttling is enabled. • Management sessions time out after inactivity. • Administrative privileges follow least privilege. • Remote authentication protocols use encrypted transport.

2. Verify that the configured BMC account is a dedicated account with only the privileges required for remote power operations.

Internal Only - General

Remediation:

Recommended remediations by configuring authentication according to the approved security baseline:

1. Change all default passwords.
2. Disable or rename default accounts where the platform permits.
3. Create individually assigned administrator accounts.
4. Remove or disable unused accounts.
5. Enforce strong password complexity and minimum-length requirements.
6. Configure account lockout or login throttling after repeated authentication failures.
7. Enable MFA where supported.
8. Integrate the controller with approved centralized authentication such as Active Directory, LDAP, RADIUS, or TACACS+ where supported.
9. Use role-based access control and grant only the privileges required for each administrative role.
10. Disable anonymous or unauthenticated management services.
11. Restrict management access to approved management networks.
12. Ensure web, API, and remote-console authentication uses TLS or another encrypted transport.
13. Verify successful and failed authentication attempts are logged and forwarded to the approved logging system.

References:

1. https://knowledge.broadcom.com/external/article/433220/changing-the-bmc-login-password-from-an.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

1.9 Host hardware must enable AMD SEV-ES, if available (Manual)

Profile Applicability:

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

Description:

AMD EPYC platforms support SEV-ES, a technology to encrypt memory and CPU register state, and limit visibility to the hypervisor, in order to increase workload security and decrease exposure to certain types of attacks. When configured properly, vSphere supports the use of SEV-ES inside guest virtual machines and containers under vSphere and vSphere with Tanzu. Enabling SEV-ES in system firmware eases future enablement inside virtual machines, containers, and guest OSes.

Rationale:

Enabling AMD SEV-ES (Secure Encrypted Virtualization-Encrypted State) on host hardware enhances the security of virtual machines by encrypting their memory and CPU state, reducing the risk of unauthorized data access and tampering from compromised hypervisors or malicious actors.

Impact:

Use of SEV-ES in a particular VM requires the guest OS to support it, and will limit some operational features such as vMotion, snapshots, and so on. Consult the documentation for more information about these tradeoffs.

Audit:

1. Execute:

`esxcfg-info | grep "\----\HV Support"` or `vsish -e cat /hardware/cpu/cpuInfo`

For an AMD host, the return value of 3 confirms AMD-V is enabled.

Remediation:

1. Place the ESXi host into maintenance mode and reboot the physical server.
2. Enter the server BIOS/UEFI configuration and enable the AMD virtualization and memory-encryption features required by the platform.

Internal Only - General

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-FB511CBA-4B89-469F-9799-D1347E1F2B0A.html?hWord=N4IghgNiBcIM4FMBuBaBcQF8g
2. https://knowledge.broadcom.com/external/article/323299/enabling-evc-on-a-host-with-an-evc-suppo.html

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

1.10 Host hardware must enable Intel SGX, if available (Manual)

Profile Applicability:

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

Description:

Intel Xeon Scalable Processor platforms have Software Guard Extensions, or SGX, a technology that helps applications protect data in system memory. When configured properly, vSphere supports the use of SGX inside guest virtual machines. Enabling SGX in system firmware eases future enablement inside virtual machines and guest OSes.

Rationale:

Intel SGX (Software Guard Extensions) provides hardware-based memory encryption that protects sensitive data from unauthorized access or modification by malicious software running at higher privilege levels, enhancing server security.

Impact:

Use of SGX requires guest OS support, and will limit some operational features inside vSphere, such as vMotion, snapshots, fault tolerance, and suspend/resume.

Audit:

1. Identify processor vendor and model:

   ```
   esxcli hardware cpu list
   ```

2. Review the server BIOS/UEFI
3. Verify that SGX is enabled.

Examples: Intel SGX = Enabled

Remediation:

1. Place the ESXi host into maintenance mode
2. Reboot the physical server
3. Enter the server BIOS/UEFI configuration and enable Intel SGX.

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-72D1F8FA-391C-41E2-83E0-32C5B062145D.html?hWord=N4IghgNiBcIJIDsAuBTCACAygcQBogF8g

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

1.11 Host hardware must secure unused external hardware ports (Manual)

Profile Applicability:

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

Description:

Unused ports, especially USB, can be used by attackers to attach storage, networking, and keyboards. Take reasonable steps to control access to these ports through disablement, access control, and/or with other means such as solid rack doors, rack side panels, and flooring that makes the ports inaccessible from outside the rack when the rack door is closed. Cables fit easily through many gaps in and around racks and rack doors, and stiff wires can be used to push them into sockets from outside the rack, as well as to dislodge cables to create a service disruption.

Where possible, USB ports should also be set to only permit keyboards.

When disabling functionality like this please consider that you may need to access the server using a USB keyboard during an outage or as part of lifecycle operations, and plan accordingly.

Rationale:

Unused external hardware ports can be exploited as potential entry points for unauthorized devices and malicious activity, thereby compromising server security.

Impact:

Security involves balancing risks, including ease of recovery from outages. Disabling external ports can hinder emergency use of the ESXi console. Servers can often toggle USB port access; ensure your choice aligns with organizational needs and is tested prior to incidents.

Audit:

Recommended physical interfaces to review and audit: USB ports SD-card slots Serial ports External PCIe expansion interfaces External management USB/vNIC interfaces Other removable-media or peripheral interfaces

Remediation:

1. Place the ESXi host into maintenance mode if remediation will require a reboot.
2. Access the server BIOS/UEFI or hardware-management controller and disable unused external interfaces.

Internal Only - General

References:

1. https://techdocs.broadcom.com/us/en/vmware-cis/vsphere/vsphere/8-0/vsphere-security/securing-esxi-hosts/general-security-recommendations/pci-pcie-devices-and-esxi.html
2. https://knowledge.broadcom.com/external/article/323377/configuring-usb-hidccid-passthrough-to-e.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	1.7 Deploy Port Level Access Control Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
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

1.12 Host integrated hardware management controller must deactivate internal networking (Manual)

Profile Applicability:

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

Description:

Many servers have integrated hardware management controllers with the ability to present virtual network interfaces to ESXi as a management interface. These approaches create potential backdoors for access and are used by adversaries to circumvent network-based/perimeter firewalls, in either direction, and avoid observation by IDS/IPS/threat analysis tools. In many cases this functionality is not strictly necessary to manage hosts.

Rationale:

Using integrated hardware management controllers to present virtual network interfaces to ESXi can inadvertently create backdoors, allowing adversaries to bypass firewalls and evade detection by security tools; often, this functionality isn't essential for host management.

Impact:

Disablement of internal networking may limit vendor management tool effectiveness.

Audit:

From the ESXi Shell

1. execute `esxcfg-advcfg -g /Net/BMCNetworkEnable`

Remediation:

To disable ESXi BMC internal networking:

1. execute `esxcfg-advcfg -s 0 /Net/BMCNetworkEnable`
2. execute `esxcfg-advcfg -g /Net/BMCNetworkEnable`

Looking for: Value of BMCNetworkEnable is 0

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	11.7 Manage Network Infrastructure Through a Dedicated Network Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

Internal Only - General

2 Base

This section contains recommendations for base ESXi install.

Internal Only - General

2.1 Host must run software that has not reached End of General Support status (Manual)

Profile Applicability:

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

Description:

The "End of General Support" (EOGS) status indicates that the software version has exceeded its primary support lifecycle, during which VMware provides new security patches, bug fixes, and technical assistance. When a product reaches this status, VMware no longer releases security updates for that version for customers outside of an extended support contract. Thus, systems still running software past its EOGS are potentially exposed to unpatched vulnerabilities and other security risks.

Rationale:

Running software beyond its EOGS can compromise the integrity, availability, and confidentiality of virtual environments. Keeping VMware ESXi software versions within the support period ensures that organizations have access to the latest security patches, critical updates, and vendor support.

Impact:

Failing to update and maintain software versions within the support period can lead to potential security breaches, data losses, and reduced operational efficiency, as the software might become incompatible with newer technologies and lack support for emerging security threats.

Audit:

1. Execute

   `vmware -vl` or `esxcli system version get`

2. Record the ESXi version/build.
3. Compare the installed release to Broadcom's current lifecycle/support matrix. The host is compliant only when the installed ESXi release remains within General Support.

Remediation:

To remediate this recommendation, upgrade the host to an ESXi release/build that is still within Broadcom General Support. Use vSphere Lifecycle Manager or the vendor-supported image, validate hardware compatibility first, place the host in maintenance mode, remediate/upgrade, reboot, and verify the new build.

Internal Only - General

References:

1. https://knowledge.broadcom.com/external/article/322186
2. https://knowledge.broadcom.com/external/article/308161

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

2.2 Host must have all software updates installed (Manual)

Profile Applicability:

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

Description:

Applying updates in a timely manner according to the severity of issues contributes greatly to the resilience of an environment. When applying updates, it is recommended to update vCenter Server first, if an update is available, and then proceed with updating ESXi. This sequence ensures that the management layer is updated before updating the ESXi hosts.

VMware publishes advisories on security vulnerabilities; for proactive notifications please subscribe to the mailing list at https://www.vmware.com/security/advisories.html

Rationale:

Issues in software that impact confidentiality, integrity, and/or availability can only be removed through patching to a version that resolves the issue. Threat actors exploit known vulnerabilities when attempting to gain unauthorized 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 brief outages. ESXi hosts that are compatible with Quick Boot may be able to greatly minimize the host restart time.

VMware vSphere Update releases add and change system functionality, whereas Patch releases only resolve issues.

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`.

Internal Only - General

Remediation:

Use VMware Lifecycle Manager to update and upgrade hosts when ESXi is managed through VMware vCenter. For standalone hosts use esxcli or API-driven methods for applying updates.

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.

Default Value:

N/A

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-lifecycle-manager/GUID-74295A37-E8BB-4EB9-BFBA-47B78F0C570D.html
2. https://kb.vmware.com/s/article/52477

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

2.3 Host must enable Secure Boot enforcement (Manual)

Profile Applicability:

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

Description:

Enabling Secure Boot enforcement ensures that the host only loads UEFI drivers and applications with valid digital signatures, as part of the UEFI firmware standard. It requires support from the server's BIOS and hypervisor boot loader, and mandates that all ESXi kernel modules, drivers, and VIBs be signed by VMware or a trusted partner subordinate.

Rationale:

Organizations should enable Secure Boot enforcement to enhance the security of their virtual environments. Requiring valid digital signatures for UEFI drivers and apps mitigates the risk of offline attacks, where an attacker could transfer the ESXi install drive to a non-Secure Boot host and boot it without detection. This control establishes a trusted boot process, reducing the risk of unauthorized access and maintaining the integrity of the ESXi host.

Impact:

Failing to enable Secure Boot enforcement exposes the ESXi host to potential security breaches. Without this control, an attacker could compromise the ESXi host by booting it on a non-Secure Boot host, bypassing ESXi's protections. This could lead to unauthorized access, data breaches, and compromise of the virtual environment's integrity. Enabling Secure Boot enforcement is crucial for maintaining a secure and trusted ESXi host, mitigating potential negative impacts, and safeguarding the virtual infrastructure.

Audit:

1. Execute

   ```
   esxcli system settings encryption get
   ```

2. Review the Secure Boot enforcement state.
3. Verify that Secure Boot is enabled at the hardware level with: `/usr/lib/vmware/secureboot/bin/secureBoot.py -s`
4. Secure Boot enforcement should be required where the platform supports it.

Remediation:

1. Enable UEFI Secure Boot and TPM 2.0 on the hardware.

Internal Only - General

2. Configure ESXi secure configuration/Secure Boot enforcement using the supported vSphere/ESXCLI procedure for the installed ESXi 8 build.
3. Reboot if required and verify both

   `secureBoot.py -s` and `esxcli system settings encryption get`

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/
3. https://knowledge.broadcom.com/external/article/434297

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

2.4 (Host image profile acceptance level must be PartnerSupported or higher (Automated)

Profile Applicability:

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

Description:

The acceptance level on ESXi regulates the type of software that can be installed on the system, with four distinct levels: VMwareCertified, VMwareAccepted, PartnerSupported, and CommunitySupported. It's advised to set the acceptance level to PartnerSupported or higher to ensure that only tested and digitally signed vSphere Installation Bundles (VIBs) are allowed for installation.

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:

Restricting the acceptance level to PartnerSupported or higher prevents the installation of CommunitySupported packages, which are unsigned and hence, potentially unreliable or insecure. This restriction, while enhancing security, might limit the range of software that can be installed on the ESXi 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".
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".

Internal Only - General

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/8.0/vsphere-security/GUID-751034F3-5337-4DB2-8272-8DAC0980EACA.html?hWord=N4IghgNiBcIApgE4BcB2BTRBlArgBzwHsV0ATEAXyA

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

2.5 Host must only run binaries delivered via signed VIB (Manual)

Profile Applicability:

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

Description:

The ESXi host is configured to only execute binaries originating from a valid, signed vSphere Installable Bundle (VIB) to enhance the integrity of the system. This measure thwarts attackers' attempts to use prebuilt toolkits on the host. The parameter governing this behavior is VMkernel.Boot.execInstalledOnly with a recommended setting of True.

Rationale:

Ensuring the execution of only signed binaries significantly mitigates the risk of running malicious or unverified code, thus enhancing the host’s security posture.

Impact:

This security control may hinder the installation or execution of third-party unsigned software, potentially impacting the flexibility and extensibility of the ESXi host environment.

Audit:

1. Execute

   ```
   esxcli system settings kernel list -o execInstalledOnly
   ```

2. Verify the configured/runtime value for execInstalledOnly is TRUE.
3. Review installed VIBs with

   `esxcli software vib list` for unauthorized or unsigned packages.

Remediation:

1. Remove unauthorized VIBs and set the kernel option with

   ```
   esxcli system settings kernel set -s execInstalledOnly -v TRUE
   ```

2. Reboot if the command or build indicates a reboot is required
3. Re-run the audit command and confirm only approved signed VIB-delivered binaries are executable.

Internal Only - General

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_software.html
2. https://developer.broadcom.com/tools/esxcli/latest/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
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.	●	●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

Internal Only - General

2.6 Host must have reliable time synchronization sources (Automated)

Profile Applicability:

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

Description:

Ensuring reliable time synchronization is crucial as various functions like cryptography, audit logging, cluster operations, and incident response/forensics are heavily dependent on synchronized time. Utilizing at least four NTP sources is recommended for achieving reliable time synchronization. Alternatively, PTP can be employed for sub-millisecond time accuracy, with NTP configured as a backup to maintain time synchronization resilience in case of primary server failure.

Rationale:

Reliable time synchronization supports accurate auditing, cryptographic integrity, cluster operations, and effective incident response/forensics. Having multiple time sources enhances the reliability and accuracy of time synchronization, which is fundamental for secure and efficient system operations.

Impact:

Inadequate time synchronization may lead to erroneous system logs, compromised cryptographic operations, inefficient cluster operations, and hindered incident response efforts. The resilience and accuracy of time synchronization are vital for maintaining operational integrity and security posture.

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:

Internal Only - General

```
# 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
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/8.0/vsphere-security/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.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
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

2.7 Host must have time synchronization services enabled and running (Manual)

Profile Applicability:

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

Description:

Ensure the host has time synchronization services enabled and operational as many functions such as cryptography, audit logging, cluster operations, and incident response/forensics depend on synchronized time. Services like NTP or PTP should be configured to start with the host and remain running to maintain time synchronization.

Rationale:

Having accurate time synchronization is crucial for the correct operation and auditing of the system. This will assist in incident response, forensics, and ensure that cryptographic functions operate correctly.

Impact:

Failure to maintain time synchronization can lead to inaccurate logging, which could complicate incident response and forensic analysis. It may also affect the functioning of cluster operations and cryptographic protocols.

Audit:

1. Execute (where available)

   `esxcli system ntp get` and `esxcli system ntp config get`

2. Verify a time synchronization service is enabled and configured.
3. Check the NTP service state with: `esxcli system process list | grep -i ntp`

   or the vSphere Client under Host > Configure > System > Time Configuration.

Remediation:

1. Configure approved NTP servers
2. Enable the NTP client firewall ruleset if required
3. Set the NTP service startup policy to start and stop with the host, and start the service.

Example: `esxcli system ntp set --enabled true` after configuring approved servers. Verify synchronization after remediation.

Internal Only - General

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

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

2.8 Host must require TPM-based configuration encryption (Manual)

Profile Applicability:

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

Description:

The host should enforce TPM-based configuration encryption to secure its configuration files, notably within the /etc/ directory or other namespaces. From vSphere 7.0 Update 2 onwards, configuration files archived are encrypted, leveraging a Trusted Platform Module (TPM) to "seal" the configuration to the host, thereby enhancing security against offline attacks. This encryption, once enabled, is irreversible and utilizes the physical TPM present during installation or upgrade.

Rationale:

Implementing TPM-based configuration encryption significantly bolsters security by protecting configuration files from unauthorized access and alterations. This measure is crucial for safeguarding the integrity of host configurations and preventing potential offline attacks.

Impact:

Enabling TPM-based configuration encryption alongside Secure Boot renders traditional root password recovery methods ineffective. It's imperative to ensure continued access to administrator accounts on ESXi to avoid access issues.

Audit:

1. Execute `esxcli system settings encryption get`
2. Verify that the host is using TPM-backed configuration encryption rather than an unprotected configuration mode
3. Confirm TPM 2.0 is healthy with `esxcli hardware trustedboot get`

Remediation:

1. Ensure TPM 2.0 and Secure Boot are enabled.
2. Take a backup of the ESXi recovery key
3. Configure the host to use TPM-backed configuration encryption using the supported ESXi secure-configuration procedure.
4. Reboot if required with the `reboot` command
5. Re-run `esxcli system settings encryption get`

References:

1. https://knowledge.broadcom.com/external/article?articleNumber=393506

Internal Only - General

2. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
3. https://developer.broadcom.com/tools/esxcli/latest/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

2.9 Host must not suppress warnings about unmitigated hyperthreading vulnerabilities (Manual)

Profile Applicability:

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

Description:

It is imperative to retain hyperthreading security warnings as they indicate unmitigated CPU vulnerabilities. The parameter governing this behavior is UserVars.SuppressHyperthreadWarning, with a recommended setting of 0.

Rationale:

Retaining these warnings ensures that potential CPU vulnerabilities are not overlooked, promoting a proactive approach towards addressing hardware-related security concerns.

Impact:

No functional impact is associated with this security control, however, ignoring hyperthreading warnings could obscure existing CPU vulnerabilities, potentially jeopardizing system security.

Audit:

1. Utilize the administrative PowerCLI session
2. Execute `Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressHyperthreadWarning`
3. Verify that the warning-suppression value is 0

Remediation:

1. Utilize the administrative PowerCLI session:

```
execute Get-VMHost | Get-AdvancedSetting -Name
UserVars.SuppressHyperthreadWarning | Set-AdvancedSetting -Value
0 -Confirm:$false
```

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
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

2.10 Host must restrict inter-VM transparent page sharing (Automated)

Profile Applicability:

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

Description:

Transparent Page Sharing (TPS) aids in optimizing memory usage among virtual machines but under certain circumstances can be exploited to access data on adjacent virtual machines unauthorizedly. By configuring the Mem.ShareForceSalting parameter, inter-VM TPS is restricted, enhancing isolation and security. The parameter governing this behavior is Mem.ShareForceSalting with a recommended setting of 2.

Rationale:

Restricting inter-VM TPS is crucial to prevent potential unauthorized access to data, ensuring an extra layer of isolation and security between virtual machines which is indispensable especially in a multi-tenant environment.

Impact:

There is no noted functional impact, indicating that restricting inter-VM TPS does not adversely affect the system's performance or operations while bolstering security against potential data access exploits.

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:

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`.

Internal Only - General

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

2.11 Host must use sufficient entropy for cryptographic operations (Manual)

Profile Applicability:

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

Description:

Starting with vSphere 8.0, ESXi has enhanced its entropy implementation to align with FIPS 140-3 and EAL4 certifications, ensuring a robust foundation for cryptographic operations. Kernel boot options dictate the activation of entropy sources on an ESXi host. The parameter governing this behavior is disableHwrng = FALSE and entropySources = 0.

Rationale:

Employing adequate entropy is crucial for ensuring the strength of cryptographic operations.

Impact:

There is no functional impact noted.

Audit:

1. Audit the first entropy control with:

   ```
   esxcli system settings kernel list -o disableHwrng
   ```

2. Verify that *disableHwrng* is absent or set to *FALSE*.
3. Hardware must support the required random-number instruction for the preferred FIPS entropy path.

Remediation:

1. Set the kernel option with:

   ```
   esxcli system settings kernel set -s disableHwrng -v FALSE
   ```

2. Reboot if required by the host/build and verify the configured and runtime values are FALSE.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

2.12 Host must enable volatile key destruction (Manual)

Profile Applicability:

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

Description:

By default, ESXi ensures that pages allocated for virtual machines (VMs), userspace applications, and kernel threads are zeroed out at the time of allocation, to prevent the exposure of sensitive data like cryptographic keys to other clients. However, these keys can remain in host memory for an extended period if the memory is not reused. The Mem.MemEagerZero parameter can be configured to enforce the zeroing out of userworld and guest memory pages when a userworld process or guest exits, and for kernel threads, memory spaces holding keys are zeroed out as soon as the secret is no longer needed. This practice adheres to the NIAP Virtualization Protection Profile and Server Virtualization Extended Package requirements of zeroing memory that may contain cryptographic keys upon process exit. The parameter governing this behavior is Mem.MemEagerZero with a recommended setting of 1.

Rationale:

Enabling volatile key destruction through the Mem.MemEagerZero parameter enhances the security posture by ensuring that sensitive information such as cryptographic keys are not left residually in the system memory, which could be exploited by malicious entities. This configuration aligns with the guidelines provided by the NIAP Virtualization Protection Profile and Server Virtualization Extended Package, indicating its criticality in maintaining a secure virtualized environment.

Impact:

Activating volatile key destruction through the Mem.MemEagerZero parameter results in additional shutdown time required for virtual machines, corresponding to the amount of allocated memory. While this may extend the downtime during reboots or migrations, the trade-off ensures a higher level of security by preventing the potential exposure of sensitive data, fulfilling compliance requirements, and aiding in the effective management of cryptographic materials within the virtualized environment.

Audit:

1. Utilize the administrative PowerCLI session.
2. Execute:

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

3. Verify that the value is 1.

Internal Only - General

Remediation:

1. Utilize the administrative PowerCLI session.
2. Execute:

```
Get-VMHost | Get-AdvancedSetting -Name Mem.MemEagerZero | Set-
AdvancedSetting -Value 1 -Confirm:$false
```

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/
3. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

3 Management

This section contains recommendations related to ESXi access management.

Internal Only - General

3.1 Host should deactivate SSH (Automated)

Profile Applicability:

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

Description:

Secure Shell (SSH) provides remote access to the ESXi shell, enabling direct host console access or remote connectivity. Deactivating SSH is a security measure aimed at minimizing remote access channels to the ESXi host, restricting it to essential connections only through vSphere Client, vCLI/PowerCLI, or published APIs. The service status should be set to "Stopped", allowing manual start and stop for troubleshooting or diagnostic activities when necessary.

Rationale:

Limiting remote access by deactivating SSH reduces potential attack vectors, promoting a secure operating environment. Enabling SSH only for diagnostics or troubleshooting ensures controlled access, aligning with security best practices.

Impact:

There is no functional impact noted; however, the measure requires alternative methods for remote management, such as vSphere Client or command-line tools, which may demand additional configurations or toolset proficiency.

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`.

Internal Only - General

3. Click on SSH then click Edit Startup Policy.
4. Set the Startup Policy is set to Start and Stop Manually.
5. Click OK.
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

3.2 Host must deactivate the ESXi shell (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. Activities performed from the ESXi Shell bypass all access controls, but are logged. The recommended setting for the ESXi shell is to be stopped and only started manually when needed, such as when running diagnostics or troubleshooting.

Rationale:

Ensuring non-essential services like the ESXi Shell are deactivated enhances the security posture.

Impact:

No functional impact is recorded. However, if ESXi shell functionalities are needed, manual activation is required.

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`.

Internal Only - General

5. Click on OK.

Alternately, use the following PowerCLI command:

```
# 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?hWord=N4IghgNiBcIKIDswCMIFMAEBBAxjtAzgRgC4D2pAFpnAMoAaAlhrdRFAL5A

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

3.3 Host must deactivate the ESXi Managed Object Browser (MOB) (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 and change system objects and configurations. It is a prudent security measure to deactivate the MOB unless it's essential for operations. The parameter governing this behavior is Config.HostAgent.plugins.solo.enableMob with a recommended setting of False.

Rationale:

Deactivating non-essential services like MOB adheres to the principle of least functionality, reducing potential attack vectors.

Impact:

There is no specified functional impact; however, if MOB functionalities are needed later, manual reactivation is required.

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/8.0/vsphere-security/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

3.4 Host must deactivate SLP (Manual)

Profile Applicability:

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

Description:

The Service Location Protocol (SLP) is used for the discovery and selection of network services in local area networks, which simplifies configuration by allowing computers to find necessary services automatically. The practice of deactivating SLP when not in use aligns with the principle of minimizing the attack surface by shutting down non-essential services. The recommended setting is to have the SLP service stopped, with the ability to start and stop it manually as required.

Rationale:

Deactivating non-essential services like SLP minimizes potential vectors of attack, thereby enhancing the host's security posture.

Impact:

There is no functional impact noted, however, manual intervention is required to start the SLP service when needed.

Audit:

1. Verify the SLP service is not running.
2. From ESXi Shell run: `/etc/init.d/slpd status`

   or Review service status in the vSphere Client.

Note: A disabled/not-running state is compliant.

Remediation:

1. Stop SLP if running:

   ```
   /etc/init.d/slpd stop
   ```

Note: Confirm no operational dependency requires SLP before disabling it.

References:

1. https://knowledge.broadcom.com/external/article/435932
2. https://knowledge.broadcom.com/external/article/313159

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

3.5 Host must deactivate CIM (Manual)

Profile Applicability:

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

Description:

Deactivating the Common Information Model (CIM) service, when not in use, aligns with the principle of minimizing the attack surface by disabling non-essential services. This action helps in reducing the potential vectors of attack, thus bolstering the host's security posture.

Rationale:

Deactivating non-essential services like CIM mitigates potential security risks associated with these services. This measure adheres to the principle of least functionality, which posits that only necessary services should be active to fulfill operational requirements.

Impact:

No functional impact has been specified. However, the deactivation of CIM might require administrators to manually start or stop the service when needed, potentially affecting operational workflows if CIM is required at a later stage.

Audit:

1. Review CIM/WBEM services in Host > Configure > Services

   or Execute: `esxcli system wbem get`

2. If CIM is not explicitly required, verify WBEM/CIM is disabled.

Remediation:

Prerequisite Confirm monitoring/storage integrations do not require CIM/WBEM. If not required:

1. Disable WBEM/CIM using: `esxcli system wbem set --enable false`

References:

1. https://knowledge.broadcom.com/external/article/313159
2. https://knowledge.broadcom.com/external/article/396097

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

3.6 Host should deactivate SNMP (Manual)

Profile Applicability:

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

Description:

Simple Network Management Protocol (SNMP) facilitates the management of networked devices. Minimize attack surface by disabling non-essential services. The recommended setting is to have the SNMP service stopped unless required and configured securely.

Rationale:

Deactivating SNMP when it's not needed reduces the attack surface, adhering to a minimalistic approach in service operation.

Impact:

While there isn't a direct functional impact, the absence of SNMP may require alternative methods for network management and monitoring.

Audit:

1. Execute `esxcli system snmp get`

If SNMP is not required, verify it is disabled. If it is required, document the exception and validate the separate SNMP hardening controls.

Remediation:

1. Disable SNMP when not required with:

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

If SNMP is required, restrict targets/communities, prefer secure SNMP configurations supported by the environment, and limit the ESXi firewall ruleset to authorized management networks.

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-4309DE28-AFB6-4B2D-A8EA-A38D36A8C6E6.html?hWord=N4IghgNiBcIM4DsC2AHEBfIA
2. https://knowledge.broadcom.com/external/article/432921
3. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
4. https://developer.broadcom.com/tools/esxcli/latest/

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

3.7 Host must automatically terminate idle DCUI sessions (Automated)

Profile Applicability:

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

Description:

By configuring a session timeout, unattended console sessions are automatically terminated, thereby reducing the potential security risks associated with lingering active sessions. The parameter governing this behavior is UserVars.DcuiTimeOut, with a recommended setting of 600 (10 minutes).

Rationale:

Automated termination of idle DCUI sessions enhances the security posture by minimizing the window of opportunity for unauthorized access through unattended sessions. It enforces a good security hygiene practice by ensuring that inactive sessions do not remain open indefinitely, which is in line with the principle of least privilege.

Impact:

While there's no functional impact specified, setting a timeout value that's too short may inconvenience users by terminating sessions prematurely, possibly interrupting workflow. Conversely, a timeout value that's too long may not adequately mitigate the risks associated with idle sessions. Hence, a balanced approach in configuring the session timeout value, aligned with the organizational security policy and user workflow, is crucial.

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`.

Internal Only - General

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:

```
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

3.8 Host must automatically terminate idle shells (Automated)

Profile Applicability:

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

Description:

The host should be configured to automatically terminate idle shell sessions to prevent potential unauthorized access due to forgotten logouts. Setting a timeout for idle SSH connections ensures that any unattended sessions are closed, thereby reducing the security risk. The parameter governing this behavior is UserVars.

Rationale:

Automatically terminating idle shells minimizes the risks associated with unattended sessions. It is a proactive measure to prevent potential unauthorized access to the host.

Impact:

There is no identified negative impact associated with enforcing this control as it serves to bolster the host's security posture.

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`.

Internal Only - General

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`.

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

3.9 Host must automatically deactivate shell services (Automated)

Profile Applicability:

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

Description:

Enabling the automatic deactivation of shell services minimizes the attack surface on the host. The time window for the ESXi Shell and SSH services' availability is defined by UserVars.ESXiShellTimeOut, after which these services are terminated. The recommended setting for this parameter is 3600.

Rationale:

Automatically deactivating shell services after a defined time window helps in reducing the risk associated with potential unauthorized access, ensuring a more secure ESXi host environment.

Impact:

There's no negative functional impact identified with this control; it contributes towards enhancing the host's security posture by limiting the availability of shell services.

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.

Internal Only - General

5. Set the value for this parameter is set to `3600` (1 hour) or less
6. Click `OK`.

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

3.10 Host must not suppress warnings that the shell is enabled (Manual)

Profile Applicability:

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

Description:

Having warnings for enabled SSH or ESXi Shell provides insight into potential security risks. Disabling such warnings can mask ongoing attacks. The parameter governing this behavior is UserVars.SuppressShellWarning with a recommended value of 0.

Rationale:

Maintaining visibility of shell service status through warnings is crucial for monitoring and early detection of unauthorized activities, helping in promptly addressing potential security threats.

Impact:

No negative functional impact is associated with this control; it enhances monitoring and response to potential security threats by ensuring warnings are visible and not suppressed.

Audit:

From an administrative PowerCLI session.

1. Execute `Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning`
2. Verify that the value is 0.

Remediation:

From an administrative PowerCLI session.

1. Execute `Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning | Set-AdvancedSetting -Value 0 -Confirm:$false`
2. Shell access should normally remain disabled; do not suppress the warning when it is enabled.

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/

Internal Only - General

2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●
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

3.11 Host must enforce password complexity (Manual)

Profile Applicability:

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

Description:

The enforcement of password complexity is managed through the Security.PasswordQualityControl parameter, allowing configuration of password length, character set requirements, and failed logon attempt restrictions. The recommended setting is "retry=3 min=disabled,15,15,15,15 max=64 similar=deny passphrase=3".

Rationale:

Abiding by NIST 800-63B Section 5.1.1.2 guidelines, not enforcing traditional composition rules facilitates the adoption of longer, more secure passphrases, enhancing overall security.

Impact:

Altering password complexity via Security.PasswordQualityControl may cause installation issues with other products and services within the VMware ecosystem not expecting such changes.

Audit:

To confirm password complexity requirements are set run the following PowerCLI command:

```
(Get-VMHost | Get-AdvancedSetting -Name
"Security.PasswordQualityControl").Value
```

- Confirm N0 is set to `disabled`.
- Confirm N1 is set to `disabled`.
- Confirm N2 is set to `disabled`.
- Confirm N3 is set to `disabled`.
- Confirm N4 is set to `15` or greater.

The above requires all passwords to be 15 or more characters long and comprised of at least one character from four distinct character sets.

Remediation:

To set the password complexity requirements, perform the following PowerCLI command:

Internal Only - General

```
Get-VMHOST | Get-AdvancedSetting -Name "Security.PasswordQualityControl" |
Set-AdvancedSetting -Value "retry=3
min=disabled,disabled,disabled,disabled,15"
```

The above requires all passwords to be 15 or more characters long and comprised of at least one character from four distinct character sets.

References:

1. http://www.openwall.com/passwdqc/README.shtml
2. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43.html#GUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43
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.	●	●	●
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

3.12 Host must lock an account after a specified number of failed login attempts (Automated)

Profile Applicability:

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

Description:

The security control involves restricting account access following a specified number of failed login attempts, acting as a deterrent against brute-force attacks. This control is applicable for SSH and vSphere Web Services SDK access, though not for the Direct Console Interface (DCUI) and the ESXi Shell. A default setting allows five failed attempts before account lockout, with automatic unlock after 15 minutes. The parameter governing this behavior is Security.AccountLockFailures with a recommended setting of 5.

Rationale:

Implementing this control bolsters the host's resilience against unauthorized access attempts, safeguarding system integrity. By thwarting brute-force attacks, it significantly elevates the security posture, making unauthorized access more challenging.

Impact:

A potential downside is the inadvertent denial-of-service scenario, especially with a low threshold for login failures. This could be exploited maliciously or trigger accidental lockouts, impacting system accessibility and possibly demanding additional administrative effort for account resets.

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.

Internal Only - General

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:

```
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

3.13 Host must unlock accounts after a specified timeout period (Automated)

Profile Applicability:

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

Description:

Ensuring that user accounts on the ESXi host are automatically unlocked after a specified period contributes to a balance between security and operational usability. This mechanism reactivates idle accounts promptly while mitigating potential unauthorized access risks. It's configured through a specific parameter which, when adjusted, defines the duration of the lockout period. The parameter governing this behavior is Security.AccountUnlockTime with a recommended setting of 900 seconds.

Rationale:

This setting reduces the inconvenience for benign users and the overhead on administrators, while also slowing down brute force credential stuffing attacks.

Impact:

No functional impact noted. The parameter's configuration ensures a security-usability balance, although misconfiguration could either expose the system to unauthorized access or disrupt user operations.

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.

Internal Only - General

5. Set the value for this parameter to `900`.

Alternately, use the following PowerCLI command:

```
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

3.14 Host must configure the password history setting to restrict the reuse of passwords (Manual)

Profile Applicability:

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

Description:

The goal is to inhibit the reuse of past passwords, acting as a deterrent against potential security breaches stemming from the exploitation of old, compromised credentials. This is achieved by configuring the Security.PasswordHistory parameter, which specifies the number of unique passwords a user must cycle through before a previous password can be reused. The recommended setting for this parameter is 5.

Rationale:

By enforcing a password history policy, organizations make it harder for malicious actors to gain unauthorized access using old passwords. This in turn elevates the overall security posture.

Impact:

The impact of altering the Security.PasswordHistory parameter is dependent on the chosen value. A lower value might diminish security by allowing password reuse sooner, while a higher value increases security but may also increase the likelihood of user frustration.

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`.

Internal Only - General

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:

```
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/
2. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-5173D050-40C3-49E3-8A75-4AE4931BC317.html?hWord=N4IghgNiBcIMoFMDGBXATgSwC4E8B0ACmAM7EDuA9mgCYASGxWVOIAvkA

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

3.15 Host must be configured with an appropriate maximum password age (Manual)

Profile Applicability:

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

Description:

Implementing a maximum password age, as determined by the Security.PasswordMaxDays parameter, is aligned with modern password policies outlined in NIST 800-63B Section 5.1.1.2, which argue against forced periodic password changes provided that passwords have sufficient complexity. The parameter governing this behavior is Security.PasswordMaxDays with a recommended setting of 99999.

Rationale:

Aligning with modern security standards by configuring an appropriate maximum password age can help in maintaining a balance between security and usability. This setting negates the need for periodic password changes, which have not been shown to significantly enhance security.

Impact:

Adjusting the Security.PasswordMaxDays parameter may affect vSphere UIs, requiring an email address for alert configurations. This necessitates either the provision of an email address or the use of PowerCLI for configuration, with the latter also requiring the configuration of an SMTP server in vCenter Server for email alerts. Various regulatory compliance frameworks have differing opinions of this practice.

Audit:

From an administrative PowerCLI session

1. Execute `Get-VMHost | Get-AdvancedSetting -Name Security.PasswordMaxDays`
2. Verify that the value matches organizational policy or 99999 when periodic password rotation is not required by policy.

Remediation:

1. Set the approved value with `Get-VMHost | Get-AdvancedSetting -Name Security.PasswordMaxDays | Set-AdvancedSetting -Value <approved_days> -Confirm:$false`
2. Document any policy-driven value that differs from the benchmark baseline.

Internal Only - General

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

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

3.16 Host must configure a session timeout for the API (Manual)

Profile Applicability:

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

Description:

A designated timeout ensures that sessions are not left open indefinitely, thereby reducing the exposure window for potential security threats. The parameter governing this behavior is Config.HostAgent.vmacore.soap.sessionTimeout with a recommended setting of 30 seconds.

Rationale:

A session timeout ensures that potential security threats from unauthorized users or malicious software exploiting open sessions are significantly reduced.

Impact:

There is no functional impact noted when configuring this security control, making it a low-risk enhancement towards securing the ESXi environment.

Audit:

Utilize the administrative PowerCLI session

1. Execute `Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.vmacore.soap.sessionTimeout`
2. Verify that the API inactivity timeout matches the organization's approved value.

Remediation:

1. Set the approved timeout with:

   ```
   Get-VMHost | Get-AdvancedSetting -Name
   Config.HostAgent.vmacore.soap.sessionTimeout | Set-
   AdvancedSetting -Value <seconds> -Confirm:$false
   ```

2. Validate administrative integrations after the change.

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

Internal Only - General

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.	●	●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	1.7 Deploy Port Level Access Control Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●

Internal Only - General

3.17 Host must automatically terminate idle host client sessions (Manual)

Profile Applicability:

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

Description:

Configuring the host to automatically terminate idle host client sessions helps mitigate security risks associated with unattended sessions, which could potentially be exploited. The recommended setting for this control is a timeout value of 900. The parameter governing this behavior is UserVars.HostClientSessionTimeout.

Rationale:

Automatic termination of idle sessions is crucial for preventing potential unauthorized access or exploitation of unattended sessions, thereby enhancing the host's security posture.

Impact:

There is no functional impact mentioned, but ensuring a balanced timeout value is essential to prevent inadvertent session terminations while maintaining security.

Audit:

Utilize administrative PowerCLI session.

1. Execute

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

2. Verify that the Host Client idle-session timeout is configured to the organization's approved limit and is not disabled with an unlimited value.

Remediation:

1. Set the approved idle timeout with

```
Get-VMHost | Get-AdvancedSetting -Name
UserVars.HostClientSessionTimeout | Set-AdvancedSetting -Value
<seconds> -Confirm:$false
```

2. Reconnect to the Host Client and confirm inactive sessions expire as expected.

Internal Only - General

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	1.7 Deploy Port Level Access Control Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●

Internal Only - General

3.18 Host must have an accurate DCUI.Access list (Manual)

Profile Applicability:

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

Description:

The DCUI.Access parameter in VMware ESXi is used to specify a list of users who are permitted to access the Direct Console User Interface (DCUI) of the ESXi host, especially when Lockdown Mode is enabled. This parameter helps in controlling and securing access to the ESXi host by allowing only authorized users to override Lockdown Mode and access the DCUI, particularly in scenarios where the host becomes isolated from vCenter. The parameter governing this behavior is DCUI.Access.

Rationale:

A properly configured DCUI.Access list ensures that only authorized users can override Lockdown Mode to access DCUI, providing a fail-safe against loss of management capability especially if the host loses connection to vCenter.

Impact:

Misconfiguration could lead to unauthorized access or potential lockout scenarios, making it crucial to validate the list and ensure the host's attachment to vCenter alongside correctly configured access and exception lists prior to Lockdown Mode activation.

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:

Internal Only - General

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.

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	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
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

3.19 Host must have an accurate Exception Users list (Manual)

Profile Applicability:

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

Description:

Establishing an accurate Exception Users list is essential for managing user privileges during lockdown mode. Users on this list retain their privileges, making it imperative to include only those necessary for direct host access like service accounts for third-party solutions. Ensuring a well-maintained list mitigates the risk associated with unauthorized actions, especially during host isolation scenarios in lockdown mode.

Rationale:

The Exception Users list is crucial for preserving necessary operational capabilities while maintaining a secure environment. By carefully managing this list, organizations can balance between security and functionality, ensuring that critical operations continue unhindered during lockdown mode.

Impact:

An improperly managed Exception Users list could potentially undermine the security posture by allowing unauthorized access, increasing the risk of malicious actions. It's vital to review and update this list regularly to align with the current operational and security requirements.

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

3.20 Host must enable lockdown mode (Automated)

Profile Applicability:

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

Description:

Implementing lockdown mode restricts direct access to ESXi hosts, mandating management via vCenter Server to uphold defined roles and access controls, mitigating risks associated with unauthorized or insufficiently audited activities. Exception Users list serves as an override mechanism, permitting specified users direct access even in lockdown mode. This mode offers a balanced approach between security and operational flexibility compared to the stricter lockdown mode which, if connectivity to vCenter Server is lost, necessitates host rebuilding.

Rationale:

Enabling normal lockdown mode enforces centralized management through vCenter Server, ensuring adherence to organizational access controls and auditing policies. This measure significantly lowers the risk of unauthorized activities by restricting direct host access, promoting a more controlled and auditable operational environment.

Impact:

The activation of lockdown mode may impede direct host access for certain operations like backup and troubleshooting. Although temporary deactivation is an option, ensuring proper reactivation post-operation is crucial to maintain the intended security posture.

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` or `Strict`.

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:

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`.

Internal Only - General

4. Click the radio button for `Normal` or `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/8.0/vsphere-security/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

3.21 Host should enable strict lockdown mode (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

3.22 Host must deny shell access for the dcui account (Manual)

Profile Applicability:

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

Description:

The dcui account, utilized for process isolation for the Direct Console User Interface (DCUI), possesses shell access which, when deactivated, minimizes the attack surface. This action is a proactive measure to enhance system security.

Rationale:

Deactivating shell access for the dcui account reduces the avenues of exploitation available to potential attackers. It is a prudent step towards a hardened security posture.

Impact:

There is no functional impact noted from denying shell access for the dcui account, making it a low-risk yet effective security control.

Audit:

1. From ESXi Shell, run:

   `getent passwd dcui` or grep '^dcui:' /etc/passwd and verify the dcui account uses a non-interactive shell such as /bin/false or another vendor-defined denied shell.

Remediation:

Configure the dcui service account to have no shell access using the supported ESXi account-management mechanism for the installed build, and verify that the account cannot establish an interactive shell.

Note: It is advised not to manually edit /etc/passwd unless directed by Broadcom support.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
v7	2.8 Implement Application Whitelisting of Libraries The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			●
v7	2.9 Implement Application Whitelisting of Scripts The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			●

Internal Only - General

3.23 Host must deny shell access for the vpxuser account (Manual)

Profile Applicability:

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

Description:

Deactivating shell access for the vpxuser account enhances security by enforcing an "API only" stance for predefined non-root ESXi users such as vpxuser and dcui.

Rationale:

This control reduces the attack surface by limiting the avenues through which system configurations can be altered, aligning with modern least privilege principles and ensuring that privileged authentication through vCenter Server remains tightly controlled.

Impact:

Deactivating shell access prevents users from granting shell access to others or changing passwords of users who have shell access, necessitating host-by-host reconfiguration through an authorized account if changes are required. This could potentially impact third-party workflows and necessitates the retention of at least one fully privileged user for necessary configurations.

Audit:

1. Execute `getent passwd vpxuser`

   or `grep '^vpxuser:' /etc/passwd` and verify the vCenter service account is denied interactive shell access.

Remediation:

Do not assign an interactive shell to vpxuser. If the account was altered, restore the vendor-supported no-shell configuration or reconnect/recreate the vCenter host management account using supported vCenter procedures.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
v7	2.8 Implement Application Whitelisting of Libraries The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			●
v7	2.9 Implement Application Whitelisting of Scripts The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			●

Internal Only - General

3.24 Host must display a login banner for the DCUI and Host Client (Manual)

Profile Applicability:

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

Description:

Enabling a login banner on the Direct Console User Interface (DCUI) and the Host Client interfaces provides a mechanism to display legal notices or organizational announcements at login. The parameter governing this behavior is Annotations.WelcomeMessage, with the recommended value being a text string aligned with organizational or legal advisories.

Rationale:

A login banner serves as a first line of legal defense against unauthorized access and misuse, stating the terms and conditions of system use. It also aids in reinforcing organizational security policies among authorized users.

Impact:

Implementation masks the "F2/F12" options and IP address information on the DCUI, potentially requiring additional documentation or training to ensure users are aware of these changes.

Audit:

From an administrative PowerCLI session

1. Execute to review the DCUI/Host Client annotation setting: `Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage`
2. Verify that the approved legal/security banner is present and matches policy.

Remediation:

Set the approved banner using Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage | Set-AdvancedSetting -Value '<approved banner>' -Confirm:$false, or configure it in Host > Configure > System > Advanced System Settings. Verify it displays in DCUI/Host Client.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

3.25 Host must display a login banner for SSH connections (Manual)

Profile Applicability:

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

Description:

ESXi facilitates the display of a login message, primarily aimed to deter unauthorized access and inform legitimate users regarding system usage obligations, particularly during SSH connections. The text for this display is defined by a specific parameter, which is advisable to be configured, especially when SSH is active, albeit it's recommended to keep SSH in a stopped state barring troubleshooting scenarios. The parameter governing this behavior is Config.Etc.Issue.

Rationale:

Displaying a login banner serves as a preliminary deterrent to unauthorized users while reinforcing legal and policy compliances for authorized users. It encapsulates a proactive security measure, alongside aligning with several compliance mandates that necessitate the use of login banners.

Impact:

There is no functional impact associated with this security control; however, the absence of a login banner might pose a risk in terms of legal protection and compliance adherence, especially during SSH connections where potential misuse could occur. It's prudent to consult with legal advisors to craft a banner text that aligns with organizational and legal requisites.

Audit:

From ESXi Shell

1. Review `/etc/ssh/sshd_config` for a Banner directive
2. Verify the referenced banner file contains the approved login warning.

If SSH is disabled, retain the compliant configuration for emergency enablement.

Remediation:

1. Configure Banner `/etc/issue` in the SSH configuration and place the approved warning text in the referenced file.
2. Restart SSH only if it is authorized to be running; otherwise leave SSH disabled.

Internal Only - General

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/
3. https://knowledge.broadcom.com/external/article/401837

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

3.26 Host must enable the highest version of TLS supported (Manual)

Profile Applicability:

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

Description:

The host should be configured to operate using the highest version of TLS supported to ensure secure communications. ESXi 8, by default, comes with TLS 1.2 enabled, although re-enabling other protocols is possible if required. Employing the highest version of TLS aids in protecting against known vulnerabilities present in older versions. The parameter governing this behavior is UserVars.ESXiVPsDisabledProtocols with the recommended setting of "sslv3,tlsv1,tlsv1.1".

Rationale:

Employing the highest version of TLS supported enhances the security posture by ensuring that communications are protected with modern encryption standards. This mitigates risks associated with known vulnerabilities in outdated TLS versions.

Impact:

Failure to enable the highest version of TLS supported may expose the host to vulnerabilities present in older versions, potentially compromising the confidentiality and integrity of communications.

Audit:

Review enabled TLS protocol settings for ESXi services. Use the vSphere Client and, where applicable, esxcli system settings advanced list/service configuration to verify legacy SSL/TLS versions are disabled and the highest ESXi 8-supported TLS version is enabled.

Remediation:

Disable unsupported/legacy protocol versions using Broadcom-supported TLS configuration procedures for ESXi 8 and dependent services. Test vCenter, backup, monitoring, and API integrations before broad deployment.

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-security/GUID-82028A21-8AB5-4E2E-90B8-A01D1FAD77B1.html?hWord=N4IghgNiBcICYEsDOYBGECmACALhJIAvkA

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

Internal Only - General

4 Logging

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

Internal Only - General

4.1 Host must configure a persistent log location for all locally stored system logs (Manual)

Profile Applicability:

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

Description:

Configure the Syslog.global.logDir parameter to specify a persistent directory for system logs, ensuring they are retained across reboots. This can be set to a directory on mounted NFS or VMFS volumes, other than the default which is an in-memory filesystem that retains only a single day's worth of logs.

Rationale:

Storing logs persistently is crucial for auditing, monitoring events, and diagnosing issues. Without persistent logging, critical indicators of compromise and user activity logs are lost at each reboot, which can hinder incident response and forensic investigations.

Impact:

There is no specified functional impact, however, consideration should be given to storage capacity as increased log retention will require more storage space. If the only local, non-vSAN storage is unreliable SD or USB media, configuring a remote logging host is advised.

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:

Internal Only - General

```
# 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
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/8.0/vsphere-security/GUID-F35D7005-58EB-48AC-99D5-B9942EB2A8EF.html?hWord=N4IghgNiBcIM4E84QPYHMQF8g
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.		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
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

4.2 Host must transmit system logs to a remote log collector (Automated)

Profile Applicability:

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

Description:

Transmitting system logs to a remote log collector ensures that ESXi logs are stored in a secure and centralized manner. This centralization not only allows for the streamlined monitoring of all hosts through a single tool but also facilitates aggregate analysis and searching capabilities.

Rationale:

Centralizing log storage on a remote log collector greatly enhances the ability to monitor, search, and analyze logs across multiple hosts. This central repository ensures that logs are protected from potential tampering, while also providing a robust long-term audit trail. By analyzing these logs, coordinated attacks or anomalies that might go unnoticed on individual hosts can be detected.

Impact:

There is no immediate functional impact when transmitting logs to a remote log collector. However, it is essential to ensure that the remote log collector is adequately secured and has sufficient storage capacity.

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:

Internal Only - General

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`.

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/8.0/vsphere-security/GUID-F35D7005-58EB-48AC-99D5-B9942EB2A8EF.html?hWord=N4IghgNiBcIM4E84QPYHMQF8g

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.		●	●

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

4.3 Host must log sufficient information for events (Manual)

Profile Applicability:

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

Description:

Set the Syslog.global.logLevel parameter to "info" to ensure that audit logs capture sufficient information for diagnosing issues and investigating security events. This setting strikes a balance between log verbosity and storage utilization. The parameter governing this behavior is Syslog.global.logLevel with a recommended setting of info.

Rationale:

Adequate log data is crucial for identifying indicators of compromise, enabling timely and effective response to cybersecurity incidents. The "info" level provides essential details without excessively consuming storage resources.

Impact:

More verbose logging levels will demand additional storage space while potentially burying critical entries under less significant data. Conversely, less verbose levels might miss capturing crucial information, hindering effective diagnostics and incident response.

Audit:

1. Execute command: `esxcli system syslog config get`
2. Review the output
3. Execute command: `esxcli system syslog config logger list`
4. Review the current logs with: `ls -lh /var/run/log`

Remediation:

1. Increase the number of rotations and/or individual log size
2. `esxcli system syslog config logger set --id=vmkernel --rotate=15 --size=10240`
3. `esxcli system syslog config logger set --id=hostd --rotate=15 --size=10240`

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	6.3 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

4.4 Host must set the logging informational level to info (Manual)

Profile Applicability:

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

Description:

Set the logging informational level to "info" via the Config.HostAgent.log.level parameter to ensure audit logs contain adequate data for diagnostics and forensics. This level provides a balanced amount of detail, suitable for routine analysis and investigation. The parameter governing this behavior is Config.HostAgent.log.level with a recommended setting of info.

Rationale:

The "info" level balances the detail in logs, aiding in diagnostics and forensics without overwhelming storage resources.

Impact:

A more verbose log level increases data volume, demanding additional storage, while a less verbose level may lack crucial information for effective diagnostics and forensics.

Audit:

From the ESXi shell:

1. execute - `esxcli system syslog config get | grep "Log Level"`

Remediation:

Using the vSphere client:

Host → Configure → System → Advanced System Settings → Syslog.global.logLevel

Set: info

Execute command: `esxcli system syslog config get | grep "Log Level"`
Verify - Log Level: info

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.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
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	6.3 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	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

Internal Only - General

4.5 Host must deactivate log filtering (Manual)

Profile Applicability:

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

Description:

Log filtering can be employed to diminish the frequency of repetitive log entries and to preclude specific log events entirely. By employing the Syslog.global.logFilters configuration parameter, one can stipulate filtering criteria, which when met, will cause the designated log events to be excluded from the system logs. The control aids in maintaining a clean, informative logging environment by filtering out unwanted or redundant log entries. The parameter governing this behavior is Syslog.global.logFiltersEnable with a recommended setting of FALSE.

Rationale:

Comprehensive logging is crucial for understanding and monitoring system behavior. By deactivating log filtering, administrators can capture all log events, regardless of their frequency or perceived importance. This guarantees a complete record of system activity, which can be invaluable for incident response and post-incident analysis.

Impact:

There is no direct functional impact from deactivating log filtering. However, it may result in increased storage requirements for log files due to the additional log entries being stored. Organizations should ensure adequate storage space is available for logs and consider adjusting log retention policies if necessary.

Audit:

From the ESXi shell:

1. execute: `esxcli system syslog config get | grep -i "Log Filtering"`

Remediation:

1. Disable log filtering
2. execute command: `esxcli system syslog config logfilter set --log-filtering-enabled=false`
3. execute: `Get-VMHost | Get-AdvancedSetting -Name "Syslog.global.logFiltersEnable"`

passing value is: False

Internal Only - General

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	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	6.3 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	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

4.6 Host must enable audit record logging (Manual)

Profile Applicability:

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

Description:

Enabling audit record logging on ESXi hosts ensures the local storage of audit records, providing a trail of activities performed on the host. This measure is pivotal for accountability, troubleshooting, and security investigations. The parameter governing this behavior is Syslog.global.auditRecord.storageEnable with a recommended setting of TRUE.

Rationale:

Enabling audit record logging is crucial for maintaining a secure and compliant operational environment. It provides visibility into host activities, aiding in identifying and investigating unauthorized or malicious actions.

Impact:

While beneficial for security and compliance, enabling audit record logging consumes additional storage space on the host, which may necessitate enhanced storage management practices to ensure optimal performance.

Audit:

From ESXi shell:

1. Execute: `esxcli system auditrecords get`

Remediation:

To enable local audit-record logging:

1. Execute command: `esxcli system auditrecords local enable`
2. Verify remediation with: `esxcli system auditrecords get`
3. passing results: Audit Record Storage Active: true

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.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
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	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

Internal Only - General

4.7 Host must configure a persistent log location for all locally stored audit records (Manual)

Profile Applicability:

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

Description:

Configuring a persistent log location for locally stored audit records on ESXi hosts is critical to ensure audit continuity. When the "/scratch" directory is linked to "/tmp/scratch", only a day's worth of records are retained, and they are reinitialized upon each reboot, creating a security risk. A persistent datastore, except a vSAN datastore, should be designated for audit record logging to preserve records across reboots. The parameter governing this behavior is Syslog.global.auditRecord.storageDirectory.

Rationale:

A persistent log location safeguards audit records, enhancing the auditability and diagnosability of system events. This setup helps in adhering to compliance requirements and facilitating future audits.

Impact:

Implementing this control will consume additional storage space for logs, necessitating a balanced approach to storage management, especially when local non-vSAN storage options are limited.

Audit:

From the ESXi shell:

1. Execute command - `esxcli system auditrecords get`
2. review the return values

Remediation:

Configure a persistent datastore location with:

```
esxcli system auditrecords local set \ --
directory=/vmfs/volumes/<Datastore-UUID>/audit/<hostname>
```

then

```
esxcli system auditrecords local enable
```

verify compliance with: `esxcli system auditrecords get`

compliant results = Audit Record Storage Active: true Audit Record Storage Directory: /vmfs/volumes/<Datastore-UUID>/audit/<hostname>

Internal Only - General

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.		●	●
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

4.8 Host must store one week of audit records (Manual)

Profile Applicability:

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

Description:

Ensuring a local storage capacity for a week's worth of audit records is imperative, especially when a remote audit record storage facility is used. This provision is critical during anticipated interruptions in record delivery to the remote facility, preventing loss or overwriting of audit records. The parameter governing this behavior is Syslog.global.auditRecord.storageCapacity with a recommended setting of 100.

Rationale:

Storing a week of audit records locally safeguards against data loss during interruptions with remote storage facilities, maintaining compliance and audit trail continuity.

Impact:

This security control entails additional storage space consumption for logs, requiring possible adjustments in storage management.

Audit:

1. Review the audit-record config with:

```
esxcli system auditrecords get
```

available audit records should span >= 7 days

Remediation:

Increase the local audit-record storage capacity to store at least 7 days worth of audit logs.

execute: `esxcli system auditrecords local set --size=<MiB>`

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.	●	●	●

Internal Only - General

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.		●	●
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

4.9 Host must transmit audit records to a remote log collector (Manual)

Profile Applicability:

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

Description:

This control enables the forwarding of audit records from the ESXi host to a designated log collector, aiding in real-time monitoring and analysis. The parameter governing this behavior is Syslog.global.auditRecord.remoteEnable with a recommended setting of TRUE.

Rationale:

Centralized logging facilitates a consolidated view of activities across ESXi hosts, enhancing the monitoring and rapid detection of unauthorized or anomalous activities.

Impact:

There is no noted functional impact from enabling this control; however, proper configuration is crucial to ensure reliable log transmission and to maintain the integrity and availability of audit records.

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`.

Internal Only - General

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`.

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.

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.		●	●
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

4.10 Host must verify certificates for TLS remote logging endpoints (Manual)

Profile Applicability:

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

Description:

When engaging in remote logging activities, it is of utmost importance to ensure that the logging endpoint is genuine and secure. To achieve this, hosts should verify the TLS certificates of these endpoints. This verification provides assurance that the endpoint is both authentic and trustworthy, mitigating the risk of transmitting logs to potentially malicious or untrusted entities. The parameter governing this behavior is Syslog.global.certificate.checkSSLCerts with a recommended setting of TRUE.

Rationale:

Ensuring the authenticity and trustworthiness of remote logging endpoints is crucial for maintaining the security and integrity of the transmitted log data. By verifying the TLS certificates of these endpoints, the potential risk of man-in-the-middle attacks, data breaches, or unintended exposure of sensitive log information is significantly reduced.

Impact:

There is no direct functional impact when verifying certificates for TLS remote logging endpoints. However, it is essential to ensure that the certificates used by the logging endpoints are valid and up-to-date. If not, there might be interruptions in log transmissions or potential trust issues, necessitating certificate management and regular updates.

Audit:

Execute command: `esxcli system syslog config get`

Remediation:

Execute command: `esxcli system syslog config set --check-ssl-certs=true`

Verify with: `esxcli system syslog config get`

remediated result should include: ssl://

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

Internal Only - General

4.11 Host must use strict x509 verification for TLS-enabled remote logging endpoints (Manual)

Profile Applicability:

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

Description:

When employing remote logging with TLS-enabled endpoints, it is essential to ensure the utmost integrity and authenticity of the certificates in use. The "x509-strict" option provides a higher level of security by performing additional validity checks on CA root certificates during the verification process. This increased scrutiny ensures that only genuinely authenticated and trusted certificates are accepted, minimizing potential vulnerabilities. The parameter governing this behavior is Syslog.global.certificate.strictX509Compliance with a recommended setting of TRUE.

Rationale:

Ensuring stringent verification of CA root certificates provides a higher level of trust and security in the remote logging process. Adopting the "x509-strict" option minimizes the risk of accepting compromised or malicious certificates, thereby reducing the potential for data breaches, man-in-the-middle attacks, or other security compromises.

Impact:

There is no immediate functional impact from using strict x509 verification for TLS-enabled remote logging endpoints. However, organizations must ensure that their CA root certificates meet the strict criteria set by this option. If certificates do not meet these criteria, there may be disruptions in log transmissions, necessitating adjustments or updates to the certificates in use.

Explicit warning: `Syslog.global.certificate.strictX509Compliance = true` can break connectivity to existing syslog endpoints if their certificates do not meet the stricter requirements.

Audit:

From ESXi shell:

Execute command: `esxcli system syslog config get`

Remediation:

Utilize PowerCLI to remediate

</> Powershell

Internal Only - General

```
Get-VMHost |
    Get-AdvancedSetting -Name
"Syslog.global.certificate.strictX509Compliance" |
    Set-AdvancedSetting -Value $true -Confirm:$false
```

Verify with

```
Get-VMHost |
    Get-AdvancedSetting -Name
"Syslog.global.certificate.strictX509Compliance"
```

Expected Calue is: Value = True

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

Internal Only - General

5 Network

This section contains recommendations related to configuring vNetwork.

Internal Only - General

5.1 Host firewall must only allow traffic from authorized networks (Manual)

Profile Applicability:

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

Description:

The host's firewall is designed to block all incoming and outgoing network traffic by default, unless exceptions are explicitly made, thus minimizing the attack surface and barring unauthorized access. The firewall settings, while simplistic, are akin to router ACLs, and might require reflexive rules to be configured for certain network scenarios. Through the VMware Host Client, restrictions can be placed on a per-IP basis to only allow traffic from authorized networks, aligning with the security control's recommended value of permitting connections solely from authorized infrastructure and administration workstations.

Rationale:

Implementing a policy where only traffic from authorized networks is allowed, significantly enhances the host’s security posture. It not only minimizes the attack surface but also helps in maintaining a clean network traffic flow, which is crucial for organizational security and operational efficiency.

Impact:

While this security control is instrumental in preventing unauthorized access, its simplistic firewall may necessitate additional configuration like reflexive rules, depending on the network setup. This could potentially require more administrative effort for correct configuration and management, ensuring that necessary communications are not inadvertently blocked.

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/8.0/vsphere-security/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

5.2 Host must block network traffic by default (Manual)

Profile Applicability:

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

Description:

By default, the host is configured to block all incoming and outgoing network traffic, except for the traffic pertaining to services enabled in the host security profile. This configuration is pivotal in reducing the attack surface and averting unauthorized access to the host. Even though there isn't a specific configuration parameter provided, the firewall settings are manageable through the VMware Host Client, wherein rules can be specified to allow or deny traffic for each service on a per-IP basis, ensuring only authorized networks have access.

Rationale:

Adhering to a policy of blocking network traffic by default significantly minimizes the risk of unauthorized access and potential external attacks. This posture promotes a principle of least privilege on the network level, ensuring only explicitly allowed traffic can communicate with the host, thereby enhancing the security posture.

Impact:

There is no functional impact mentioned for this security control. However, overly restrictive configurations might impede necessary communications if not properly managed, potentially affecting service availability and operational efficiency. Therefore, careful consideration and testing are advised when adjusting firewall settings to ensure essential traffic is not inadvertently blocked.

Audit:

1. Execute

   ```
   esxcli network firewall get
   ```

2. Verify the firewall is enabled.
3. Review each ruleset with esxcli network firewall ruleset list and confirm only explicitly required rulesets are enabled.

Remediation:

1. Enable the ESXi firewall if disabled and disable unnecessary rulesets.
2. Use: `esxcli network firewall set --enabled true`
3. Configure only the required rulesets for documented services.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●
v7	2.9 Implement Application Whitelisting of Scripts The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			●

Internal Only - General

5.3 Host must restrict use of the dvFilter network API (Manual)

Profile Applicability:

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

Description:

The Net.DVFilterBindIpAddress parameter controls the use of the dvFilter network API, allowing network information to be sent to a specified IP address. If enabled with a compromised IP address, unauthorized network access to other virtual machines on the host could occur. It's essential to keep this parameter unconfigured, unless required by a product like VMware NSX. The parameter governing this behavior is Net.DVFilterBindIpAddress with a recommended setting of "".

Rationale:

Limiting the use of the dvFilter network API by keeping the Net.DVFilterBindIpAddress parameter unconfigured helps in reducing potential security risks. This restriction aids in maintaining secure network communication and minimizes the attack surface.

Impact:

No functional impact is identified when restricting the dvFilter network API. However, incorrect configuration can lead to insecure network communication, posing a risk to the network security of virtual machines on the host.

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:

Internal Only - General

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. 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/6.7/com.vmware.vsphere.security.doc/GUID-CD0783C9-1734-4B9A-B821-ED17A77B0206.html?hWord=N4IghgNiBcICYDcCWAzJEAuBTATiAvkA

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

5.4 Host must filter Bridge Protocol Data Unit (BPDU) packets (Manual)

Profile Applicability:

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

Description:

To prevent cascading lockout of uplink interfaces from the ESXi host, the Net.BlockGuestBPDU parameter can be set to 1, enabling BPDU Filter to drop BPDU packets sent from virtual machines to the physical switch. This is crucial as ESXi's Standard and Distributed Virtual Switches do not support STP, making them prone to network loops if BPDUs are unfiltered. The parameter governing this behavior is Net.BlockGuestBPDU with a recommended setting of 1.

Rationale:

Configuring Net.BlockGuestBPDU aids in maintaining network stability by preventing potential disruptions caused by BPDU packets. This configuration is vital for avoiding unintended network lockouts and ensuring robust network communications.

Impact:

While beneficial for network stability, enabling BPDU filtering could block legitimate BPDU packets from network-oriented workloads. Ensure no legitimate BPDU packets are generated by virtual machines on the ESXi host before enabling this control.

Audit:

From an administrative PowerCLI session:

1. Execute: `Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU`
2. Verify that the value is 1 unless a documented workload requires guest-generated BPDUs.

Remediation:

From an administrative PowerCLI session:

Execute -

```
Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU | Set-
AdvancedSetting -Value 1 -Confirm:$false.
```

Validate network appliances/virtual switching workloads before enforcing this setting.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●

Internal Only - General

5.5 Host should deactivate virtual hardware management network interfaces (Manual)

Profile Applicability:

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

Description:

Hardware management controllers may present virtual or USB NICs to the host, potentially serving as backdoors if left active. It's recommended to deactivate these interfaces both in the hardware configuration and within ESXi to prevent unauthorized access. The parameter governing this behavior is Net.BMCNetworkEnable with a recommended value of 0.

Rationale:

Deactivating virtual hardware management network interfaces minimizes the attack surface, thereby enhancing the security posture of the host.

Impact:

While this control enhances security, it may impact third-party managed solutions that require these interfaces, necessitating alternative configurations or additional management considerations.

Audit:

Inspect host networking in the vSphere Client and with esxcli network ip interface list. Identify VMkernel interfaces used for hardware/BMC management or other virtual hardware management functions. Verify that such interfaces are absent unless explicitly required.

Remediation:

To remediate this recommendation, remove or deactivate unnecessary virtual hardware management VMkernel interfaces and associated port groups. Keep out-of-band BMC/iDRAC/iLO management on dedicated physical management networks wherever possible.

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

5.6 Host should reject forged transmits on standard virtual switches and port groups (Automated)

Profile Applicability:

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

Description:

Setting the "Forged transmits" option to "Reject" helps prevent MAC impersonation by comparing the source MAC address from the guest operating system with the effective MAC address of its virtual machine adapter. If there's a mismatch, the packet is dropped, preventing potential malicious activities through impersonated MAC addresses.

Rationale:

Rejecting forged transmits enhances network security by preventing unauthorized network access and malicious activities stemming from MAC impersonation. This setting upholds network integrity by ensuring only authorized communications occur within the network.

Impact:

This setting may affect workloads like clustered applications and network devices/functions that rely on MAC address modifications. Creating a separate port group for authorized virtual machines that require such behavior is recommended to balance operational needs with network security.

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/8.0/vsphere-security/GUID-3507432E-AFEA-4B6B-B404-17A020575358.html#GUID-7DC6486F-5400-44DF-8A62-6273798A2F80

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

5.7 Host should reject MAC address changes on standard virtual switches and port groups (Automated)

Profile Applicability:

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

Description:

Enforcing MAC address stability on standard virtual switches and port groups prevents MAC impersonation by disallowing changes to the MAC address by virtual machines. This mitigates the risk of malicious activities initiated by impersonating authorized network adapters.

Rationale:

Preventing MAC address changes hinders unauthorized network access and potential malicious acts, contributing to a more secure network environment. This control aids in maintaining network integrity by ensuring only authorized network communications occur.

Impact:

Certain workloads and operations reliant on MAC address modifications could be affected. Creating a separate port group for authorized virtual machines that require MAC address changes is recommended to balance operational and security needs.

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

5.8 Host should reject promiscuous mode requests on standard virtual switches and port groups (Automated)

Profile Applicability:

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

Description:

Enabling promiscuous mode allows all virtual machines in a port group to read all packets transmitted across it, regardless of the intended recipient. Rejecting promiscuous mode requests on standard virtual switches and port groups prevents unauthorized packet inspection, enhancing network isolation and data privacy.

Rationale:

Rejecting promiscuous mode requests helps maintain network isolation and data privacy by ensuring packets reach only their intended recipients. This control minimizes the risk of data interception or unauthorized packet inspection.

Impact:

Some workloads like DHCP servers or security monitoring may require promiscuous mode. In such cases, a separate port group allowing this behavior, with only authorized virtual machines connected, is advisable to balance operational needs with security controls.

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

5.9 Host must restrict access to a default or native VLAN on standard virtual switches (Automated)

Profile Applicability:

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

Description:

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:

```
# 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:

Internal Only - General

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

5.10 Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches (Automated)

Profile Applicability:

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

Description:

When a port group is set to VLAN 4095 on standard virtual switches, it enables Virtual Guest Tagging (VGT), letting all network frames pass to the attached virtual machines (VMs) without altering the VLAN tags. This requires VMs to process VLAN information themselves via an 802.1Q driver. Only authorized and capable VMs should be allowed to use VGT to prevent potential network issues like denial of service or unauthorized VLAN traffic interaction.

Rationale:

Restricting VGT use helps maintain network security by ensuring controlled VLAN tag management. It mitigates risks associated with denial of service or unauthorized VLAN interactions, contributing to a stable network environment.

Impact:

Incorrect VGT configuration can lead to denial of service or unauthorized VLAN traffic interaction. Restricting VGT may require alternative configurations for VMs needing independent VLAN tag management, potentially affecting network operation.

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:

Internal Only - General

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. 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

5.11 Host must isolate management communications (Manual)

Profile Applicability:

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

Description:

Ensure that only vmk interfaces designated for management purposes have management services enabled to uphold network isolation and security. Incorrect configuration may undermine security efforts by breaching network isolation principles.

Rationale:

Restricting management services to designated vmk interfaces minimizes the attack surface and ensures that management communications are isolated from other traffic, adhering to network segmentation best practices.

Impact:

This control may affect third-party managed solutions requiring specific configurations. Configurations may need to be tailored based on the particular environment and third-party solutions in use.

Audit:

Review VMkernel adapters with:

```
esxcli network ip interface list
```

Verify that management traffic is carried only on dedicated, approved VMkernel interfaces/VLANs and is not mixed with untrusted VM, storage, vMotion, or public traffic without an approved design.

Remediation:

To remediate this recommendation, create or move management VMkernel interfaces to dedicated management port groups/VLANs, apply firewall/ACL restrictions, and remove management service flags from interfaces that do not require them. Test vCenter connectivity before deleting the old path.

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

6 Features

Internal Only - General

6.1 CIM

Internal Only - General

6.1.1 Host CIM services, if enabled, must limit access (Manual)

Profile Applicability:

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

Description:

The Common Information Model (CIM) system allows for hardware-level management from remote applications through standard APIs. Ensuring only minimal access necessary to these applications is imperative to prevent potential security compromises. A dedicated service account, specific to each CIM application, should be created to limit access and privileges.

Rationale:

Restricting access to CIM services is essential to prevent unauthorized or over-privileged access, which could lead to potential security vulnerabilities. This practice adheres to the principle of least privilege, promoting a more secure environment.

Impact:

If improper access is granted to CIM-based hardware monitoring tools or other third-party applications, they may not function as expected or could be exploited to compromise the host's security.

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

6.2 Core Storage

Internal Only - General

6.2.1 Host must isolate storage communications (Manual)

Profile Applicability:

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

Description:

Isolating storage communications through zoning and Logical Unit Number (LUN) masking is instrumental in segregating Storage Area Network (SAN) activity. Zoning defines the connections between host bus adapters (HBAs) and targets, ensuring devices outside a zone remain invisible to the devices within, thus facilitating the independent management of zones such as testing and production. On the other hand, LUN masking controls the visibility and accessibility of LUNs to different hosts, further enhancing the granularity of access control within the storage network. By implementing these measures, the attack surface of the SAN is reduced, non-ESXi systems are prevented from accessing the SAN, and separation of environments like test and production is achieved.

Rationale:

Employing zoning and LUN masking to isolate storage communications is vital to reduce the risk of unauthorized access and potential cross-contamination between different operational environments. It allows for a more structured and secure management of storage resources, ensuring that unauthorized or incompatible systems are prevented from interacting with or accessing the SAN, thus contributing to the overall security and operational integrity of the environment.

Impact:

Failing to isolate storage communications can lead to an increased risk of unauthorized access to storage resources, potential data leakage, or interference between different operational zones. The lack of segregation might also pose challenges in managing and troubleshooting storage network activities, leading to operational inefficiencies and potential security risks.

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.

Internal Only - General

References:

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

6.2.2 Host must ensure all datastores have unique names (Manual)

Profile Applicability:

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

Description:

Ensuring unique naming for datastores is crucial to avoid potential errors that could affect the integrity and availability of data. A descriptive and unique name for each datastore facilitates better identification and management. Although there's no specific parameter to enforce this, manual or automated naming conventions should be adhered to.

Rationale:

Unique and descriptive naming for datastores minimizes the risk of errors, improves manageability, and aids in quicker identification, especially in environments with numerous datastores. It's a proactive measure to maintain order and avoid issues that arise from the default names given to VMFS and vSAN datastores.

Impact:

Not adhering to a unique naming convention can lead to confusion, misconfiguration, or incorrect data access. While renaming datastores could have downstream effects on systems like automation, monitoring, and backup, the benefits of unique naming conventions outweigh the potential negatives.

Audit:

List datastores with: `esxcli storage filesystem list`

or

PowerCLI

```
Get-Datastore
```

Verify that datastore names are unique across the managed vCenter inventory and are descriptive enough to prevent administrative ambiguity.

Internal Only - General

Remediation:

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	14.7 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

6.3 iSCSI

Internal Only - General

6.3.1 Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication (Automated)

Profile Applicability:

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

Description:

Implementing bidirectional CHAP authentication for iSCSI connections elevates security by necessitating mutual verification between the initiator (client) and target (server), ensuring data integrity during transmission. Configuration involves setting the iSCSI storage adapter authentication to "Use bidirectional CHAP" and providing the requisite credentials. This setup ensures that all communication between the client and server remains secure and unaltered, significantly reducing the risk of data interception by unauthorized entities. The parameter governing this behavior is set iSCSI storage adapter authentication to "Use bidirectional CHAP" with a recommended setting of Enabled.

Rationale:

Employing bidirectional CHAP authentication significantly minimizes risks associated with data interception or alteration by unauthorized entities during transmissions between the initiator and target. This additional layer of security is crucial in maintaining data integrity and confidentiality in iSCSI connections.

Impact:

No functional impact is anticipated upon the implementation of this control. However, it's imperative to ensure correct configuration to avoid potential communication disruptions between the iSCSI client and server.

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:

Internal Only - General

```
# 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`.
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

Internal Only - General

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`

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

6.3.2 Host iSCSI client, if enabled, must employ unique CHAP authentication secrets (Manual)

Profile Applicability:

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

Description:

Challenge-Handshake Authentication Protocol (CHAP) requires both client and host to know a secret to establish a connection. It is essential to employ unique CHAP authentication secrets for each iSCSI session to ensure secure communications. The parameter governing this behavior is outlined in the iSCSI or iSER storage adapter configuration under CHAP settings.

Rationale:

Utilizing unique CHAP authentication secrets for each iSCSI session promotes secure data transmission and mitigates the risk of unauthorized access.

Impact:

While enhancing security, misconfiguration or sharing of CHAP secrets across sessions could potentially lead to connectivity issues or unauthorized access.

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

Internal Only - General

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. 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.	●	●	●

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

6.4 SNMP

Internal Only - General

6.4.1 Host SNMP services, if enabled, must limit access (Manual)

Profile Applicability:

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

Description:

To manage hosts securely, if SNMP is enabled, access must be restricted. Preferably, SNMPv3 should be employed as it offers superior security through key authentication and encryption compared to SNMPv1 or SNMPv2. Configuring the destination for SNMP traps is essential for ensuring monitoring data is directed to a legitimate and secure host.

Rationale:

Proper SNMP configuration is crucial to reduce the risk of misuse or compromise, especially if other management means are in place. SNMPv3's enhanced security features are pivotal for secure management and monitoring.

Impact:

Improper SNMP configuration can redirect sensitive monitoring data to malicious hosts, risking exploitation and compromising host security.

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:

Internal Only - General

```
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.

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/8.0/vsphere-monitoring-performance/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

6.5 SSH

Internal Only - General

6.5.1 Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers (Manual)

Profile Applicability:

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

Description:

For enhanced security, if the SSH daemon is enabled on the host, it must utilize FIPS 140-2/140-3 validated ciphers. This requirement ensures the encryption standards are robust and compliant with regulatory mandates.

Rationale:

Employing FIPS validated ciphers is vital for maintaining a high level of security and integrity in communications. It aligns with industry best practices and regulatory compliance requirements, ensuring secure SSH connections.

Impact:

There is no functional impact noted for this control; however, it significantly improves the security posture by enforcing the use of strong, validated encryption ciphers for SSH communications.

Audit:

Review `/etc/ssh/sshd_config` and ESXi SSH effective settings for `Ciphers`. Verify that only organization-approved FIPS 140-2/140-3 validated cipher algorithms supported by ESXi 8 are enabled.

Remediation:

To remediate this recommendation, configure the SSH daemon to use only the approved FIPS-capable cipher list supported by the installed ESXi build. Validate access from approved administration clients before deploying broadly.

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).		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

Internal Only - General

6.5.2 Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules (Manual)

Profile Applicability:

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

Description:

When enabled, the SSH daemon on the host should employ FIPS 140-2/140-3 validated cryptographic modules provided by OpenSSH. Although these modules are enabled by default, they can be deactivated for backward compatibility, thus auditing and ensuring the correct setting is crucial for maintaining security standards.

Rationale:

Utilizing FIPS validated cryptographic modules ensures adherence to recognized security standards, which is essential for protecting data during SSH sessions. This aligns with industry best practices and compliance requirements, promoting a secure operating environment.

Impact:

There's no functional impact associated with this control. It significantly enhances the security posture by enforcing the use of validated cryptographic modules, minimizing the risks associated with SSH communications.

Audit:

Verify ESXi is operating with Broadcom-supported cryptographic modules and that SSH is using the platform-provided OpenSSH/crypto libraries. Review installed VIBs and do not accept replacement third-party SSH/crypto binaries.

Remediation:

To remediate this recommendation, remove unsupported SSH/cryptographic binaries and restore the signed ESXi components from an approved image/profile. Keep ESXi patched so the validated cryptographic modules remain current.

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).		●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

Internal Only - General

6.5.3 Host SSH daemon, if enabled, must not allow use of gateway ports (Manual)

Profile Applicability:

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

Description:

When enabled, the SSH daemon on the host should have the gateway ports feature disabled to prevent remote hosts from forwarding connections. This is a hardening measure to ensure that the SSH service is securely configured against potential forwarding misuses.

Rationale:

Disabling gateway ports is a preventative measure to avoid unauthorized forwarding by remote hosts, thus enhancing the security posture of the system. It is a prudent step in minimizing the attack surface associated with SSH service.

Impact:

There are no noted functional impacts associated with this control. It is a proactive security measure designed to prevent potential misuse of SSH service forwarding capabilities, without affecting the normal operation of the host.

Audit:

Review `/etc/ssh/sshd_config` and verify `GatewayPorts no`.

Remediation:

To remediate this recommendation, set `GatewayPorts no` in the supported ESXi SSH configuration. Restart SSH only during an authorized maintenance/admin window and verify the effective setting.

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.		●	●
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

6.5.4 Host SSH daemon, if enabled, must not allow host-based authentication (Manual)

Profile Applicability:

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

Description:

Ensuring the SSH daemon on the host disallows host-based authentication is a crucial step towards hardening system services. This prevents a host from authenticating on behalf of the users, thereby enforcing individual accountability and minimizing the risk of unauthorized access.

Rationale:

Disallowing host-based authentication enforces a more secure user authentication mechanism, promoting individual accountability. It minimizes the risk associated with trust relationships among hosts, thereby enhancing the overall security of the system.

Impact:

No functional impact is associated with this control. It solely acts to enhance security by enforcing stricter authentication practices, without hindering system operations.

Audit:

Review `/etc/ssh/sshd_config` and verify `HostbasedAuthentication no`.

Remediation:

To remediate this recommendation, set `HostbasedAuthentication no`, restart SSH if it is authorized to run, and verify host-based authentication is rejected.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

Internal Only - General

6.5.5 Host SSH daemon, if enabled, must set a timeout count on idle sessions (Manual)

Profile Applicability:

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

Description:

Setting a timeout count on idle SSH sessions ensures that inactive sessions are automatically disconnected after a specified period. This period is calculated by multiplying the timeout count with the idle timeout interval. Automatic disconnection of idle sessions reduces the window of opportunity for unauthorized access.

Rationale:

Implementing a timeout count on idle sessions promotes better security hygiene by minimizing the exposure of open SSH sessions. It adds a layer of protection against potential unauthorized access arising from forgotten or unattended sessions.

Impact:

There's no functional impact reported with this control. It's a preventive measure aimed at enhancing the security posture by mitigating the risks associated with lingering idle sessions.

Audit:

Review `/etc/ssh/sshd_config`

1. Verify `ClientAliveCountMax` is set to the benchmark/organization-approved value so idle sessions cannot remain indefinitely.

Remediation:

To remediate this recommendation, set `ClientAliveCountMax` to the approved value, then restart SSH if enabled and test that inactive sessions are closed after the configured interval/count.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.6 Host SSH daemon, if enabled, must set a timeout interval on idle sessions (Manual)

Profile Applicability:

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

Description:

Implementing a timeout interval on idle SSH sessions ensures that any inactive session gets disconnected after a certain period, improving the security posture. The total timeout duration is calculated by multiplying the timeout count by the idle timeout interval.

Rationale:

Enforcing a timeout interval on idle SSH sessions minimizes the risk of unauthorized access through forgotten or unattended sessions, thereby hardening the system services as per security best practices.

Impact:

No functional impact is reported with this control. The measure is preventive, aiming to mitigate risks associated with open, idle SSH sessions.

Audit:

Review `/etc/ssh/sshd_config`

1. Verify `ClientAliveInterval` is set to the benchmark/organization-approved idle-session interval.

Remediation:

To remediate this recommendation, set `ClientAliveInterval` to the approved number of seconds. Restart SSH if enabled and validate timeout behavior together with `ClientAliveCountMax`.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.7 Host SSH daemon, if enabled, must display the system login banner before granting access (Manual)

Profile Applicability:

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

Description:

Implementing a system login banner before granting SSH access ensures that crucial information or notices are conveyed to users attempting to login. The banner text is set through the host's Config.Etc.Issue advanced parameter.

Rationale:

Displaying a system login banner helps in providing legal notices or other critical information to users, ensuring they are informed before gaining access, which is a step towards hardening and securing system services.

Impact:

There is no functional impact reported with the enforcement of this control. It primarily serves to inform users or provide legal disclaimers, aiding in legal and regulatory compliance.

Audit:

Review `/etc/ssh/sshd_config` for a `Banner` directive and verify the referenced file contains the approved system-use/login warning.

Remediation:

To remediate this recommendation, configure the approved SSH banner file and `Banner` directive. Restart SSH only if enabled/authorized and confirm the banner appears before authentication.

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.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.8 Host SSH daemon, if enabled, must ignore .rhosts files (Manual)

Profile Applicability:

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

Description:

Ignoring .rhosts files is crucial in hardening the SSH daemon on the host, ensuring that trust relationships are explicitly defined and not implicitly accepted, thereby reducing the attack surface.

Rationale:

Ignoring .rhosts files removes potential security risks associated with outdated or overly permissive trust relationships, which is a step towards a hardened and more secure system service configuration.

Impact:

There are no reported functional impacts associated with ignoring .rhosts files; however, this practice enhances the security posture by mitigating risks associated with unauthorized access.

Audit:

Review `/etc/ssh/sshd_config` and verify `IgnoreRhosts yes`.

Remediation:

To remediate this recommendation, set `IgnoreRhosts yes`, restart SSH if authorized, and verify `.rhosts`-based trust is ignored.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.9 Host SSH daemon, if enabled, must disable stream local forwarding (Manual)

Profile Applicability:

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

Description:

Disabling stream local forwarding on the SSH daemon ensures that no Unix domain sockets are forwarded, thus enforcing a security boundary. This measure aids in maintaining the integrity and confidentiality of the system.

Rationale:

Disabling stream local forwarding helps in preventing potential misuse of Unix domain sockets which can be a vector for certain types of attacks or data leaks.

Impact:

There is no functional impact reported, indicating that disabling stream local forwarding is a safe measure towards enhancing system security without affecting operations.

Audit:

Review `/etc/ssh/sshd_config`

1. Verify `AllowStreamLocalForwarding no`.

Remediation:

To remediate this recommendation, set `AllowStreamLocalForwarding no`, restart SSH if authorized, and verify stream-local forwarding cannot be established.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

Internal Only - General

6.5.10 Host SSH daemon, if enabled, must disable TCP forwarding (Manual)

Profile Applicability:

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

Description:

Disabling TCP forwarding in the SSH daemon is a measure to prevent potential unauthorized tunneling and forwarding activities that could lead to data leaks or unauthorized data access. This measure adds a layer of security to the SSH service when enabled, making the system more resilient against certain types of network attacks.

Rationale:

Preventing TCP forwarding aids in ensuring that the SSH daemon is not misused for unauthorized tunneling. This measure assists in maintaining a more secure and controlled network environment.

Impact:

No functional impact has been reported. This indicates that disabling TCP forwarding is a precautionary measure that does not interfere with the normal operation of the host.

Audit:

Review `/etc/ssh/sshd_config`

1. Verify `AllowTcpForwarding no` unless an approved administrative use case requires it.

Remediation:

To remediate this recommendation, set `AllowTcpForwarding no`, restart SSH if authorized, and test that TCP forwarding is blocked. Document any approved exception.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.11 Host SSH daemon, if enabled, must not permit tunnels (Manual)

Profile Applicability:

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

Description:

Preventing tunnel creation in the SSH daemon is a security measure aimed at thwarting unauthorized network tunneling through the host. This control, when enforced, helps mitigate the risks associated with potential data exfiltration or unauthorized network access that could occur via SSH tunnels.

Rationale:

By disallowing tunnel creation, organizations can ensure that the SSH daemon is not exploited for unauthorized tunneling activities, thus contributing to a more secure network posture.

Impact:

There is no reported functional impact associated with this security control, indicating that the prevention of SSH tunneling does not adversely affect the host's normal operational behavior.

Audit:

Review `/etc/ssh/sshd_config` and verify `PermitTunnel no`.

Remediation:

To remediate this recommendation, set `PermitTunnel no`, restart SSH if authorized, and verify SSH tunnel devices cannot be created.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html
2. https://developer.broadcom.com/tools/esxcli/latest/

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

6.5.12 Host SSH daemon, if enabled, must not permit user environment settings (Manual)

Profile Applicability:

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

Description:

Preventing user environment settings in the SSH daemon ensures a consistent and controlled environment, reducing the attack surface by limiting the customization of the SSH environment by users.

Rationale:

Disallowing user environment settings within the SSH daemon reduces the potential for malicious or inadvertent misconfiguration, thus enhancing the security posture.

Impact:

There is no functional impact noted, indicating that restricting user environment settings does not adversely affect the operational aspects of the host.

Audit:

Review `/etc/ssh/sshd_config` and verify `PermitUserEnvironment no`.

Remediation:

To remediate this recommendation, set `PermitUserEnvironment no`, restart SSH if authorized, and verify users cannot alter the SSH environment through per-user environment settings.

References:

1. https://developer.broadcom.com/xapis/esxcli-command-reference/latest/namespace/esxcli_system.html

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.	●	●	●

Internal Only - General

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

7 Virtual Machine

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

Internal Only - General

7.1 Virtual machines must enable Secure Boot (Manual)

Profile Applicability:

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

Description:

Enable Secure Boot on virtual machines to ensure that only authenticated code runs from the firmware up through the operating system, thus providing a fundamental security measure against boot-time malware and unauthorized code execution. Supported by all modern guest operating systems, Secure Boot employs public key cryptography to validate the firmware, boot loader, drivers, and OS kernel at boot time.

Rationale:

By enforcing Secure Boot, organizations can mitigate the risk of boot-time malware and unauthorized code execution, which is crucial for maintaining the integrity and trustworthiness of the system from the first instruction.

Impact:

Activation of Secure Boot post guest OS installation may entail more than merely enabling a setting; consult the respective guest OS documentation for detailed instructions. This may introduce additional steps in the setup process, potentially extending the deployment time.

Audit:

The following PowerCLI command may be used:

```
(Get-VM -Name $VM).ExtensionData.Config.BootOptions.EfiSecureBootEnabled
```

Remediation:

The following PowerCLI command may be used:

```
$VMobj = (Get-VM -Name $VM)
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$bootOptions = New-Object VMware.Vim.VirtualMachineBootOptions
$bootOptions.EfiSecureBootEnabled = $true
$ConfigSpec.BootOptions = $bootOptions
$task = $VMobj.ExtensionData.ReconfigVM_Task($ConfigSpec)
```

Default Value:

Depends on VM Hardware version and guest OS selection.

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

7.2 Virtual machines must require encryption for vMotion (Manual)

Profile Applicability:

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

Description:

Requiring encryption for vMotion ensures the secure transfer of data among virtual machines. While the default 'opportunistic' encryption setting generally provides encryption due to prevalent AES-NI support, enforcing 'required' encryption eradicates the possibility of unencrypted transfers. The parameter governing this behavior is VM Configuration with the recommended setting being required.

Rationale:

Enforcing encryption for vMotion is crucial to prevent potential data leakage or unauthorized data access during data transfer processes, thereby bolstering the overall security infrastructure.

Impact:

There is no functional impact noted.

Audit:

The following PowerCLI command may be used:

```
(Get-VM -Name $VM).ExtensionData.Config.MigrateEncryption
```

Remediation:

The following PowerCLI command may be used:

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.MigrateEncryption = New-Object
VMware.Vim.VirtualMachineConfigSpecEncryptedVMotionModes
$ConfigSpec.MigrateEncryption = "required"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Default Value:

opportunistic

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	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

Internal Only - General

7.3 Virtual machines must require encryption for Fault Tolerance (Manual)

Profile Applicability:

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

Description:

Requiring encryption for Fault Tolerance in virtual machines is critical for ensuring secure data transmission between primary and secondary VMs, especially in environments where sensitive data is processed. While the default setting 'opportunistic' may result in encryption due to widespread AES-NI support in vSphere-compatible hardware, enforcing the 'required' setting for encryption guarantees that no unencrypted operations occur. The parameter governing this behavior is VM Configuration with a recommended setting of ftEncryptionRequired.

Rationale:

By enforcing encryption for Fault Tolerance, organizations bolster the security posture of their virtual environments against potential data interception or leakage during transmission. This requirement is vital for maintaining data integrity and confidentiality.

Impact:

There are no identified negative impacts associated with enforcing encryption for Fault Tolerance, and it's instrumental in enhancing the security of data transmission within virtual environments.

Audit:

The following PowerCLI command may be used:

```
(Get-VM -Name $VM).ExtensionData.Config.FtEncryptionMode
```

Remediation:

The following PowerCLI command may be used:

```
$VMview = Get-VM -Name $VM | Get-View
$ConfigSpec = New-Object VMware.Vim.VirtualMachineConfigSpec
$ConfigSpec.FtEncryptionMode = New-object
VMware.Vim.VirtualMachineConfigSpecEncryptedFtModes
$ConfigSpec.FtEncryptionMode = "ftEncryptionRequired"
$VMview.ReconfigVM_Task($ConfigSpec)
```

Default Value:

ftEncryptionOpportunistic

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	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

Internal Only - General

7.4 Virtual machines should deactivate 3D graphics features when not required (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.

Impact:

GPU and Virtual Desktops may require this functionality.

Audit:

The following PowerCLI command may be used:

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d
```

Remediation:

The following PowerCLI command may be used:

```
Get-VM -Name $VM | Get-AdvancedSetting mks.enable3d | Set-AdvancedSetting -
Value FALSE
```

Default Value:

Depends on VM Hardware version and guest OS selection.

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

7.5 Virtual machines must be configured to lock when the last console connection is closed (Manual)

Profile Applicability:

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

Description:

Configuring virtual machines to lock upon closing the last console connection enhances security by mitigating the risk of unauthorized access via open console sessions. This configuration is particularly useful in environments where multiple users have access to the console. The parameter governing this behavior is tools.guest.desktop.autolock with the recommended setting being TRUE.

Rationale:

Implementing this control provides an additional layer of security by ensuring that open console sessions do not remain accessible after the last connection is closed, thus reducing the potential for unauthorized access.

Impact:

No functional impact is associated with this control; it serves as a proactive measure to prevent unauthorized access through open console sessions.

Audit:

The following PowerCLI command may be used:

```
Get-VM -Name $VM | Get-AdvancedSetting tools.guest.desktop.autolock
```

Remediation:

The following PowerCLI command may be used:

If the audit returns blank or the value is not yet set

```
Get-VM -Name $VM | New-AdvancedSetting -Name tools.guest.desktop.autolock
$True
```

otherwise use

```
Get-VM | get-AdvancedSetting -Name tools.guest.desktop.autolock | set-
advancedsetting -Value $True
```

Default Value:

FALSE

Internal Only - General

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.	●	●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	1.7 Deploy Port Level Access Control Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●

Internal Only - General

7.6 Virtual machines must limit console sharing. (Automated)

Profile Applicability:

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

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

Internal Only - General

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

7.7 Virtual machines must limit PCI/PCIe device passthrough functionality (Automated)

Profile Applicability:

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

Description:

DirectPath I/O features provide virtual machines the ability to directly access system hardware, which while advantageous for performance, can impact risk mitigation tools like vMotion, DRS, and High Availability. It also opens up a potential attack vector for privileged hardware access. It is crucial to ensure that only necessary VMs have this privilege and that compensatory measures are taken within the guest OS to enhance security.

Rationale:

Limiting PCI/PCIe device passthrough functionality is essential for minimizing potential attack vectors and ensuring that risk mitigation tools function as intended. Moreover, audit and documentation of the business need for these VMs are critical for maintaining a secure and compliant environment.

Impact:

Passthrough devices, like GPUs, may be adversely affected if disconnected. It's imperative to audit and document the business rationale for VMs requiring this functionality to understand the associated risks and ensure adequate compensatory controls are in place.

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
``
A return value other than "false" needs to be remediated.
```

Remediation:

The following PowerCLI command can be used:

Internal Only - General

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

References:

1. https://docs.vmware.com/en/VMware-vSphere/8.0/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.		●	●
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

7.8 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

7.9 Virtual machines must prevent unauthorized connection of devices (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

7.10 Virtual machines must remove unnecessary audio devices (Manual)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

Audit:

From an administrative PowerCLI session

1. Execute `Get-VM | Get-SoundCard` where supported, or inspect each VM's Edit Settings > Virtual Hardware. Verify that audio devices are absent unless specifically required.

Remediation:

To remediate this recommendation, power off the VM when required, remove unnecessary sound/audio devices from Virtual Hardware, and validate the guest application after the change. Document any approved exception.

References:

1. https://knowledge.broadcom.com/external/article?legacyId=2007240
2. https://knowledge.broadcom.com/external/article/315390

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

7.11 Virtual machines must remove unnecessary AHCI devices (Manual)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

Audit:

Inspect VM hardware for unnecessary SATA/AHCI controllers. With PowerCLI/Get-View, review virtual devices and identify `VirtualAHCIController` devices that do not back a required virtual disk or CD/DVD device.

Remediation:

To remediate this recommendation, power off the VM if required and remove unused AHCI/SATA controllers only after removing or moving dependent devices. Do not remove a controller that is actively backing a required virtual disk.

References:

1. https://knowledge.broadcom.com/external/article?legacyId=2007240
2. https://knowledge.broadcom.com/external/article/315390

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

7.12 Virtual machines must remove unnecessary USB/XHCI devices (Automated)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

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

7.13 Virtual machines must remove unnecessary serial port devices (Automated)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

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.

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

7.14 Virtual machines must remove unnecessary parallel port devices (Automated)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

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.

Internal Only - General

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

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

7.15 Virtual machines must remove unnecessary CD/DVD devices (Automated)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

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

7.16 Virtual machines must remove unnecessary floppy devices (Automated)

Profile Applicability:

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

Description:

Removing unnecessary devices from virtual machines minimizes the attack surface and reduces potential pathways for data exfiltration or unauthorized data capture. This practice aligns with the principle of least functionality, ensuring that VMs have only the essential components required to perform their designated functions.

Rationale:

Eliminating unnecessary devices reduces attack surface and streamlines the virtual machine configuration, promoting a cleaner, more manageable, and less vulnerable setup.

Impact:

Careful analysis and understanding of the virtual machine's requirements and dependencies are crucial before implementing this security control to avoid unintended disruptions or degradation of service.

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

7.17 Virtual machines must deactivate console drag and drop operations (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 -Name $VM | Get-AdvancedSetting isolation.tools.dnd.disable
```

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 -Name $VM | Remove-AdvancedSetting -Name isolation.tools.dnd.disable
```

Default Value:

TRUE

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

7.18 Virtual machines must deactivate console copy operations (Automated)

Profile Applicability:

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

Description:

Deactivating console copy operations is critical for preventing data transfer between the virtual machine and the local client, irrespective of the access method, whether via Web Console, VMRC, or others. The parameter governing this behavior is isolation.tools.copy.disable with a recommended setting of TRUE or Undefined.

Rationale:

Deactivating console copy operations minimizes the risk of unauthorized data access or leakage, enforcing a higher level of data security and integrity across the virtual environment.

Impact:

There is no identified functional impact; however, this restriction enhances data security by minimizing unauthorized data transfer channels.

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`.

Internal Only - General

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:

```
# 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

7.19 Virtual machines must deactivate console paste operations (Automated)

Profile Applicability:

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

Description:

Disabling console paste operations on virtual machines obstructs data transfer from the local client to the VM, irrespective of the access method - be it Web Console, VMRC, or another console. This security measure aims to curtail potential avenues for unauthorized data transfer into the virtual environment. The parameter governing this behavior is isolation.tools.paste.disable with a recommended setting of TRUE or Undefined.

Rationale:

By disabling console paste operations, organizations add a layer of security that helps in preventing unauthorized data introduction into the VM, which could potentially lead to various security risks.

Impact:

There is no functional impact identified. The control simply enhances the security posture by reducing possible data transfer channels into the VM.

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`.

Internal Only - General

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:

```
# 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

7.20 Virtual machines must limit access through the "dvfilter" network API (Manual)

Profile Applicability:

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

Description:

The dvFilter interface facilitates network traffic filtering and inspection, predominantly via tools like NSX. It's vital to allow only authorized tools to access this interface to uphold network security. Unauthorized access could lead to illicit network traffic inspection or misuse. The parameter governing this behavior is ethernet*.filter*.name with a recommended setting of Not Present.

Rationale:

Limiting access through the "dvfilter" network API to authorized tools is essential for preserving network integrity and security. This restriction curtails the risk of unauthorized data inspection and potential network vulnerabilities.

Impact:

While enhancing security by restricting access to the dvFilter interface, this control may hinder the functionality of legitimate network tools like NSX, which necessitate access to the "dvfilter" network API for proper operation.

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:

Internal Only - General

1. Verify that the following is 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: 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.

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

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	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

7.21 Virtual machines must deactivate virtual disk shrinking operations (Automated)

Profile Applicability:

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

Description:

Disabling virtual disk shrinking on virtual machines prevents potential disk unavailability issues. This operation is usually restricted for non-administrative users within the guest environment. The parameter governing this behavior is isolation.tools.diskShrink.disable with a recommended setting of TRUE or Undefined.

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:

There is no functional impact noted.

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:

Internal Only - General

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.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

7.22 Virtual machines must deactivate virtual disk wiping operations (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:

Deactivating virtual disk wiping operations contributes to maintaining disk availability, which is vital for continuous system operations.

Impact:

There isn't a functional impact noted

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`.

Internal Only - General

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:

```
# 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

7.23 Virtual machines must restrict sharing of memory pages with other VMs (Manual)

Profile Applicability:

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

Description:

Configuring virtual machines with the sched.mem.pshare.salt option restricts Transparent Page Sharing (TPS) among different VMs, mitigating the risk of unauthorized data access under certain conditions. By doing so, each VM operates with a distinct memory sharing pool, thereby enhancing isolation and security. The parameter governing this behavior is sched.mem.pshare.salt.

Rationale:

Restricting memory page sharing among VMs minimizes the potential for unauthorized data access, thus aligning with best practices of data isolation and security. This configuration is a proactive measure to mitigate vulnerabilities associated with memory sharing.

Impact:

There is no functional impact associated with this security control as it serves to bolster the security posture of the VMs without affecting their operational performance or functionality.

Audit:

From an administrative PowerCLI session

1. Execute `Get-VM | Get-AdvancedSetting -Name sched.mem.pshare.salt`
2. Verify that any explicitly configured salt does not intentionally enable cross-VM sharing; review cluster/host TPS policy and confirm inter-VM transparent page sharing is restricted.

Remediation:

To remediate this recommendation, remove legacy settings that deliberately use a common salt across VMs. Where an explicit salt is required, configure a unique value per VM and maintain the ESXi default behavior that prevents inter-VM page sharing.

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

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

7.24 Virtual machines must not be able to obtain host information from the hypervisor (Automated)

Profile Applicability:

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

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

7.25 Virtual machines must enable diagnostic logging (Manual)

Profile Applicability:

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

Description:

Enabling diagnostic logging on virtual machines facilitates forensic analysis and troubleshooting by collecting necessary operational data. The parameter governing this behavior is Enable Logging with a recommended setting of TRUE.

Rationale:

Diagnostic logging is crucial for identifying and analyzing issues that may arise within a virtual machine environment. It supports timely resolution of problems, thus maintaining system integrity and operational efficiency.

Impact:

There is no negative functional impact identified for enabling diagnostic logging. This control significantly aids in issue resolution, enhancing overall system reliability and performance.

Audit:

From an administrative PowerCLI session:

1. Execute `Get-VM | Get-AdvancedSetting -Name logging`
2. Verify that VM diagnostic logging is enabled (`TRUE`) or that the setting is absent and the platform default provides logging. Confirm each VM has current vmware.log files in its datastore directory.

Remediation:

To remediate this recommendation, set `logging` to `TRUE` for affected VMs using `Set-AdvancedSetting` or create the setting with `New-AdvancedSetting` if necessary. Verify new VM log entries are generated.

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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	6.3 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

7.26 Virtual machines must limit the number of retained diagnostic logs (Automated)

Profile Applicability:

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

Description:

Limiting the number of retained diagnostic logs in virtual machines helps in managing datastore space effectively without hampering diagnostic capabilities. The parameter governing this behavior is log.keepOld with a recommended setting of 10 or Undefined.

Rationale:

Maintaining a sensible limit on the number of diagnostic logs retained helps in avoiding potential issues related to datastore space exhaustion, while still retaining a useful set of recent logs for troubleshooting purposes.

Impact:

There is no negative functional impact.

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`.
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.

Internal Only - General

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"
```

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

7.27 Virtual machines must limit the size of diagnostic logs (Automated)

Profile Applicability:

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

Description:

Limiting the size of diagnostic logs on virtual machines ensures efficient utilization of datastore space, particularly beneficial for long-running VMs. This control assists in maintaining an optimal balance between diagnostic capabilities and storage resources. The parameter governing this behavior is log.rotateSize.

Rationale:

Setting a limit on the size of diagnostic logs helps in preventing excessive space consumption, thus ensuring that ample storage remains available for other essential operations.

Impact:

There is no negative functional impact identified by limiting the size of diagnostic logs. This control facilitates proficient management of storage resources, ensuring other vital functions are not compromised due to space exhaustion.

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`.
3. Click on `EDIT CONFIGURATION`.

Internal Only - General

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

7.28 Virtual machines must limit informational messages from the virtual machine to the VMX file (Manual)

Profile Applicability:

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

Description:

Limit the number of informational messages from the virtual machine to the VMX file to prevent the file from exceeding its default size of 1MB, thereby avoiding potential denial of service situations due to a full datastore. The parameter governing this behavior is tools.setInfo.sizeLimit with a recommended setting of 1048576 or Undefined.

Rationale:

This control helps in maintaining a clutter-free VMX file, ensuring the datastore operates optimally without being overwhelmed by excessive informational messages, which in turn supports system reliability and performance.

Impact:

No negative functional impact identified.

Audit:

From an administrative PowerCLI session:

1. Execute `Get-VM | Get-AdvancedSetting -Name tools.setInfo.sizeLimit`
2. Verify that a finite approved limit is configured for information written by VMware Tools to the VMX file.

Remediation:

To remediate this recommendation, set `tools.setInfo.sizeLimit` to the organization-approved limit using `Set-AdvancedSetting/New-AdvancedSetting`. Validate any guest-management tooling that relies on guest information exchange.

References:

1. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/get-advancedsetting/
2. https://developer.broadcom.com/powercli/latest/vmware.vimautomation.core/commands/set-advancedsetting

Internal Only - General

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

7.29 Virtual machines should have virtual machine hardware version 19 or newer (Manual)

Profile Applicability:

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

Description:

Upgrade to hardware version 19 or newer to access enhanced features and better performance. Test the upgrades and ensure compatibility across all operational landscapes.

Rationale:

Upgrading facilitates improved performance and feature access, aligning with ESXi and vSphere updates, while ensuring service continuity across various environments.

Impact:

Changes in device versions within the guest may occur, requiring thorough testing to prevent service disruptions. Snapshots can aid in testing, allowing you to revert the hardware version if needed.

Audit:

From an administrative PowerCLI session:

1. Execute `Get-VM | Select Name,Version`
2. Verify that virtual machine hardware compatibility is version 19 (`vmx-19`) or newer for VMs in scope.

Remediation:

Before remediation, confirm guest OS and application compatibility, take required backups/snapshots according to policy, then use vSphere Client > Compatibility > Upgrade VM Compatibility or PowerCLI to upgrade to hardware version 19 or later. A VM power cycle may be required.

References:

1. https://knowledge.broadcom.com/external/article/315390
2. https://knowledge.broadcom.com/external/article?legacyId=2007240

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.	●	●	●
v7	18.3 Verify That Acquired Software is Still Supported Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		●	●

Internal Only - General

8 VMware Tools

Internal Only - General

8.1 VMware Tools must be a version that has not reached End of General Support status (Manual)

Profile Applicability:

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

Description:

Ensuring VMware Tools is running a version that has not reached its End of General Support (EOGS) status is imperative for maintaining a secure and supported environment. A version within its support period guarantees regular updates, security patches, and vendor support. It's advisable to have a procedure in place for regular checking and updating of VMware Tools to a supported version.

Rationale:

Running a supported version of VMware Tools ensures that the environment benefits from the latest security patches and updates, thereby reducing the risk of vulnerabilities. It also ensures that the organization can receive necessary support from the vendor when needed.

Impact:

Using a version of VMware Tools that has reached its EOGS can expose the environment to security risks due to lack of updates and patches. It also may lead to compliance issues and lack of vendor support which could result in operational inefficiencies.

Audit:

Within each applicable guest operating system, execute `VMwareToolboxCmd.exe -v`. Compare the installed VMware Tools version to Broadcom lifecycle/support information and verify it has not reached End of General Support.

Remediation:

To remediate this recommendation, upgrade VMware Tools to a supported release using vSphere, the guest package manager/open-vm-tools, or an enterprise software deployment tool. Reboot the guest if required and verify the installed version.

References:

1. https://knowledge.broadcom.com/external/article/415766
2. https://knowledge.broadcom.com/external/article/392913

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

8.2 VMware Tools must have all software updates installed (Manual)

Profile Applicability:

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

Description:

Ensuring that all software updates are installed on VMware Tools is crucial for maintaining a healthy and secure virtual environment. These updates provide essential drivers, enable effective management of guest operating systems, and offer features necessary for VM deployment and customization. It's vital to run a supported version compatible with the guest OS, be it Linux or Microsoft Windows, and keep it updated to benefit from the latest enhancements and security patches.

Rationale:

Keeping VMware Tools updated ensures that the virtual machines are running efficiently with the latest drivers and features, which in turn supports operational effectiveness. Additionally, updated software mitigates potential security risks, ensuring a more secure environment.

Impact:

Neglecting to update VMware Tools could result in outdated drivers, lack of new features, and potential security vulnerabilities, which may hinder the performance and security of the virtual environment.

Audit:

Determine the installed VMware Tools version in each guest and compare it with the current approved security/update baseline. Review Broadcom security advisories for fixes applicable to that Tools release.

Remediation:

To remediate this recommendation, install all approved VMware Tools updates using vSphere, open-vm-tools packages, or enterprise endpoint management. Reboot if required and verify the post-update version.

References:

1. https://knowledge.broadcom.com/external/article/392913
2. https://knowledge.broadcom.com/external/article/415766

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

Internal Only - General

8.3 VMware Tools should configure automatic upgrades as appropriate for the environment (Manual)

Profile Applicability:

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

Description:

Automatic upgrades of VMware Tools can be managed via vSphere, ensuring VMware Tools versions remain current. This functionality is advisable unless alternative management and update mechanisms are in place. It is recommended to have automatic updates enabled to minimize administrative overhead and maintain up-to-date features and security patches. The parameter governing this behavior is autoupgrade allow-upgrade with a recommended setting of true.

Rationale:

Enabling automatic upgrades via vSphere ensures a streamlined process for keeping VMware Tools updated, reducing the administrative burden. It also ensures that VMs are running the latest versions with necessary security patches and updated features.

Impact:

Disabling automatic upgrades necessitates alternative methods for updating and reconfiguring VMware Tools, which could increase administrative overhead and potentially leave VMs with outdated versions, posing security risks and operational inefficiencies.

Audit:

Review each VM's VMware Tools upgrade policy in vSphere (`Edit Settings > VM Options > VMware Tools`) and the guest's package-management policy. Verify that automatic upgrade behavior matches the organization's approved change-management model.

Remediation:

To remediate this recommendation, enable automatic VMware Tools upgrades only where appropriate, or configure a controlled centralized update process. In vSphere select the approved 'check and upgrade Tools during power cycling' behavior as appropriate for the environment.

References:

1. https://knowledge.broadcom.com/external/article/392913
2. https://knowledge.broadcom.com/external/article/413891

Internal Only - General

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

Internal Only - General

8.4 VMware Tools on deployed virtual machines must prevent being recustomized (Manual)

Profile Applicability:

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

Description:

Preventing re-customization of deployed virtual machines is essential to mitigate the risk of adversarial access through cloning and subsequent customization. Once a VM is deployed, it should be safeguarded against further customization to maintain the integrity of its configurations and data. The parameter governing this behavior is deployPkg enable-customization with a recommended setting of false.

Rationale:

This control mitigates the risk of unauthorized access and potential data exposure that may arise from cloning and re-customizing a VM. By adhering to this control, organizations uphold the integrity and security of deployed virtual machines.

Impact:

Disabling re-customization on deployed VMs may affect disaster recovery processes that necessitate IP address modifications. Such processes, facilitated by VMware Site Recovery Manager or VMware Cloud Disaster Recovery, will require alternative strategies for IP address management in recovery scenarios.

Audit:

Review VMware Tools guest customization settings on deployed VMs and verify deployed systems cannot be unexpectedly recustomized. Do not apply this control to templates where customization is intentionally required.

Remediation:

To remediate this recommendation, disable post-deployment recustomization using the VMware Tools configuration supported for the guest OS and environment. Test provisioning/customization workflows first and retain customization capability only on approved templates or build images.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

8.5 VMware Tools must limit the automatic addition of features (Manual)

Profile Applicability:

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

Description:

Limit the automatic addition of features during VMware Tools upgrade processes to maintain the desired security profile of the guest operating system from vSphere. This control can be managed by setting the configuration parameter to a specified value. The parameter governing this behavior is autoupgrade allow-add-feature with a recommended setting of false.

Rationale:

Restricting the automatic addition of features through VMware Tools upgrade processes helps in preserving the security configurations and minimizes the potential introduction of vulnerabilities.

Impact:

With this control enforced, administrators will need to employ alternative methods to update and reconfigure VMware Tools as required, which might necessitate additional administrative effort and oversight.

Audit:

Review VMware Tools configuration for automatic feature installation. Verify that automatic addition of optional Tools features is disabled or restricted unless explicitly required by the guest's management design.

Remediation:

To remediate this recommendation, configure VMware Tools so optional features are not automatically added during reconfiguration/upgrade. Use the supported vmware-toolbox-cmd config set/Windows VMwareToolboxCmd.exe config set mechanism or enterprise deployment package and document required exceptions.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf
2. https://knowledge.broadcom.com/external/article/413891

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

8.6 VMware Tools must limit the automatic removal of features (Manual)

Profile Applicability:

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

Description:

Limiting the automatic removal of features by VMware Tools during upgrade processes is crucial to maintain the intended security profile of the guest OS from vSphere. The automatic upgrade could potentially remove essential features, impacting the security posture inadvertently. The parameter governing this behavior is autoupgrade allow-remove-feature with a recommended setting of false.

Rationale:

Restricting automatic removal of features ensures that the security configurations and other essential features remain intact during upgrades, thus maintaining a consistent security posture.

Impact:

With this control, administrators would need to employ alternative methods for updating and reconfiguring VMware Tools, which might necessitate additional administrative effort.

Audit:

Review VMware Tools configuration for automatic feature removal. Verify that features are not automatically removed unless the behavior is explicitly approved.

Remediation:

To remediate this recommendation, configure VMware Tools to prevent automatic removal of installed features during reconfiguration/upgrade unless required. Apply the guest-OS-specific VMware Tools configuration and validate application dependencies.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

Internal Only - General

8.7 VMware Tools must deactivate GlobalConf unless required (Manual)

Profile Applicability:

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

Description:

The GlobalConf feature within VMware Tools facilitates the delivery of tools.conf configurations to virtual machines, simplifying configuration management. However, if not necessary, it's advisable to deactivate this feature to reduce potential security risks. The parameter governing this behavior is globalconf enabled with a recommended setting of false.

Rationale:

Deactivating GlobalConf minimizes the attack surface by reducing the number of channels through which configurations can be pushed to virtual machines, hence enhancing security.

Impact:

With GlobalConf deactivated, administrators would need to employ alternative methods for updating and reconfiguring VMware Tools, which might require additional steps or tools.

Audit:

Within the guest operating system

1. Execute `VMwareToolboxCmd.exe config get globalconf enabled```. Unless required, verify the value is false.

Remediation:

To remediate this recommendation, execute VMwareToolboxCmd.exe equivalent. Restart VMware Tools if required and verify the setting.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	9.1 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

8.8 VMware Tools must deactivate ContainerInfo unless required (Manual)

Profile Applicability:

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

Description:

Deactivating the ContainerInfo plugin within VMware Tools is advised unless its functionality is required. This plugin collects data on running containers within a Linux guest operating system. The parameter governing this behavior is containerinfo poll-interval with a recommended setting of 0.

Rationale:

Restricting unnecessary data collection is a prudent practice to minimize potential security risks, and to comply with least privilege principles.

Impact:

Disabling ContainerInfo could affect certain products and services within the VMware ecosystem that rely on this functionality, necessitating other configurations or methods to obtain the required container information.

Audit:

Within the guest operating system, execute vmware-toolbox-cmd config get containerinfo poll-interval (or the Windows executable where applicable). Unless required, verify the polling interval is 0.

Remediation:

To remediate this recommendation, execute vmware-toolbox-cmd config set containerinfo poll-interval 0 (or VMwareToolboxCmd.exe on Windows where supported). Restart Tools if required and verify the plugin no longer gathers container information.

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	9.1 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

8.9 VMware Tools must deactivate Appinfo information gathering unless required (Manual)

Profile Applicability:

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

Description:

Deactivating the Appinfo module, unless necessary, through VMware Tools is a prudent measure to minimize the attack surface. This module is designed for application discovery, but if not in use, it should be disabled. The parameter governing this behavior is appinfo disabled with a recommended setting of true.

Rationale:

By deactivating the Appinfo module when not in use, potential vectors for unauthorized access or data leakage can be reduced.

Impact:

Disabling Appinfo may affect products and services within the VMware ecosystem that depend on this functionality, necessitating alternative configurations or solutions to retain those capabilities.

Audit:

Within the guest operating system, execute `vmware-toolbox-cmd config get appinfo disabled` (or the Windows executable). Unless application discovery is required, verify the value is `true`.

Remediation:

To remediate this recommendation, execute `vmware-toolbox-cmd config set appinfo disabled true` or the Windows equivalent. Restart Tools if required and verify AppInfo collection is disabled.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	9.1 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

8.10 VMware Tools must deactivate Guest Store Upgrade operations unless required (Manual)

Profile Applicability:

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

Description:

The GuestStore feature facilitates the distribution of specific content to multiple guests. If not required, it is advisable to disable this plugin to minimize potential attack vectors. The parameter governing this behavior is gueststoreupgrade policy with a recommended setting of off.

Rationale:

Minimizing the attack surface by disabling unnecessary features is a prudent security measure. This control aids in reducing potential exposure points in the system.

Impact:

Deactivating Guest Store Upgrade operations may affect certain products and services within the VMware ecosystem that rely on this functionality, necessitating alternative configurations or methods to maintain required operational capabilities.

Audit:

Within the guest operating system, execute `vmware-toolbox-cmd config get gueststoreupgrade policy` (or VMwareToolboxCmd.exe). Unless required, verify the value is `off`.

Remediation:

To remediate this recommendation, execute vmware-toolbox-cmd config set gueststoreupgrade policy off or the Windows equivalent. Restart VMware Tools if required and verify the setting.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	9.1 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

8.11 VMware Tools must deactivate Service Discovery unless required (Manual)

Profile Applicability:

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

Description:

The VMware Tools Service Discovery plugin is designed to connect to Aria Operations, furnishing it with additional data concerning guests and workloads. Disabling this plugin, when not in use, is a prudent step to diminish the attack surface. The parameter governing this behavior is servicediscovery disabled with a recommended setting of true.

Rationale:

Reducing the attack surface by disabling non-essential features is a fundamental security best practice. This control assists in minimizing potential exposure points, especially when the Service Discovery feature is not in use.

Impact:

Disabling Service Discovery may affect certain products and services within the VMware ecosystem dependent on this functionality, necessitating alternative configurations or methods to retain required operational capabilities.

Audit:

Within the guest operating system, execute vmware-toolbox-cmd config get servicediscovery disabled (or VMwareToolboxCmd.exe). Unless Service Discovery is required, verify the value is true.

Remediation:

To remediate this recommendation, execute `vmware-toolbox-cmd config set servicediscovery disabled true` or the Windows equivalent. Restart VMware Tools if required and verify the plugin is disabled.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	9.1 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

8.12 VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools (Manual)

Profile Applicability:

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

Description:

Limiting the use of MSI transforms during VMware Tools reconfiguration is crucial to prevent unintended alterations to the installation database on Microsoft Windows guest operating systems from vSphere. This control is managed through a specific configuration parameter. The parameter governing this behavior is autoupgrade allow-msi-transforms with a recommended setting of false.

Rationale:

By restricting the use of MSI transforms, organizations can maintain a consistent security profile of the guest OS and minimize risks associated with unintended configuration changes during VMware Tools reconfiguration.

Impact:

Implementing this control will necessitate administrators to leverage alternative methods for updating and reconfiguring VMware Tools as required, which may demand additional administrative effort and oversight.

Audit:

On applicable Windows guests, execute `VMwareToolboxCmd.exe config get autoupgrade allow-msi-transforms`. Verify that the value is false. Treat this control as not applicable to non-Windows guests that do not use MSI.

Remediation:

To remediate this recommendation, execute VMwareToolboxCmd.exe config set autoupgrade allow-msi-transforms false. Restart VMware Tools if required and verify the value remains false.

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	9.1 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

8.13 VMware Tools must enable VMware Tools logging (Manual)

Profile Applicability:

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

Description:

Enable logging within VMware Tools to ensure the collection of pertinent information, facilitating diagnostic or forensic activities. Logging within VMware Tools is highly customizable, allowing for tailored logging setups. The parameter governing this behavior is logging log with a recommended setting of true.

Rationale:

Logging is crucial for diagnosing issues and understanding system interactions. It provides a clear trail of events, aiding in the identification and rectification of potential problems.

Impact:

There is no known negative functional impact from enabling VMware Tools logging. This control solely promotes the capture of essential data for diagnostics and analysis.

Audit:

Review VMware Tools logging configuration inside the guest using vmware-toolbox-cmd config get logging log / the applicable tools.conf settings. Verify that Tools logging is enabled and produces expected log records.

Remediation:

Enable VMware Tools logging using the guest's supported tools.conf/vmware-toolbox-cmd config set mechanism. Restart the VMware Tools service if required and verify log generation.

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.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

Internal Only - General

8.14 VMware Tools must send VMware Tools logs to the system log service (Manual)

Profile Applicability:

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

Description:

Adjusting the logging destination in VMware Tools from the default file on disk to system log services streamlines log management. It redirects logs to syslog on Linux guests and the Windows Event Service on Microsoft Windows guests for centralized monitoring, management, and archiving. The parameter governing this behavior is logging vmsvc.handler with a recommended setting of syslog.

Rationale:

Centralizing log management through system log services enhances monitoring and archival processes. It also fosters a more structured approach to analyzing log data which is crucial for troubleshooting and compliance purposes.

Impact:

Processes dependent on log files in the default location may require modifications to function correctly with the new logging setup, necessitating updates to ensure proper operation and log data retrieval.

Audit:

Review VMware Tools logging destination and verify Tools messages are sent to the guest operating system's system logging facility (syslog/journald on Linux or the approved Windows logging mechanism) rather than only to an unmanaged local file.

Remediation:

To remediate this recommendation, configure VMware Tools logging to use the system log service for the guest OS. Restart VMware Tools if required and verify a test Tools event reaches the system log.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

Internal Only - General

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.		●	●
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

8.15 VMware Tools must deactivate Guest Operations unless required (Manual)

Profile Applicability:

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

Description:

Guest Operations are a set of functions that underpin most host-to-guest interaction. Deactivating them reduces attack surface but also drastically reduces functionality. Ensure that your environment does not require these functions. Do not do this on template VMs. For a list of functions see:

https://vdc-download.vmware.com/vmwb-repository/dcr-public/fe08899f-1eec-4d8d-b3bc-a6664c168c2c/7fdf97a1-4c0d-4be0-9d43-2ceebbc174d9/doc/vim.vm.guest.GuestOperationsManager.html

Rationale:

Reducing the attack surface by deactivating unnecessary functions is a standard security measure. This control is crucial for mitigating risks associated with host-to-guest interactions.

Impact:

Deactivation of Guest Operations can hinder the functionality of certain products and services within the VMware ecosystem, requiring alternative configurations or methods to maintain required functionalities. This includes guest customization.

Audit:

Within the guest operating system, execute vmware-toolbox-cmd config get guestoperations disabled (or VMwareToolboxCmd.exe). Unless Guest Operations is required, verify the value is true. Do not treat templates requiring guest customization as automatically noncompliant without reviewing the operational need.

Remediation:

To remediate this recommendation, execute vmware-toolbox-cmd config set guestoperations disabled true or VMwareToolboxCmd.exe config set guestoperations disabled true. Restart VMware Tools if required and test dependent workflows such as guest customization, backup, automation, and orchestration.

References:

1. https://github.com/vmware/open-vm-tools/blob/master/open-vm-tools/tools.conf

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	9.1 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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Hardware**		
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware (Manual)	☐	☐
1.2	Host hardware must enable UEFI Secure Boot (Manual)	☐	☐
1.3	Host hardware must enable Intel TXT, if available (Manual)	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0 (Manual)	☐	☐
1.5	Host integrated hardware management controller must be secure (Manual)	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization (Manual)	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events (Manual)	☐	☐
1.8	Host integrated hardware management controller must secure authentication (Manual)	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available (Manual)	☐	☐
1.10	Host hardware must enable Intel SGX, if available (Manual)	☐	☐
1.11	Host hardware must secure unused external hardware ports (Manual)	☐	☐
1.12	Host integrated hardware management controller must deactivate internal networking (Manual)	☐	☐
2	**Base**		

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1	Host must run software that has not reached End of General Support status (Manual)	☐	☐
2.2	Host must have all software updates installed (Manual)	☐	☐
2.3	Host must enable Secure Boot enforcement (Manual)	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher (Automated)	☐	☐
2.5	Host must only run binaries delivered via signed VIB (Manual)	☐	☐
2.6	Host must have reliable time synchronization sources (Automated)	☐	☐
2.7	Host must have time synchronization services enabled and running (Manual)	☐	☐
2.8	Host must require TPM-based configuration encryption (Manual)	☐	☐
2.9	Host must not suppress warnings about unmitigated hyperthreading vulnerabilities (Manual)	☐	☐
2.10	Host must restrict inter-VM transparent page sharing (Automated)	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations (Manual)	☐	☐
2.12	Host must enable volatile key destruction (Manual)	☐	☐
3	**Management**		
3.1	Host should deactivate SSH (Automated)	☐	☐
3.2	Host must deactivate the ESXi shell (Automated)	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB) (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4	Host must deactivate SLP (Manual)	☐	☐
3.5	Host must deactivate CIM (Manual)	☐	☐
3.6	Host should deactivate SNMP (Manual)	☐	☐
3.7	Host must automatically terminate idle DCUI sessions (Automated)	☐	☐
3.8	Host must automatically terminate idle shells (Automated)	☐	☐
3.9	Host must automatically deactivate shell services (Automated)	☐	☐
3.10	Host must not suppress warnings that the shell is enabled (Manual)	☐	☐
3.11	Host must enforce password complexity (Manual)	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts (Automated)	☐	☐
3.13	Host must unlock accounts after a specified timeout period (Automated)	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords (Manual)	☐	☐
3.15	Host must be configured with an appropriate maximum password age (Manual)	☐	☐
3.16	Host must configure a session timeout for the API (Manual)	☐	☐
3.17	Host must automatically terminate idle host client sessions (Manual)	☐	☐
3.18	Host must have an accurate DCUI.Access list (Manual)	☐	☐
3.19	Host must have an accurate Exception Users list (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.20	Host must enable lockdown mode (Automated)	☐	☐
3.21	Host should enable strict lockdown mode (Automated)	☐	☐
3.22	Host must deny shell access for the dcui account (Manual)	☐	☐
3.23	Host must deny shell access for the vpxuser account (Manual)	☐	☐
3.24	Host must display a login banner for the DCUI and Host Client (Manual)	☐	☐
3.25	Host must display a login banner for SSH connections (Manual)	☐	☐
3.26	Host must enable the highest version of TLS supported (Manual)	☐	☐
4	**Logging**		
4.1	Host must configure a persistent log location for all locally stored system logs (Manual)	☐	☐
4.2	Host must transmit system logs to a remote log collector (Automated)	☐	☐
4.3	Host must log sufficient information for events (Manual)	☐	☐
4.4	Host must set the logging informational level to info (Manual)	☐	☐
4.5	Host must deactivate log filtering (Manual)	☐	☐
4.6	Host must enable audit record logging (Manual)	☐	☐
4.7	Host must configure a persistent log location for all locally stored audit records (Manual)	☐	☐
4.8	Host must store one week of audit records (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.9	Host must transmit audit records to a remote log collector (Manual)	☐	☐
4.10	Host must verify certificates for TLS remote logging endpoints (Manual)	☐	☐
4.11	Host must use strict x509 verification for TLS-enabled remote logging endpoints (Manual)	☐	☐
5	**Network**		
5.1	Host firewall must only allow traffic from authorized networks (Manual)	☐	☐
5.2	Host must block network traffic by default (Manual)	☐	☐
5.3	Host must restrict use of the dvFilter network API (Manual)	☐	☐
5.4	Host must filter Bridge Protocol Data Unit (BPDU) packets (Manual)	☐	☐
5.5	Host should deactivate virtual hardware management network interfaces (Manual)	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups (Automated)	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups (Automated)	☐	☐
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups (Automated)	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches (Automated)	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches (Automated)	☐	☐
5.11	Host must isolate management communications (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6	**Features**		
6.1	**CIM**		
6.1.1	Host CIM services, if enabled, must limit access (Manual)	☐	☐
6.2	**Core Storage**		
6.2.1	Host must isolate storage communications (Manual)	☐	☐
6.2.2	Host must ensure all datastores have unique names (Manual)	☐	☐
6.3	**iSCSI**		
6.3.1	Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication (Automated)	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets (Manual)	☐	☐
6.4	**SNMP**		
6.4.1	Host SNMP services, if enabled, must limit access (Manual)	☐	☐
6.5	**SSH**		
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers (Manual)	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules (Manual)	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports (Manual)	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions (Manual)	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions (Manual)	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access (Manual)	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files (Manual)	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding (Manual)	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding (Manual)	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels (Manual)	☐	☐
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings (Manual)	☐	☐
7	**Virtual Machine**		
7.1	Virtual machines must enable Secure Boot (Manual)	☐	☐
7.2	Virtual machines must require encryption for vMotion (Manual)	☐	☐
7.3	Virtual machines must require encryption for Fault Tolerance (Manual)	☐	☐
7.4	Virtual machines should deactivate 3D graphics features when not required (Automated)	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed (Manual)	☐	☐
7.6	Virtual machines must limit console sharing. (Automated)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.7	Virtual machines must limit PCI/PCIe device passthrough functionality (Automated)	☐	☐
7.8	Ensure unauthorized modification and disconnection of devices is disabled (Automated)	☐	☐
7.9	Virtual machines must prevent unauthorized connection of devices (Automated)	☐	☐
7.10	Virtual machines must remove unnecessary audio devices (Manual)	☐	☐
7.11	Virtual machines must remove unnecessary AHCI devices (Manual)	☐	☐
7.12	Virtual machines must remove unnecessary USB/XHCI devices (Automated)	☐	☐
7.13	Virtual machines must remove unnecessary serial port devices (Automated)	☐	☐
7.14	Virtual machines must remove unnecessary parallel port devices (Automated)	☐	☐
7.15	Virtual machines must remove unnecessary CD/DVD devices (Automated)	☐	☐
7.16	Virtual machines must remove unnecessary floppy devices (Automated)	☐	☐
7.17	Virtual machines must deactivate console drag and drop operations (Automated)	☐	☐
7.18	Virtual machines must deactivate console copy operations (Automated)	☐	☐
7.19	Virtual machines must deactivate console paste operations (Automated)	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.21	Virtual machines must deactivate virtual disk shrinking operations (Automated)	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations (Automated)	☐	☐
7.23	Virtual machines must restrict sharing of memory pages with other VMs (Manual)	☐	☐
7.24	Virtual machines must not be able to obtain host information from the hypervisor (Automated)	☐	☐
7.25	Virtual machines must enable diagnostic logging (Manual)	☐	☐
7.26	Virtual machines must limit the number of retained diagnostic logs (Automated)	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs (Automated)	☐	☐
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file (Manual)	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer (Manual)	☐	☐
8	**VMware Tools**		
8.1	VMware Tools must be a version that has not reached End of General Support status (Manual)	☐	☐
8.2	VMware Tools must have all software updates installed (Manual)	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment (Manual)	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized (Manual)	☐	☐

Internal Only - General

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.5	VMware Tools must limit the automatic addition of features (Manual)	☐	☐
8.6	VMware Tools must limit the automatic removal of features (Manual)	☐	☐
8.7	VMware Tools must deactivate GlobalConf unless required (Manual)	☐	☐
8.8	VMware Tools must deactivate ContainerInfo unless required (Manual)	☐	☐
8.9	VMware Tools must deactivate Appinfo information gathering unless required (Manual)	☐	☐
8.10	VMware Tools must deactivate Guest Store Upgrade operations unless required (Manual)	☐	☐
8.11	VMware Tools must deactivate Service Discovery unless required (Manual)	☐	☐
8.12	VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools (Manual)	☐	☐
8.13	VMware Tools must enable VMware Tools logging (Manual)	☐	☐
8.14	VMware Tools must send VMware Tools logs to the system log service (Manual)	☐	☐
8.15	VMware Tools must deactivate Guest Operations unless required (Manual)	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐
3.9	Host must automatically deactivate shell services	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
6.1.1	Host CIM services, if enabled, must limit access	☐	☐
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐

Internal Only - General

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.2	Host hardware must enable UEFI Secure Boot	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0	☐	☐
1.5	Host integrated hardware management controller must be secure	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
1.11	Host hardware must secure unused external hardware ports	☐	☐
1.12	Host integrated hardware management controller must deactivate internal networking	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.6	Host must have reliable time synchronization sources	☐	☐
2.7	Host must have time synchronization services enabled and running	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.9	Host must not suppress warnings about unmitigated hyperthreading vulnerabilities	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.1	Host should deactivate SSH	☐	☐
3.2	Host must deactivate the ESXi shell	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.4	Host must deactivate SLP	☐	☐
3.5	Host must deactivate CIM	☐	☐
3.6	Host should deactivate SNMP	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐
3.9	Host must automatically deactivate shell services	☐	☐
3.10	Host must not suppress warnings that the shell is enabled	☐	☐
3.11	Host must enforce password complexity	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords	☐	☐
3.15	Host must be configured with an appropriate maximum password age	☐	☐
3.16	Host must configure a session timeout for the API	☐	☐
3.17	Host must automatically terminate idle host client sessions	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐
3.20	Host must enable lockdown mode	☐	☐
3.21	Host should enable strict lockdown mode	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
4.3	Host must log sufficient information for events	☐	☐
4.4	Host must set the logging informational level to info	☐	☐
4.5	Host must deactivate log filtering	☐	☐
4.6	Host must enable audit record logging	☐	☐
4.7	Host must configure a persistent log location for all locally stored audit records	☐	☐
4.8	Host must store one week of audit records	☐	☐
4.9	Host must transmit audit records to a remote log collector	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.3	Host must restrict use of the dvFilter network API	☐	☐
5.4	Host must filter Bridge Protocol Data Unit (BPDU) packets	☐	☐
5.5	Host should deactivate virtual hardware management network interfaces	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
6.1.1	Host CIM services, if enabled, must limit access	☐	☐
6.2.1	Host must isolate storage communications	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
6.3.1	Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets	☐	☐
6.4.1	Host SNMP services, if enabled, must limit access	☐	☐
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐
7.2	Virtual machines must require encryption for vMotion	☐	☐
7.3	Virtual machines must require encryption for Fault Tolerance	☐	☐
7.4	Virtual machines should deactivate 3D graphics features when not required	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.6	Virtual machines must limit console sharing.	☐	☐
7.7	Virtual machines must limit PCI/PCIe device passthrough functionality	☐	☐
7.8	Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
7.9	Virtual machines must prevent unauthorized connection of devices	☐	☐
7.10	Virtual machines must remove unnecessary audio devices	☐	☐
7.11	Virtual machines must remove unnecessary AHCI devices	☐	☐
7.12	Virtual machines must remove unnecessary USB/XHCI devices	☐	☐
7.13	Virtual machines must remove unnecessary serial port devices	☐	☐
7.14	Virtual machines must remove unnecessary parallel port devices	☐	☐
7.15	Virtual machines must remove unnecessary CD/DVD devices	☐	☐
7.16	Virtual machines must remove unnecessary floppy devices	☐	☐
7.17	Virtual machines must deactivate console drag and drop operations	☐	☐
7.18	Virtual machines must deactivate console copy operations	☐	☐
7.19	Virtual machines must deactivate console paste operations	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations	☐	☐
7.23	Virtual machines must restrict sharing of memory pages with other VMs	☐	☐
7.25	Virtual machines must enable diagnostic logging	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.26	Virtual machines must limit the number of retained diagnostic logs	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs	☐	☐
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.5	VMware Tools must limit the automatic addition of features	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.7	VMware Tools must deactivate GlobalConf unless required	☐	☐
8.8	VMware Tools must deactivate ContainerInfo unless required	☐	☐
8.9	VMware Tools must deactivate Appinfo information gathering unless required	☐	☐
8.10	VMware Tools must deactivate Guest Store Upgrade operations unless required	☐	☐
8.11	VMware Tools must deactivate Service Discovery unless required	☐	☐
8.12	VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐
8.14	VMware Tools must send VMware Tools logs to the system log service	☐	☐
8.15	VMware Tools must deactivate Guest Operations unless required	☐	☐

Internal Only - General

Internal Only - General

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.2	Host hardware must enable UEFI Secure Boot	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0	☐	☐
1.5	Host integrated hardware management controller must be secure	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
1.11	Host hardware must secure unused external hardware ports	☐	☐
1.12	Host integrated hardware management controller must deactivate internal networking	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.6	Host must have reliable time synchronization sources	☐	☐
2.7	Host must have time synchronization services enabled and running	☐	☐
2.8	Host must require TPM-based configuration encryption	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.9	Host must not suppress warnings about unmitigated hyperthreading vulnerabilities	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.1	Host should deactivate SSH	☐	☐
3.2	Host must deactivate the ESXi shell	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.4	Host must deactivate SLP	☐	☐
3.5	Host must deactivate CIM	☐	☐
3.6	Host should deactivate SNMP	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐
3.9	Host must automatically deactivate shell services	☐	☐
3.10	Host must not suppress warnings that the shell is enabled	☐	☐
3.11	Host must enforce password complexity	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords	☐	☐
3.15	Host must be configured with an appropriate maximum password age	☐	☐
3.16	Host must configure a session timeout for the API	☐	☐
3.17	Host must automatically terminate idle host client sessions	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐
3.20	Host must enable lockdown mode	☐	☐
3.21	Host should enable strict lockdown mode	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.22	Host must deny shell access for the dcui account	☐	☐
3.23	Host must deny shell access for the vpxuser account	☐	☐
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
3.26	Host must enable the highest version of TLS supported	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
4.3	Host must log sufficient information for events	☐	☐
4.4	Host must set the logging informational level to info	☐	☐
4.5	Host must deactivate log filtering	☐	☐
4.6	Host must enable audit record logging	☐	☐
4.7	Host must configure a persistent log location for all locally stored audit records	☐	☐
4.8	Host must store one week of audit records	☐	☐
4.9	Host must transmit audit records to a remote log collector	☐	☐
4.10	Host must verify certificates for TLS remote logging endpoints	☐	☐
4.11	Host must use strict x509 verification for TLS-enabled remote logging endpoints	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.2	Host must block network traffic by default	☐	☐
5.3	Host must restrict use of the dvFilter network API	☐	☐
5.4	Host must filter Bridge Protocol Data Unit (BPDU) packets	☐	☐
5.5	Host should deactivate virtual hardware management network interfaces	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
5.11	Host must isolate management communications	☐	☐
6.1.1	Host CIM services, if enabled, must limit access	☐	☐
6.2.1	Host must isolate storage communications	☐	☐
6.2.2	Host must ensure all datastores have unique names	☐	☐
6.3.1	Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets	☐	☐
6.4.1	Host SNMP services, if enabled, must limit access	☐	☐
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐
7.2	Virtual machines must require encryption for vMotion	☐	☐
7.3	Virtual machines must require encryption for Fault Tolerance	☐	☐
7.4	Virtual machines should deactivate 3D graphics features when not required	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed	☐	☐
7.6	Virtual machines must limit console sharing.	☐	☐
7.7	Virtual machines must limit PCI/PCIe device passthrough functionality	☐	☐
7.8	Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
7.9	Virtual machines must prevent unauthorized connection of devices	☐	☐
7.10	Virtual machines must remove unnecessary audio devices	☐	☐
7.11	Virtual machines must remove unnecessary AHCI devices	☐	☐
7.12	Virtual machines must remove unnecessary USB/XHCI devices	☐	☐
7.13	Virtual machines must remove unnecessary serial port devices	☐	☐
7.14	Virtual machines must remove unnecessary parallel port devices	☐	☐
7.15	Virtual machines must remove unnecessary CD/DVD devices	☐	☐
7.16	Virtual machines must remove unnecessary floppy devices	☐	☐
7.17	Virtual machines must deactivate console drag and drop operations	☐	☐
7.18	Virtual machines must deactivate console copy operations	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.19	Virtual machines must deactivate console paste operations	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations	☐	☐
7.23	Virtual machines must restrict sharing of memory pages with other VMs	☐	☐
7.24	Virtual machines must not be able to obtain host information from the hypervisor	☐	☐
7.25	Virtual machines must enable diagnostic logging	☐	☐
7.26	Virtual machines must limit the number of retained diagnostic logs	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs	☐	☐
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.5	VMware Tools must limit the automatic addition of features	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.7	VMware Tools must deactivate GlobalConf unless required	☐	☐
8.8	VMware Tools must deactivate ContainerInfo unless required	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.9	VMware Tools must deactivate Appinfo information gathering unless required	☐	☐
8.10	VMware Tools must deactivate Guest Store Upgrade operations unless required	☐	☐
8.11	VMware Tools must deactivate Service Discovery unless required	☐	☐
8.12	VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐
8.14	VMware Tools must send VMware Tools logs to the system log service	☐	☐
8.15	VMware Tools must deactivate Guest Operations unless required	☐	☐

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	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0	☐	☐
1.5	Host integrated hardware management controller must be secure	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.9	Host must automatically deactivate shell services	☐	☐
3.11	Host must enforce password complexity	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords	☐	☐
3.15	Host must be configured with an appropriate maximum password age	☐	☐
3.16	Host must configure a session timeout for the API	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
4.4	Host must set the logging informational level to info	☐	☐
4.5	Host must deactivate log filtering	☐	☐
4.6	Host must enable audit record logging	☐	☐
4.8	Host must store one week of audit records	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed	☐	☐
7.6	Virtual machines must limit console sharing.	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations	☐	☐
7.24	Virtual machines must not be able to obtain host information from the hypervisor	☐	☐
7.26	Virtual machines must limit the number of retained diagnostic logs	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.2	Host hardware must enable UEFI Secure Boot	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0	☐	☐
1.5	Host integrated hardware management controller must be secure	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
1.11	Host hardware must secure unused external hardware ports	☐	☐
1.12	Host integrated hardware management controller must deactivate internal networking	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.6	Host must have reliable time synchronization sources	☐	☐
2.7	Host must have time synchronization services enabled and running	☐	☐
2.8	Host must require TPM-based configuration encryption	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.9	Host must not suppress warnings about unmitigated hyperthreading vulnerabilities	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.1	Host should deactivate SSH	☐	☐
3.2	Host must deactivate the ESXi shell	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.4	Host must deactivate SLP	☐	☐
3.5	Host must deactivate CIM	☐	☐
3.6	Host should deactivate SNMP	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐
3.9	Host must automatically deactivate shell services	☐	☐
3.11	Host must enforce password complexity	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords	☐	☐
3.15	Host must be configured with an appropriate maximum password age	☐	☐
3.16	Host must configure a session timeout for the API	☐	☐
3.17	Host must automatically terminate idle host client sessions	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐
3.20	Host must enable lockdown mode	☐	☐
3.21	Host should enable strict lockdown mode	☐	☐
3.22	Host must deny shell access for the dcui account	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.23	Host must deny shell access for the vpxuser account	☐	☐
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
3.26	Host must enable the highest version of TLS supported	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
4.3	Host must log sufficient information for events	☐	☐
4.4	Host must set the logging informational level to info	☐	☐
4.5	Host must deactivate log filtering	☐	☐
4.6	Host must enable audit record logging	☐	☐
4.7	Host must configure a persistent log location for all locally stored audit records	☐	☐
4.8	Host must store one week of audit records	☐	☐
4.9	Host must transmit audit records to a remote log collector	☐	☐
4.10	Host must verify certificates for TLS remote logging endpoints	☐	☐
4.11	Host must use strict x509 verification for TLS-enabled remote logging endpoints	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.2	Host must block network traffic by default	☐	☐
5.3	Host must restrict use of the dvFilter network API	☐	☐
5.4	Host must filter Bridge Protocol Data Unit (BPDU) packets	☐	☐
5.5	Host should deactivate virtual hardware management network interfaces	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
6.1.1	Host CIM services, if enabled, must limit access	☐	☐
6.2.1	Host must isolate storage communications	☐	☐
6.2.2	Host must ensure all datastores have unique names	☐	☐
6.3.1	Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets	☐	☐
6.4.1	Host SNMP services, if enabled, must limit access	☐	☐
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.2	Virtual machines must require encryption for vMotion	☐	☐
7.3	Virtual machines must require encryption for Fault Tolerance	☐	☐
7.4	Virtual machines should deactivate 3D graphics features when not required	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed	☐	☐
7.6	Virtual machines must limit console sharing.	☐	☐
7.7	Virtual machines must limit PCI/PCIe device passthrough functionality	☐	☐
7.8	Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
7.9	Virtual machines must prevent unauthorized connection of devices	☐	☐
7.10	Virtual machines must remove unnecessary audio devices	☐	☐
7.11	Virtual machines must remove unnecessary AHCI devices	☐	☐
7.12	Virtual machines must remove unnecessary USB/XHCI devices	☐	☐
7.13	Virtual machines must remove unnecessary serial port devices	☐	☐
7.14	Virtual machines must remove unnecessary parallel port devices	☐	☐
7.15	Virtual machines must remove unnecessary CD/DVD devices	☐	☐
7.16	Virtual machines must remove unnecessary floppy devices	☐	☐
7.17	Virtual machines must deactivate console drag and drop operations	☐	☐
7.18	Virtual machines must deactivate console copy operations	☐	☐
7.19	Virtual machines must deactivate console paste operations	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations	☐	☐
7.23	Virtual machines must restrict sharing of memory pages with other VMs	☐	☐
7.24	Virtual machines must not be able to obtain host information from the hypervisor	☐	☐
7.25	Virtual machines must enable diagnostic logging	☐	☐
7.26	Virtual machines must limit the number of retained diagnostic logs	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs	☐	☐
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.5	VMware Tools must limit the automatic addition of features	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.7	VMware Tools must deactivate GlobalConf unless required	☐	☐
8.8	VMware Tools must deactivate ContainerInfo unless required	☐	☐
8.9	VMware Tools must deactivate Appinfo information gathering unless required	☐	☐
8.10	VMware Tools must deactivate Guest Store Upgrade operations unless required	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.11	VMware Tools must deactivate Service Discovery unless required	☐	☐
8.12	VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐
8.14	VMware Tools must send VMware Tools logs to the system log service	☐	☐
8.15	VMware Tools must deactivate Guest Operations unless required	☐	☐

Internal Only - General

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Host hardware must have auditable, authentic, and up to date system & device firmware	☐	☐
1.2	Host hardware must enable UEFI Secure Boot	☐	☐
1.3	Host hardware must enable Intel TXT, if available	☐	☐
1.4	Host hardware must enable and configure a TPM 2.0	☐	☐
1.5	Host integrated hardware management controller must be secure	☐	☐
1.6	Host integrated hardware management controller must enable time synchronization	☐	☐
1.7	Host integrated hardware management controller must enable remote logging of events	☐	☐
1.8	Host integrated hardware management controller must secure authentication	☐	☐
1.9	Host hardware must enable AMD SEV-ES, if available	☐	☐
1.10	Host hardware must enable Intel SGX, if available	☐	☐
1.11	Host hardware must secure unused external hardware ports	☐	☐
1.12	Host integrated hardware management controller must deactivate internal networking	☐	☐
2.1	Host must run software that has not reached End of General Support status	☐	☐
2.2	Host must have all software updates installed	☐	☐
2.3	Host must enable Secure Boot enforcement	☐	☐
2.4	(Host image profile acceptance level must be PartnerSupported or higher	☐	☐
2.5	Host must only run binaries delivered via signed VIB	☐	☐
2.6	Host must have reliable time synchronization sources	☐	☐
2.7	Host must have time synchronization services enabled and running	☐	☐
2.8	Host must require TPM-based configuration encryption	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
2.9	Host must not suppress warnings about unmitigated hyperthreading vulnerabilities	☐	☐
2.10	Host must restrict inter-VM transparent page sharing	☐	☐
2.11	Host must use sufficient entropy for cryptographic operations	☐	☐
2.12	Host must enable volatile key destruction	☐	☐
3.1	Host should deactivate SSH	☐	☐
3.2	Host must deactivate the ESXi shell	☐	☐
3.3	Host must deactivate the ESXi Managed Object Browser (MOB)	☐	☐
3.4	Host must deactivate SLP	☐	☐
3.5	Host must deactivate CIM	☐	☐
3.6	Host should deactivate SNMP	☐	☐
3.7	Host must automatically terminate idle DCUI sessions	☐	☐
3.8	Host must automatically terminate idle shells	☐	☐
3.9	Host must automatically deactivate shell services	☐	☐
3.10	Host must not suppress warnings that the shell is enabled	☐	☐
3.11	Host must enforce password complexity	☐	☐
3.12	Host must lock an account after a specified number of failed login attempts	☐	☐
3.13	Host must unlock accounts after a specified timeout period	☐	☐
3.14	Host must configure the password history setting to restrict the reuse of passwords	☐	☐
3.15	Host must be configured with an appropriate maximum password age	☐	☐
3.16	Host must configure a session timeout for the API	☐	☐
3.17	Host must automatically terminate idle host client sessions	☐	☐
3.18	Host must have an accurate DCUI.Access list	☐	☐
3.19	Host must have an accurate Exception Users list	☐	☐
3.20	Host must enable lockdown mode	☐	☐
3.21	Host should enable strict lockdown mode	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
3.22	Host must deny shell access for the dcui account	☐	☐
3.23	Host must deny shell access for the vpxuser account	☐	☐
3.24	Host must display a login banner for the DCUI and Host Client	☐	☐
3.25	Host must display a login banner for SSH connections	☐	☐
3.26	Host must enable the highest version of TLS supported	☐	☐
4.1	Host must configure a persistent log location for all locally stored system logs	☐	☐
4.2	Host must transmit system logs to a remote log collector	☐	☐
4.3	Host must log sufficient information for events	☐	☐
4.4	Host must set the logging informational level to info	☐	☐
4.5	Host must deactivate log filtering	☐	☐
4.6	Host must enable audit record logging	☐	☐
4.7	Host must configure a persistent log location for all locally stored audit records	☐	☐
4.8	Host must store one week of audit records	☐	☐
4.9	Host must transmit audit records to a remote log collector	☐	☐
4.10	Host must verify certificates for TLS remote logging endpoints	☐	☐
4.11	Host must use strict x509 verification for TLS-enabled remote logging endpoints	☐	☐
5.1	Host firewall must only allow traffic from authorized networks	☐	☐
5.2	Host must block network traffic by default	☐	☐
5.3	Host must restrict use of the dvFilter network API	☐	☐
5.4	Host must filter Bridge Protocol Data Unit (BPDU) packets	☐	☐
5.5	Host should deactivate virtual hardware management network interfaces	☐	☐
5.6	Host should reject forged transmits on standard virtual switches and port groups	☐	☐
5.7	Host should reject MAC address changes on standard virtual switches and port groups	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
5.8	Host should reject promiscuous mode requests on standard virtual switches and port groups	☐	☐
5.9	Host must restrict access to a default or native VLAN on standard virtual switches	☐	☐
5.10	Host must restrict the use of Virtual Guest Tagging (VGT) on standard virtual switches	☐	☐
5.11	Host must isolate management communications	☐	☐
6.1.1	Host CIM services, if enabled, must limit access	☐	☐
6.2.1	Host must isolate storage communications	☐	☐
6.2.2	Host must ensure all datastores have unique names	☐	☐
6.3.1	Host iSCSI client, if enabled, must employ bidirectional/mutual CHAP authentication	☐	☐
6.3.2	Host iSCSI client, if enabled, must employ unique CHAP authentication secrets	☐	☐
6.4.1	Host SNMP services, if enabled, must limit access	☐	☐
6.5.1	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated ciphers	☐	☐
6.5.2	Host SSH daemon, if enabled, must use FIPS 140-2/140-3 validated cryptographic modules	☐	☐
6.5.3	Host SSH daemon, if enabled, must not allow use of gateway ports	☐	☐
6.5.4	Host SSH daemon, if enabled, must not allow host-based authentication	☐	☐
6.5.5	Host SSH daemon, if enabled, must set a timeout count on idle sessions	☐	☐
6.5.6	Host SSH daemon, if enabled, must set a timeout interval on idle sessions	☐	☐
6.5.7	Host SSH daemon, if enabled, must display the system login banner before granting access	☐	☐
6.5.8	Host SSH daemon, if enabled, must ignore .rhosts files	☐	☐
6.5.9	Host SSH daemon, if enabled, must disable stream local forwarding	☐	☐
6.5.10	Host SSH daemon, if enabled, must disable TCP forwarding	☐	☐
6.5.11	Host SSH daemon, if enabled, must not permit tunnels	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
6.5.12	Host SSH daemon, if enabled, must not permit user environment settings	☐	☐
7.1	Virtual machines must enable Secure Boot	☐	☐
7.2	Virtual machines must require encryption for vMotion	☐	☐
7.3	Virtual machines must require encryption for Fault Tolerance	☐	☐
7.4	Virtual machines should deactivate 3D graphics features when not required	☐	☐
7.5	Virtual machines must be configured to lock when the last console connection is closed	☐	☐
7.6	Virtual machines must limit console sharing.	☐	☐
7.7	Virtual machines must limit PCI/PCIe device passthrough functionality	☐	☐
7.8	Ensure unauthorized modification and disconnection of devices is disabled	☐	☐
7.9	Virtual machines must prevent unauthorized connection of devices	☐	☐
7.10	Virtual machines must remove unnecessary audio devices	☐	☐
7.11	Virtual machines must remove unnecessary AHCI devices	☐	☐
7.12	Virtual machines must remove unnecessary USB/XHCI devices	☐	☐
7.13	Virtual machines must remove unnecessary serial port devices	☐	☐
7.14	Virtual machines must remove unnecessary parallel port devices	☐	☐
7.15	Virtual machines must remove unnecessary CD/DVD devices	☐	☐
7.16	Virtual machines must remove unnecessary floppy devices	☐	☐
7.17	Virtual machines must deactivate console drag and drop operations	☐	☐
7.18	Virtual machines must deactivate console copy operations	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
7.19	Virtual machines must deactivate console paste operations	☐	☐
7.20	Virtual machines must limit access through the "dvfilter" network API	☐	☐
7.21	Virtual machines must deactivate virtual disk shrinking operations	☐	☐
7.22	Virtual machines must deactivate virtual disk wiping operations	☐	☐
7.23	Virtual machines must restrict sharing of memory pages with other VMs	☐	☐
7.24	Virtual machines must not be able to obtain host information from the hypervisor	☐	☐
7.25	Virtual machines must enable diagnostic logging	☐	☐
7.26	Virtual machines must limit the number of retained diagnostic logs	☐	☐
7.27	Virtual machines must limit the size of diagnostic logs	☐	☐
7.28	Virtual machines must limit informational messages from the virtual machine to the VMX file	☐	☐
7.29	Virtual machines should have virtual machine hardware version 19 or newer	☐	☐
8.1	VMware Tools must be a version that has not reached End of General Support status	☐	☐
8.2	VMware Tools must have all software updates installed	☐	☐
8.3	VMware Tools should configure automatic upgrades as appropriate for the environment	☐	☐
8.4	VMware Tools on deployed virtual machines must prevent being recustomized	☐	☐
8.5	VMware Tools must limit the automatic addition of features	☐	☐
8.6	VMware Tools must limit the automatic removal of features	☐	☐
8.7	VMware Tools must deactivate GlobalConf unless required	☐	☐
8.8	VMware Tools must deactivate ContainerInfo unless required	☐	☐

Internal Only - General

Recommendation		Set Correctly	
		Yes	No
8.9	VMware Tools must deactivate Appinfo information gathering unless required	☐	☐
8.10	VMware Tools must deactivate Guest Store Upgrade operations unless required	☐	☐
8.11	VMware Tools must deactivate Service Discovery unless required	☐	☐
8.12	VMware Tools must limit the use of MSI transforms when reconfiguring VMware Tools	☐	☐
8.13	VMware Tools must enable VMware Tools logging	☐	☐
8.14	VMware Tools must send VMware Tools logs to the system log service	☐	☐
8.15	VMware Tools must deactivate Guest Operations unless required	☐	☐

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	1.4.0	Updated to support the latest ESXi 8 Update 3j
8/31/2026	1.4.0	Edited remediation for recommendation 3.11. Ticket #21459.
8/31/2026	1.4.0	Updated remediation settings for recommendation 7.16. Ticket # 20313
8/31/2026	1.4.0	Added audit and remediation to recommendations: 1.2, 1.4, 2.1, 2.3, 2.5, 2.7, 2.8, 2.9, 2.11.a, 2.11.b, 2.12, 3.4.a, 3.4.b, 3.5.a, 3.5.b, 3.6, 3.10, 3.15, 3.16, 3.17, 3.22, 3.23, 3.24, 3.25, 3.26, 4.3, 4.4, 4.5, 4.7, 4.8, 4.9, 4.10, 4.11, 5.2.a, 5.2.b, 5.4, 5.5, 5.11, 6.2.2, 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10, 6.5.11, 6.5.12, 7.10, 7.11, 7.23, 7.25, 7.28, 7.29, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12, 8.13, 8.14, and 8.15. Ticket # 27876
8/31/2026	1.4.0	Edited grammar and punctuation in various recommendation
8/31/2026	1.4.0	Recommendation 3.8 remediation has been modified to reflect 300 or less. Ticket # 22202
8/31/2026	1.4.0	Recommendation 3.9 has been updated to reflect new timeout value of 3600. Ticket # 21479

Internal Only - General

Date	Version	Changes for this version
8/31/2026	1.4.0	Changed acceptance level for recommendation 2.4. Ticket #26538
8/31/2026	1.4.0	Updated remediation process for recommendation 7.5 Ticket #23520
8/31/2026	1.4.0	Updated and added URL reference links
2/26/2026	1.3.0	Tested and updated with the latest build: ESXi 8.0.3 P08
2/25/2026	1.3.0	Recommendation 7.13 edited to point to new references Ticket 25424
3/10/2025	1.3.0	Updated links to references for recommendation 7.26 Ticket #25424
3/092025	1.2.0	Tested and updated with the latest build: ESXi 8.0.3 P04
3/1/2024	1.2.0	Validated against latest CIS-CAT version release.
3/1/2024	1.1.0	Tested and updated with the latest build: ESXi 8.0 Update 2b
	1.1.0	Validated against latest CIS-CAT version release.

Internal Only - General

Internal Only - General