CIS Google Container-Optimized OS Benchmark

v1.2.0 - 05-31-2024

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/

Table of Contents

Overview

All CIS 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 for vulnerabilities and quickly updating with the latest security patches.
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches.

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

This document provides prescriptive guidance for establishing a secure posture for Linux systems based on Container-Optimized OS and are running on Google Cloud Platform.
Level-1 recommendations are supported starting from COS-89+.
The guidance within broadly assumes that operations are being performed as the root user. Operations performed using sudo instead of the root user may produce unexpected results, or fail to make the intended changes to the system. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify root users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.
To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/. If you have questions, comments, or have identified ways to improve this guide, please write us at benchmarkinfo@cisecurity.org.

Intended Audience

This benchmark 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 Container-Optimized OS and are running on Google Cloud Platform.

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/.

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).

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.

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.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1 - Server**

  Items in this profile intend to:

  - be practical and prudent;
  - provide security focused best practice hardening of a technology; and
  - limit impact to the utility of the technology beyond acceptable means.

  This profile is intended for servers.

- **Level 2 - Server**

  This profile extends the "Level 1 - Server" 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
  - acts as defense in depth measure
  - may impact the utility or performance of the technology
  - may include additional licensing, cost, or addition of third party software

  This profile is intended for servers.

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:

This benchmark is based upon previous Linux benchmarks published and would not be possible without the contributions provided over the history of all of these benchmarks. The CIS community thanks everyone who has contributed to the Linux benchmarks.

Contributor
Rael Daruszka
Ron Colvin
Bill Erickson
Dave Billing
Dominic Pace
Elliot Anderson
Ely Pinto
Fredrik Silverskär
Joy Latten
Kirill Antonenko
Koen Laevens
Marcelo Cerri
Mark Birch
Martynas Brijunas
Michel Verbraak
Mike Thompson
Pradeep R B
Rakesh Jain
Robert Thomas
Tom Pietschmann
Vineetha Hari Pai
William E. Triest Iii
Anurag Pal
Bradley Hieber
Thomas Sjögren
James Trigg
Matthew Woods
Kenneth Karlsson
Mike Wicks
Anil Altinay
Michael Kochera
Vaibhav Rustagi

Editor
Jonathan Lewis Christopherson
Eric Pinnell

Recommendations

1 Initial Setup

Items in this section are advised for all systems, but may be difficult or require extensive preparation after the initial setup of the system.

1.1 Filesystem Configuration

Directories that are used for system-wide functions can be further protected by placing them on separate partitions. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use. Users' data can be stored on separate partitions and have stricter mount options. A user partition is a filesystem that has been established for use by the users and does not contain software for system operations.

The recommendations in this section are easier to perform during initial system installation. If the system is already installed, it is recommended that a full backup be performed before repartitioning the system.

Note: If you are repartitioning a system that has already been installed, make sure the data has been copied over to the new partition, unmount it and then remove the data from the directory that was in the old partition. Otherwise it will still consume space in the old partition that will be masked when the new filesystem is mounted. For example, if a system is in single-user mode with no filesystems mounted and the administrator adds a lot of data to the `/tmp` directory, this data will still consume space in `/` once the `/tmp` filesystem is mounted unless it is removed first.

1.1.1 Disable unused filesystems

A number of uncommon filesystem types are supported under Linux. Removing support for unneeded filesystem types reduces the local attack surface of the system. If a filesystem type is not needed it should be disabled. Native Linux file systems are designed to ensure that built-in security controls function as expected. Non-native filesystems can lead to unexpected consequences to both the security and functionality of the system and should be used with caution. Many filesystems are created for niche use cases and are not maintained and supported as the operating systems are updated and patched. Users of non-native filesystems should ensure that there is attention and ongoing support for them, especially in light of frequent operating system changes.

Standard network connectivity and Internet access to cloud storage may make the use of non-standard filesystem formats to directly attach heterogeneous devices much less attractive.

Note: This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment.

1.1.1.1 Ensure mounting of udf filesystems is disabled (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `udf` filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats.

Rationale:

Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Audit:

Run the following commands and verify the output is as indicated:

```
# modprobe -n -v udf
install /bin/true
# lsmod | grep udf
<No output>
```

Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in .conf
Example: `vim /etc/modprobe.d/udf.conf`
and add the following line:

```
install udf /bin/true
```

Run the following command to unload the `udf` module:

```
# rmmod udf
```

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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.5** <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		●	●
v7	**3.3** <u>Protect Dedicated Assessment Accounts</u> Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●

1.1.2 Ensure /tmp is configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/tmp` directory is a world-writable directory used for temporary storage by all users and some applications.

Rationale:

Making /tmp its own file system allows an administrator to set the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Impact:

Since the `/tmp` directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.

Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily.

/tmp utilizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Audit:

Run the following command and verify output shows `/tmp` is mounted:

```
# mount | grep -E '\s/tmp\s'
tmpfs on /tmp type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Run the following command and verify that output shows `static`

```
# systemctl is-enabled tmp.mount
static
```

Remediation:

Run the following commands to configure mount options

```
systemctl edit tmp.mount
```

Edit the file to define the options that needs to be set. For example:

```
[Mount]
Options=
Options=mode=1777,strictatime,noexec,nodev,nosuid
```

Restart the tmp.mount

```
systemctl daemon-reload # might be optional
systemctl restart tmp.mount
```

/etc is stateless on Container-Optimized OS. Therefore, /etc cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/
2. https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/

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

1.1.3 Ensure nodev option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/tmp` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/tmp` .

Audit:

Verify that the `nodev` option is set if a `/tmp` partition exists
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v nodev
```

Remediation:

Run the following command to remount `/tmp` :

```
# mount -o remount,nodev /tmp
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3** <u>Configure Data Access Control Lists</u> 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	**5.1** <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	🟢	🟠	🔵

1.1.4 Ensure nosuid option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot create `setuid` files in `/tmp` .

Audit:

Verify that the `nosuid` option is set if a `/tmp` partition exists
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v nosuid
```

Remediation:

Run the following command to remount `/tmp` :

```
# mount -o remount,nosuid /tmp
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

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

1.1.5 Ensure noexec option set on /tmp partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/tmp` filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from `/tmp` .

Audit:

Verify that the `noexec` option is set if a `/tmp` partition exists
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/tmp\s' | grep -v noexec
```

Remediation:

Run the following command to remount `/tmp` :

```
# mount -o remount,noexec /tmp
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.6 Ensure nosuid option set on /var partition (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Since the `/var` filesystem is only intended for temporary dynamic data, set this option to ensure that users cannot create `setuid` files in `/var`.

Audit:

Verify that the `nosuid` option is set if a `/var` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var\s' | grep -v nosuid
```

Remediation:

Run the following command to remount `/var` :

```
# mount -o remount,nosuid /var
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

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

1.1.7 Ensure noexec option set on /var partition (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Since the `/var` filesystem is only intended for services to write data and not execute, set this option to ensure that users cannot run executable binaries from `/var`.

Audit:

Verify that the `noexec` option is set if a `/var` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var\s' | grep -v noexec
```

Remediation:

Run the following command to remount `/var` :

```
# mount -o remount,noexec /var
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.8 Ensure nodev option set on /var partition (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/var` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in `/var` .

Audit:

Verify that the `nodev` option is set if a `/var` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/var\s' | grep -v nodev
```

Remediation:

Run the following command to remount `/var` :

```
# mount -o remount,nodev /var
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 　　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	5.1 <u>Establish Secure Configurations</u> 　　Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.1.9 Ensure nodev option set on /home partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The nodev mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Audit:

Verify that the nodev option is set if a /home partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/home\s' | grep -v nodev
```

Remediation:

Run the following command to remount /var :

```
# mount -o remount,nodev /home
```

/etc is stateless on Container-Optimized OS. Therefore, /etc cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

Additional Information:

The actions in this recommendation refer to the /home partition, which is the default user partition that is defined in many distributions. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

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.	●	●	●

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

1.1.10 Ensure nodev option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/dev/shm` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in `/dev/shm` partitions.

Audit:

Verify that the `nodev` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nodev
```

Remediation:

Run the following command to remount `/dev/shm` :

```
# mount -o remount,nodev /dev/shm
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

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

1.1.11 Ensure nosuid option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Verify that the `nosuid` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v nosuid
```

Remediation:

Run the following command to remount `/dev/shm` :

```
# mount -o remount,nosuid /dev/shm
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

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

1.1.12 Ensure noexec option set on /dev/shm partition (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Audit:

Verify that the `noexec` option is set if a `/dev/shm` partition exists.
Run the following command and verify that nothing is returned:

```
# mount | grep -E '\s/dev/shm\s' | grep -v noexec
```

Remediation:

Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec /dev/shm
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 <u>Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v7	2.6 <u>Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

1.1.13 Disable Automounting (Automated)

Profile Applicability:

- Level 1 - Server

Description:

`autofs` allows automatic mounting of devices, typically including CD/DVDs and USB drives.

Rationale:

With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

Impact:

The use of portable hard drives is very common for workstation users. If your organization allows the use of portable storage or media on workstations and physical access controls to workstations is considered adequate there is little value add in turning off automounting.

Audit:

```
# systemctl is-enabled autofs
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `autofs`:

```
# systemctl disable autofs
```

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

This control should align with the tolerance of the use of portable drives and optical media in the organization. On a server requiring an admin to manually mount media can be part of defense-in-depth to reduce the risk of unapproved software or information being introduced or proprietary software or information being exfiltrated. If admins commonly use flash drives and Server access has sufficient physical controls, requiring manual mounting may not increase security.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.3 Disable Autorun and Autoplay for Removable Media** Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v8	**10.4 Configure Automatic Anti-Malware Scanning of Removable Media** Configure anti-malware software to automatically scan removable media.		●	●
v7	**8.4 Configure Anti-Malware Scanning of Removable Devices** Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	●	●	●
v7	**8.5 Configure Devices Not To Auto-run Content** Configure devices to not auto-run content from removable media.	●	●	●

1.2 Filesystem Integrity Checking

The recommendation in this section focus on securing the integrity of the root filesystem using dm-verity.

1.2.1 Ensure dm-verity is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

device-mapper-verity (dm-verity) kernel feature feature provides transparent integrity checking of block devices using a cryptographic digest provided by the kernel crypto API. When a dm-verity device is configured, it is expected that the caller has been authenticated in some way (cryptographic signatures, etc). After instantiation, all hashes will be verified on-demand during disk access. If they cannot be verified up to the root node of the tree, the root hash, then the I/O will fail. This should detect tampering with any data on the device and the hash data.

Rationale:

The Container-Optimized OS root filesystem is always mounted as read-only. Additionally, its checksum is computed at build time and verified by the kernel on each boot. This mechanism prevents against attackers from "owning" the machine through permanent local changes.

Audit:

Verify dm-verity is enabled in kernel config with the following command:

```
# zcat /proc/config.gz | grep CONFIG_DM_VERITY
CONFIG_DM_VERITY=y
```

Remediation:

An OS image update that has the dm-verity enabled kernel is required.

References:

1. AIDE stable manual: http://aide.sourceforge.net/stable/manual.html

Additional Information:

The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run `prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.14 Log Sensitive Data Access** Log sensitive data access, including modification and disposal.			●
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	**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).			●

1.3 Secure Boot Settings

The recommendations in this section focus on securing the bootloader and settings involved in the boot process directly.

1.3.1 Ensure authentication required for single user mode (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.

Rationale:

Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.

Audit:

Run the following commands and verify that `/sbin/sulogin` or `/usr/sbin/sulogin` is used as shown:

```
# grep /systemd-sulogin-shell /usr/lib/systemd/system/rescue.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
# grep /systemd-sulogin-shell /usr/lib/systemd/system/emergency.service

ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency
```

Remediation:

Rootfs is read-only file system. Therefore, update to an OS image which requires single user mode authentication.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.4 Additional Process Hardening

1.4.1 Ensure core dumps are restricted (Automated)

Profile Applicability:

- Level 2 - Server

Description:

A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.

Rationale:

Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see `limits.conf(5)`). In addition, setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

Audit:

Run the following commands and verify output matches:

```
# grep "hard core" /etc/security/limits.conf /etc/security/limits.d/*
* hard core 0
# sysctl fs.suid_dumpable
fs.suid_dumpable = 0
```

Run the following commands to check if systemd-coredump is installed:

```
# systemctl is-enabled systemd-coredump@.service
# systemctl is-enabled systemd-coredump.socket
```

if `static` is returned systemd-coredump is installed

Remediation:

Add the following line to `/etc/security/limits.conf` or a `/etc/security/limits.d/*` file:

```
* hard core 0
```

Run the following command to set the active kernel parameter:

```
# sysctl -w fs.suid_dumpable=0
```

If systemd-coredump@ is installed:
edit `/etc/systemd/coredump.conf` and add/modify the following lines:

```
Storage=none
ProcessSizeMax=0
```

Run the command:

```
systemctl daemon-reload
```

/etc is stateless on Container-Optimized OS. Therefore, /etc cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

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

1.4.2 Ensure XD/NX support is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The NX bit (no-execute) is a technology used in CPUs to segregate areas of memory for use by either storage of processor instructions or for storage of data. An operating system with support for the NX bit may mark certain areas of memory as non-executable. The processor will then refuse to execute any code residing in these areas of memory. This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible.

Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. On AMD processors, this ability is called No Execute (NX), on Intel processors it is called Execute Disable (XD) and on ARM processors it is called Execute Never (XN). Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature. Starting from ARMv6, the XN bit is supported by default and the kernel cannot disable it. For this reason, this recommend is not applicable for Container-Optimized OS ARM images.

Rationale:

Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.

Audit:

Run the following command and verify your kernel has identified and activated NX/XD protection.

```
# journalctl | grep 'protection: active'

kernel: NX (Execute Disable) protection: active
```

OR
on systems without journalctl

```
[[ -n $(grep noexec[0-9]*=off /proc/cmdline) || -z $(grep -E -i ' (pae|nx) '
/proc/cpuinfo) || -n $(grep '\sNX\s.*\sprotection:\s' /var/log/dmesg | grep -
v active) ]] && echo "NX Protection is not active"
```

Nothing should be returned

Remediation:

On 32 bit systems install a kernel with PAE support, no installation is required on 64 bit systems:
If necessary configure your bootloader to load the new kernel and reboot the system.
You may need to enable NX or XD support in your bios.

Additional Information:

Ensure your system supports the XD or NX bit and has PAE support before implementing this recommendation as this may prevent it from booting if these are not supported by your hardware.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**10.5 Enable Anti-Exploitation Features** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		🟠	🔵
v7	**8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies** Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		🟠	🔵

1.4.3 Ensure address space layout randomization (ASLR) is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.

Rationale:

Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Audit:

Run the following command and verify output matches:

```
# sysctl kernel.randomize_va_space
kernel.randomize_va_space = 2
# grep "kernel\.randomize_va_space" /etc/sysctl.conf /etc/sysctl.d/*
kernel.randomize_va_space = 2
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
kernel.randomize_va_space = 2
```

Run the following command to set the active kernel parameter:

```
# sysctl -w kernel.randomize_va_space=2
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.5 <u>Enable Anti-Exploitation Features</u> Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

1.5 Warning Banners

Presenting a warning message prior to the normal user login may assist in the prosecution of trespassers on the computer system. Changing some of these login banners also has the side effect of hiding OS version information and other detailed system information from attackers attempting to target specific exploits at a system.

Guidelines published by the US Department of Defense require that warning messages include at least the name of the organization that owns the system, the fact that the system is subject to monitoring and that such monitoring is in compliance with local statutes, and that use of the system implies consent to such monitoring. It is important that the organization's legal counsel review the content of all messages before any system modifications are made, as these warning messages are inherently site-specific. More information (including citations of relevant case law) can be found at http://www.justice.gov/criminal/cybercrime/

Note: The text provided in the remediation actions for these items is intended as an example only. Please edit to include the specific text for your organization as approved by your legal department.

1.5.1 Command Line Warning Banners

The `/etc/motd`, `/etc/issue`, and `/etc/issue.net` files govern warning banners for standard command line logins for both local and remote users.

1.5.1.1 Ensure message of the day is configured properly (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/motd
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 |
sed -e 's/"//g'))" /etc/motd
```

Remediation:

Edit the `/etc/motd` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform` `/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

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

1.5.1.2 Ensure local login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version - or the operating system's name

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 |
sed -e 's/"//g'))" /etc/issue
```

Remediation:

Edit the `/etc/issue` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`

```
# echo "Authorized uses only. All activity may be monitored and reported." >
/etc/issue
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

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

1.5.1.3 Ensure remote login warning banner is configured properly (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information: `\m` - machine architecture `\r` - operating system release `\s` - operating system name `\v` - operating system version

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " `uname -a` " command once they have logged in.

Audit:

Run the following command and verify that the contents match site policy:

```
# cat /etc/issue.net
```

Run the following command and verify no results are returned:

```
# grep -E -i "(\\v|\\r|\\m|\\s|$(grep '^ID=' /etc/os-release | cut -d= -f2 |
sed -e 's/"//g'))" /etc/issue.net
```

Remediation:

Edit the `/etc/issue.net` file with the appropriate contents according to your site policy, remove any instances of `\m` , `\r` , `\s` , `\v` or references to the `OS platform`

```
# echo "Authorized uses only. All activity may be monitored and reported." >
/etc/issue.net
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

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

1.5.1.4 Ensure permissions on /etc/motd are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The contents of the `/etc/motd` file are displayed to users after login and function as a message of the day for authenticated users.

Rationale:

If the `/etc/motd` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/motd
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/motd` :

```
# chown root:root /etc/motd
# chmod 644 /etc/motd
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.1.5 Ensure permissions on /etc/issue are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The contents of the `/etc/issue` file are displayed to users prior to login for local terminals.

Rationale:

If the `/etc/issue` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644`:

```
# stat /etc/issue
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue` :

```
# chown root:root /etc/issue
# chmod 644 /etc/issue
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.5.1.6 Ensure permissions on /etc/issue.net are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The contents of the `/etc/issue.net` file are displayed to users prior to login for remote connections from configured services.

Rationale:

If the `/etc/issue.net` file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/issue.net
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set permissions on `/etc/issue.net` :

```
# chown root:root /etc/issue.net
# chmod 644 /etc/issue.net
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

1.6 Ensure AppArmor is installed (Automated)

Profile Applicability:

- Level 1 - Server

Description:

SELinux and AppArmor provide Mandatory Access Controls.

Rationale:

Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.

Audit:

Verify that AppArmor is installed with the following command:

```
# grep '\"name\": \"apparmor\"' /etc/cos-package-info.json
"name": "apparmor",
```

Remediation:

Update to an OS image that includes the the apparmor package.

Additional Information:

SELinux and AppArmor both have several package names in use on different distributions. Research the appropriate packages for your environment.

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	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.	●	●	●

2 Services

While applying system updates and patches helps correct known vulnerabilities, one of the best ways to protect the system against as yet unreported vulnerabilities is to disable all services that are not required for normal system operation. This prevents the exploitation of vulnerabilities discovered at a later date. If a service is not enabled, it cannot be exploited. The actions in this section of the document provide guidance on some services which can be safely disabled and under which circumstances, greatly reducing the number of possible threats to the resulting system. Additionally some services which should remain enabled but with secure configuration are covered as well as insecure service clients.

2.1 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that they be disabled or deleted from the system to reduce the potential attack surface.

2.1.1 Time Synchronization

It is recommended that physical systems and virtual guests lacking direct access to the physical host's clock be configured to synchronize their time using a service such as NTP or chrony.

2.1.1.1 Ensure time synchronization is in use (Manual)

Profile Applicability:

- Level 1 - Server

Description:

System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.

Rationale:

Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.

Audit:

On physical systems or virtual systems where host based time synchronization is not available verify that chrony is installed with the following command:

```
# grep '\"name\": \"chrony\"' /etc/cos-package-info.json

"name": "chrony",
```

On virtual systems where host based time synchronization is available consult your virtualization software documentation and verify that host based synchronization is in use.

Remediation:

On physical systems or virtual systems where host based time synchronization is not available update to an image that comes with chrony package installed.
On virtual systems where host based time synchronization is available consult your virtualization software documentation and setup host based synchronization.

Additional Information:

systemd-timesyncd is part of systemd. Some versions of systemd have been compiled without systemd-timesycnd. On these distributions, chrony or NTP should be used instead of systemd-timesycnd.

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.		●	●

2.1.1.2 Ensure chrony is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

chrony is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server.

Rationale:

If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

This recommendation only applies if chrony is in use on the system.

Audit:

Run the following command and verify remote server is configured properly:

```
# grep -E "^(server|pool)" /etc/chrony/chrony.conf
server <remote-server>
```

Multiple servers may be configured.
Run the following command and verify the first field for the chronyd process is ntp or chrony:

```
# ps -ef | grep chronyd
ntp      491      1  0 20:32 ?        00:00:00 /usr/sbin/chronyd
```

Or

```
# ps -ef | grep chronyd
chrony      491      1  0 20:32 ?        00:00:00 /usr/sbin/chronyd
```

Remediation:

Update to an OS image that has the correct chrony configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		🟠	🔵

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.		●	●

2.1.2 Ensure X Window System is not installed (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.

Rationale:

Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.

Impact:

Many Linux systems run applications which require a Java runtime. Some Linux Java packages have a dependency on specific X Windows xorg-x11-fonts. One workaround to avoid this dependency is to use the "headless" Java packages for your specific Java runtime, if provided by your distribution.

Audit:

Verify X Windows System is not installed. The following command should return empty result.

```
# grep xorg /etc/cos-package-info.json
```

Remediation:

An OS image update that does not include X Window System is required.

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.	●	●	●
v7	**2.6 Address unapproved software** Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.1.3 Ensure NFS and RPC are not enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network.

Rationale:

If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce the remote attack surface.

Audit:

Run the following commands to verify the `nfs-server` and `rpcbind` are not enabled:

```
# systemctl is-enabled nfs-server

disabled
# systemctl is-enabled rpcbind

disabled
```

Verify result is not "enabled" for both.

Remediation:

Run the following commands to disable the `nfs-server` and `rpcbind`:

```
# systemctl --now disable nfs-server
# systemctl --now disable rpcbind
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

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.	●	●	●
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
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.		●	●

2.1.4 Ensure rsync service is not enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `rsyncd` service can be used to synchronize files between systems over network links.

Rationale:

The `rsyncd` service presents a security risk as it uses unencrypted protocols for communication.

Audit:

Run the following command to verify `rsyncd` is not enabled:

```
# systemctl is-enabled rsyncd
disabled
```

Verify result is not "enabled".

Remediation:

Run the following command to disable `rsyncd` :

```
# systemctl --now disable rsyncd
```

`/etc` is stateless on Container-Optimized OS. Therefore, the steps mentioned above needs to be performed after every boot.

Additional Information:

Additional methods of disabling a service exist. Consult your distribution documentation for appropriate methods.

On some distributions the rsync service is known as `rsync`, not `rsyncd`.

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
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.		●	●

3 Network Configuration

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

3.1 Network Parameters (Host Only)

The following network parameters are intended for use if the system is to act as a host only. A system is considered host only if the system has a single interface, or has multiple interfaces but will not be configured as a router.

3.1.1 Ensure packet redirect sending is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects.

Rationale:

An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.send_redirects
net.ipv4.conf.all.send_redirects = 0
# sysctl net.ipv4.conf.default.send_redirects
net.ipv4.conf.default.send_redirects = 0
# grep "net\.ipv4\.conf\.all\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*
net.ipv4.conf.all.send_redirects = 0
# grep "net\.ipv4\.conf\.default\.send_redirects" /etc/sysctl.conf
/etc/sysctl.d/*
net.ipv4.conf.default.send_redirects= 0
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.send_redirects=0
# sysctl -w net.ipv4.conf.default.send_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 <u>Securely Manage Network Infrastructure</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2 Network Parameters (Host and Router)

The following network parameters are intended for use on both host only and router systems. A system acts as a router if it has at least two interfaces and is configured to perform routing functions.

3.2.1 Ensure source routed packets are not accepted (Automated)

Profile Applicability:

- Level 2 - Server

Description:

In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used.

Rationale:

Setting `net.ipv4.conf.all.accept_source_route,` `net.ipv4.conf.default.accept_source_route,` `net.ipv6.conf.all.accept_source_route` and `net.ipv6.conf.default.accept_source_route` to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_source_route

net.ipv4.conf.all.accept_source_route = 0
# sysctl net.ipv4.conf.default.accept_source_route

net.ipv4.conf.default.accept_source_route = 0
# sysctl net.ipv6.conf.all.accept_source_route

net.ipv6.conf.all.accept_source_route = 0
# sysctl net.ipv6.conf.default.accept_source_route

net.ipv6.conf.default.accept_source_route = 0
```

Remediation:

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_source_route=0
# sysctl -w net.ipv4.conf.default.accept_source_route=0
# sysctl -w net.ipv6.conf.all.accept_source_route=0
# sysctl -w net.ipv6.conf.default.accept_source_route=0
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.2 Ensure ICMP redirects are not accepted (Automated)

Profile Applicability:

- Level 2 - Server

Description:

ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting `net.ipv4.conf.all.accept_redirects` and `net.ipv6.conf.all.accept_redirects` to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables.

Rationale:

Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.accept_redirects
net.ipv4.conf.all.accept_redirects = 0
# sysctl net.ipv4.conf.default.accept_redirects
net.ipv4.conf.default.accept_redirects = 0
# sysctl net.ipv6.conf.all.accept_redirects
net.ipv6.conf.all.accept_redirects = 0
# sysctl net.ipv6.conf.default.accept_redirects
net.ipv6.conf.default.accept_redirects = 0
```

Remediation:

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.accept_redirects=0
# sysctl -w net.ipv4.conf.default.accept_redirects=0
# sysctl -w net.ipv6.conf.all.accept_redirects=0
# sysctl -w net.ipv6.conf.default.accept_redirects=0
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

/etc is stateless on Container-Optimized OS. Therefore, /etc cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.2 Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.3 Ensure secure ICMP redirects are not accepted (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure.

Rationale:

It is still possible for even known gateways to be compromised. Setting `net.ipv4.conf.all.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.secure_redirects
net.ipv4.conf.all.secure_redirects = 0
# sysctl net.ipv4.conf.default.secure_redirects
net.ipv4.conf.default.secure_redirects = 0
```

Remediation:

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.secure_redirects=0
# sysctl -w net.ipv4.conf.default.secure_redirects=0
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		🟠	🔵

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.	●	●	●

3.2.4 Ensure suspicious packets are logged (Automated)

Profile Applicability:

- Level 2 - Server

Description:

When enabled, this feature logs packets with un-routable source addresses to the kernel log.

Rationale:

Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.log_martians
net.ipv4.conf.all.log_martians = 1
# sysctl net.ipv4.conf.default.log_martians
net.ipv4.conf.default.log_martians = 1
```

Remediation:

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.log_martians=1
# sysctl -w net.ipv4.conf.default.log_martians=1
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 <u>Collect Detailed Audit Logs</u> 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.		●	●

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.		🟠	🔵

3.2.5 Ensure broadcast ICMP requests are ignored (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Setting `net.ipv4.icmp_echo_ignore_broadcasts` to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses.

Rationale:

Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
# grep "net\.ipv4\.icmp_echo_ignore_broadcasts" /etc/sysctl.conf
/etc/sysctl.d/*
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.2 Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.6 Ensure bogus ICMP responses are ignored (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Setting `icmp_ignore_bogus_error_responses` to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages.

Rationale:

Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.icmp_ignore_bogus_error_responses

net.ipv4.icmp_ignore_bogus_error_responses = 1
# grep "net.ipv4.icmp_ignore_bogus_error_responses" /etc/sysctl.conf
/etc/sysctl.d/*

net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Remediation:

Set the following parameter in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.7 Ensure Reverse Path Filtering is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Setting `net.ipv4.conf.all.rp_filter` and `net.ipv4.conf.default.rp_filter` to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if `log_martians` is set).

Rationale:

Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.conf.all.rp_filter
net.ipv4.conf.all.rp_filter = 1
# sysctl net.ipv4.conf.default.rp_filter
net.ipv4.conf.default.rp_filter = 1
# grep "net\.ipv4\.conf\.all\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.conf.all.rp_filter = 1
# grep "net\.ipv4\.conf\.default\.rp_filter" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.conf.default.rp_filter = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.conf.all.rp_filter=1
# sysctl -w net.ipv4.conf.default.rp_filter=1
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**12.2 <u>Establish and Maintain a Secure Network Architecture</u>** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	**5.1 <u>Establish Secure Configurations</u>** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.8 Ensure TCP SYN Cookies is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue.

Rationale:

Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
# grep "net\.ipv4\.tcp_syncookies" /etc/sysctl.conf /etc/sysctl.d/*
net.ipv4.tcp_syncookies = 1
```

Remediation:

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

```
net.ipv4.tcp_syncookies = 1
```

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv4.tcp_syncookies=1
# sysctl -w net.ipv4.route.flush=1
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 <u>Establish and Maintain a Secure Network Architecture</u> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.9 Ensure IPv6 router advertisements are not accepted (Automated)

Profile Applicability:

- Level 2 - Server

Description:

This setting disables the system's ability to accept IPv6 router advertisements.

Rationale:

It is recommended that systems do not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Audit:

Run the following commands and verify output matches:

```
# sysctl net.ipv6.conf.all.accept_ra
net.ipv6.conf.all.accept_ra = 0
# sysctl net.ipv6.conf.default.accept_ra
net.ipv6.conf.default.accept_ra = 0
```

Remediation:

Run the following commands to set the active kernel parameters:

```
# sysctl -w net.ipv6.conf.all.accept_ra=0
# sysctl -w net.ipv6.conf.default.accept_ra=0
# sysctl -w net.ipv6.route.flush=1
```

/etc is stateless on Container-Optimized OS. Therefore, /etc cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●

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.	●	●	●

3.3 Firewall Configuration

IPtables is an application that allows a system administrator to configure the IPv4 tables, IPv6 tables, chains and rules provided by the Linux kernel firewall. While several methods of configuration exist this section is intended only to ensure the resulting IPtables and rules are in place, not how they are configured. If IPv6 is in use in your environment, similar settings should be applied to the IP6tables as well.

3.3.1 Configure IPv6 ip6tables

Ip6tables is used to set up, maintain, and inspect the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains. Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

If IPv6 in enabled on the system, the ip6tables should be configured.

Note: This section broadly assumes starting with an empty ip6tables firewall ruleset (established by flushing the rules with ip6tables -F). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```bash
#!/bin/bash

# Flush ip6tables rules
ip6tables -F

# Ensure default deny firewall policy
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP

# Ensure loopback traffic is configured
ip6tables -A INPUT -i lo -j ACCEPT
ip6tables -A OUTPUT -o lo -j ACCEPT
ip6tables -A INPUT -s ::1 -j DROP

# Ensure outbound and established connections are configured
ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
ip6tables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.3.1.1 Ensure IPv6 default deny firewall policy (Automated)

Profile Applicability:

- Level 2 - Server

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the INPUT, OUTPUT, and FORWARD chains is DROP or REJECT:

```
# ip6tables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# ip6tables -P INPUT DROP
# ip6tables -P OUTPUT DROP
# ip6tables -P FORWARD DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
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.	●	●	●

3.3.1.2 Ensure IPv6 loopback traffic is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# ip6tables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in      out     source
destination
    0     0 ACCEPT     all      lo     *       ::/0                    ::/0
    0     0 DROP       all      *      *       ::1                     ::/0


# ip6tables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in      out     source
destination
    0     0 ACCEPT     all      *      lo      ::/0                    ::/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# ip6tables -A INPUT -i lo -j ACCEPT
# ip6tables -A OUTPUT -o lo -j ACCEPT
# ip6tables -A INPUT -s ::1 -j DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 <u>Implement and Manage a Firewall on Servers</u>** 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 <u>Apply Host-based Firewalls or Port Filtering</u>** 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.	●	●	●

3.3.1.3 Ensure IPv6 outbound and established connections are configured (Manual)

Profile Applicability:

- Level 2 - Server

Description:

Configure the firewall rules for new outbound, and established IPv6 connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# ip6tables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# ip6tables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# ip6tables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 <u>Implement and Manage a Firewall on Servers</u>** 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 <u>Apply Host-based Firewalls or Port Filtering</u>** 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.	●	●	●

3.3.1.4 Ensure IPv6 firewall rules exist for all open ports (Manual)

Profile Applicability:

- Level 2 - Server

Description:

Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic.

Rationale:

Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Audit:

Run the following command to determine open ports:

```
# ss -6tuln

Netid  State      Recv-Q Send-Q     Local Address:Port                      Peer
Address:Port
udp    UNCONN     0      0                        ::1:123
:::*
udp    UNCONN     0      0                        :::123
:::*
tcp    LISTEN     0      128                      :::22
:::*
tcp    LISTEN     0      20                       ::1:25
:::*
```

Run the following command to determine firewall rules:

```
# ip6tables -L INPUT -v -n

Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out       source
destination
    0     0 ACCEPT     all       lo      *       ::/0                     ::/0
    0     0 DROP       all       *       *       ::1                      ::/0
    0     0 ACCEPT     tcp       *       *       ::/0                     ::/0
tcp dpt:22 state NEW
```

Verify all open ports listening on non-localhost addresses have at least one firewall rule. The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.

Remediation:

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

```
# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j
ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

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.	●	●	●
v8	**12.2 Establish and Maintain a Secure Network Architecture** Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
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.	●	●	●

3.3.2 Configure IPv4 iptables

Iptables is used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user-defined chains.

Each chain is a list of rules which can match a set of packets. Each rule specifies what to do with a packet that matches. This is called a 'target', which may be a jump to a user-defined chain in the same table.

Note: This section broadly assumes starting with an empty IPtables firewall ruleset (established by flushing the rules with iptables -F). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot. The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere:

```bash
#!/bin/bash

# Flush IPtables rules
iptables -F

# Ensure default deny firewall policy
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Ensure loopback traffic is configured
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -s 127.0.0.0/8 -j DROP

# Ensure outbound and established connections are configured
iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT

# Open inbound ssh(tcp port 22) connections
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j ACCEPT
```

3.3.2.1 Ensure default deny firewall policy (Automated)

Profile Applicability:

- Level 2 - Server

Description:

A default deny all policy on connections ensures that any unconfigured network usage will be rejected.

Rationale:

With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Audit:

Run the following command and verify that the policy for the `INPUT` , `OUTPUT` , and `FORWARD` chains is `DROP` or `REJECT` :

```
# iptables -L
Chain INPUT (policy DROP)
Chain FORWARD (policy DROP)
Chain OUTPUT (policy DROP)
```

Remediation:

Run the following commands to implement a default DROP policy:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT DROP
# iptables -P FORWARD DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4 <u>Implement and Manage a Firewall on Servers</u>** 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 <u>Apply Host-based Firewalls or Port Filtering</u>** 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.	●	●	●

3.3.2.2 Ensure loopback traffic is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).

Rationale:

Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Audit:

Run the following commands and verify output includes the listed rules in order (packet and byte counts may differ):

```
# iptables -L INPUT -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out     source
destination
    0     0 ACCEPT     all  --  lo      *       0.0.0.0/0               0.0.0.0/0
    0     0 DROP       all  --  *       *       127.0.0.0/8             0.0.0.0/0

 # iptables -L OUTPUT -v -n
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in      out     source
destination
    0     0 ACCEPT     all  --  *       lo      0.0.0.0/0               0.0.0.0/0
```

Remediation:

Run the following commands to implement the loopback rules:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
# iptables -A INPUT -s 127.0.0.0/8 -j DROP
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4** <u>Implement and Manage a Firewall on Servers</u> 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** <u>Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

3.3.2.3 Ensure outbound and established connections are configured (Manual)

Profile Applicability:

- Level 2 - Server

Description:

Configure the firewall rules for new outbound, and established connections.

Rationale:

If rules are not in place for new outbound, and established connections all packets will be dropped by the default policy preventing network usage.

Audit:

Run the following command and verify all rules for new outbound, and established connections match site policy:

```
# iptables -L -v -n
```

Remediation:

Configure iptables in accordance with site policy. The following commands will implement a policy to allow all outbound connections and all established connections:

```
# iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
# iptables -A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
```

Additional Information:

Changing firewall settings while connected over network can result in being locked out of the system.

Remediation will only affect the active system firewall, be sure to configure the default policy in your firewall management to apply on boot as well.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.4** <u>Implement and Manage a Firewall on Servers</u> 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** <u>Apply Host-based Firewalls or Port Filtering</u> 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.	●	●	●

3.3.3 Ensure iptables is installed (Automated)

Profile Applicability:

- Level 1 - Server

Description:

`iptables` allows configuration of the IPv4 and IPv6 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to `iptables`.

Rationale:

iptables is required for firewall management and configuration.

Audit:

Run the following command and verify iptables is installed:

```
grep '\"name\": \"iptables\"' /etc/cos-package-info.json

"name": "iptables"
```

Remediation:

Update to an OS image that includes the iptables package.

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.	●	●	●

4 Logging and Auditing

The items in this section describe how to configure logging, log monitoring, and auditing, using tools included in most distributions.

It is recommended that `rsyslog` be used for logging (with `logwatch` providing summarization) and `auditd` be used for auditing (with `aureport` providing summarization) to automatically monitor logs for intrusion attempts and other suspicious system behavior.

In addition to the local log files created by the steps in this section, it is also recommended that sites collect copies of their system logs on a secure, centralized log server via an encrypted connection. Not only does centralized logging help sites correlate events that may be occurring on multiple systems, but having a second copy of the system log information may be critical after a system compromise where the attacker has modified the local log files on the affected system(s). If a log correlation system is deployed, configure it to process the logs described in this section.

Because it is often necessary to correlate log information from many different systems (particularly after a security incident) it is recommended that the time be synchronized among systems and devices connected to the local network. The standard Internet protocol for time synchronization is the Network Time Protocol (NTP), which is supported by most network-ready devices. See the `ntpd(8)` manual page for more information on configuring NTP.

It is important that all logs described in this section be monitored on a regular basis and correlated to determine trends. A seemingly innocuous entry in one log could be more significant when compared to an entry in another log.

Note on log file permissions: There really isn't a "one size fits all" solution to the permissions on log files. Many sites utilize group permissions so that administrators who are in a defined security group, such as "wheel" do not have to elevate privileges to root in order to read log files. Also, if a third party log aggregation tool is used, it may need to have group permissions to read the log files, which is preferable to having it run setuid to root. Therefore, there are two remediation and audit steps for log file permissions. One is for systems that do not have a secured group method implemented that only permits root to read the log files (`root:root 600`). The other is for sites that do have such a setup and are designated as `root:securegrp 640` where `securegrp` is the defined security group (in some cases `wheel`).

4.1 Configure Logging

Logging services should be configured to prevent information leaks and to aggregate logs on a remote server so that they can be reviewed in the event of a system compromise and ease log analysis.

4.1.1 Configure logging agent

The stackdriver logging agent and the fluent-bit logging agent are the two logging agents COS uses in Google supported images. Fluent-bit is used in COS on ARM for Milestone 101 and above. The stackdriver logging agent is used everywhere else. They stream logs from your VM instances and from selected third-party software packages to Cloud Logging. It is a best practice to run the logging agent on all your VM instances.

4.1.1.1 Ensure correct container image is set for stackdriver logging agent (Automated)

Profile Applicability:

- Level 2 - Server

Description:

`stackdriver-logging` service runs stackdriver container image to export logs to Cloud Logging.

Note: This recommendation is not applicable for COS images using Fluent-bit as it isn't containerized.

Rationale:

If the logging agent is not set correctly, the logs cannot be exported to Cloud Logging.

Audit:

Verify `LOGGING_AGENT_DOCKER_IMAGE` is set to a correct stackdriver container image. Use the following command to verify:

```
# grep LOGGING_AGENT_DOCKER_IMAGE /etc/stackdriver/env_vars
LOGGING_AGENT_DOCKER_IMAGE="gcr.io/stackdriver-agents/stackdriver-logging-
agent:<version>"
```

Remediation:

Edit the `LOGGING_AGENT_DOCKER_IMAGE` variable in the `/etc/stackdriver/env_vars` file to set the correct logging agent.
Run the following command to restart `stackdriver-logging` service :

```
# systemctl restart stackdriver-logging
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●

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	**6.2 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.		●	●

4.1.1.2 Ensure Logging Service is Running (Manual)

Profile Applicability:

- Level 2 - Server

Description:

Some form of logging for the OS should be used. On COS **Stackdriver-logging agent** or **fluent-bit logging agent** are provided and can be activated simply by following the guides. It is not require to use these for logging but they are simple to set up and will work well.

Rationale:

If no logging is running, their will be less of a trail for audit if things go wrong. It is a good practice to have logging enabled for better visibility.

Audit:

This audit procedure is only if you are using one of the supporting logging services described.
Stackdriver-Logging Agent
Run the following command to verify `stackdriver-logging` is running:

```
# systemctl status stackdriver-logging | grep Active
Active: active (running) since <Day date time>
```

Fluent-bit Logging
Or if your system has fluent-bit, run the following command to verify `fluent-bit` is running:

```
# systemctl status fluent-bit | grep Active
Active: active (running) since <Day date time>
```

Remediation:

This remediation is only if you want to use one of the supported logging services described.
Stackdriver-logging Agent
Run the following command to enable `stackdriver-logging` :

```
# systemctl start stackdriver-logging
```

Fluent-bit Logging
Run the following command to enable `fluent-bit` :

```
# systemctl start fluent-bit
```

Works for Both
Simply update the instance metadata to enable logging as follows:

```
# gcloud compute instances add-metadata <instance-name> \
    --zone <compute-zone> \
    --metadata google-logging-enabled=true
```

CIS Controls:

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

4.1.1.3 Ensure logging is configured (Manual)

Profile Applicability:

- Level 2 - Server

Description:

For an image using stackdriver, the `/etc/stackdriver/logging.config.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages. An image using fluent-bit uses `/usr/share/fluent-bit/fluent-bit.conf` for the same purpose.

Rationale:

A great deal of important security-related information is sent via logging (e.g., successful and failed su attempts, failed login attempts, root login attempts, etc.).

Audit:

Review the contents of the /etc/stackdriver/logging.config.d/*.conf if using an image with stackdriver or /usr/share/fluent-bit/fluent-bit.conf if using an image with fluent-bit to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information:

```
# ls -l /var/log/
```

Remediation:

Edit the contents of `/etc/stackdriver/logging.config.d/*.conf` if using an image with stackdriver or `/usr/share/fluent-bit/fluent-bit.conf` if using an image with fluent-bit as appropriate for your environment.
Then run the following commands to reload the logging configuration:
For stackdriver-logging:

```
# systemctl restart stackdriver-logging
```

For fluent-bit:

```
# systemctl restart fluent-bit
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above need to be performed after every boot for images using stackdriver. This is not the case for fluent-bit as the logging agent is in `/usr/share/` which isn't stateless so changes will be persistent across reboots.

References:

1. See the rsyslog.conf(5) man page for more information.

CIS Controls:

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

4.1.2 Configure journald

systemd-journald is a system service that collects and stores logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources: Kernel log messages, via kmsg

Any changes made to the systemd-journald configuration will require a re-start of systemd-journald

4.1.2.1 Ensure journald is configured to compress large log files (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The journald system includes the capability of compressing overly large files to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

Uncompressed large files may unexpectedly fill a filesystem leading to resource unavailability. Compressing logs prior to write can prevent sudden, unexpected filesystem impacts.

Audit:

Review `/etc/systemd/journald.conf` and verify that large files will be compressed:

```
# grep -e Compress /etc/systemd/journald.conf
# Compress=yes
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Compress=yes
```

Reload the configuration to be effective.

```
# systemctl force-reload systemd-journald
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

References:

1. https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**8.3** <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	**6.4** <u>Ensure adequate storage for logs</u> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

4.1.2.2 Ensure journald is configured to write logfiles to persistent disk (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Data from journald may be stored in volatile memory or persisted locally on the server. Logs in memory will be lost upon a system reboot. By persisting logs to local disk on the server they are protected from loss.

Rationale:

Writing log data to disk will provide the ability to forensically reconstruct events which may have impacted the operations or security of a system even after a system crash or reboot.

Audit:

Review `/etc/systemd/journald.conf` and verify that logs are persisted to disk:

```
# grep -e Storage /etc/systemd/journald.conf
# Storage=persistent
```

Remediation:

Edit the `/etc/systemd/journald.conf` file and add the following line:

```
Storage=persistent
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

References:

1. [https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemd journaldconf](https://github.com/konstruktoid/hardening/blob/master/systemd.adoc#etcsystemdjournaldconf)

Additional Information:

The main configuration file `/etc/systemd/journald.conf` is read before any of the custom *.conf files. If there are custom configs present, they override the main configuration parameters

CIS Controls:

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

4.1.3 Ensure permissions on all logfiles are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well.

Rationale:

It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Audit:

Run the following command and verify that other has no permissions on any files and group does not have write or execute permissions on any files:

```
# find /var/log -type f -ls
```

Remediation:

Run the following commands to set permissions on all existing log files:

```
find /var/log -type f -exec chmod g-wx,o-rwx "{}" + -o -type d -exec chmod g-w,o-rwx "{}" +
```

Additional Information:

You may also need to change the configuration for your logging software or services for any logs that had incorrect permissions.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.2 Ensure logrotate is configured (Manual)

Profile Applicability:

- Level 2 - Server

Description:

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large.

Rationale:

By keeping the log files smaller and more manageable, a system administrator can easily archive these files to another system and spend less time looking through inordinately large log files.

Audit:

Review `/etc/logrotate.conf` and `/etc/logrotate.d/*` and verify logs are rotated according to site policy.

Remediation:

Edit `/etc/logrotate.conf` and `/etc/logrotate.d/*` to ensure logs are rotated according to site policy.
`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

Additional Information:

If no `maxage` setting is set for logrotate a situation can occur where logrotate is interrupted and fails to delete rotated logfiles. It is recommended to set this to a value greater than the longest any log file should exist on your system to ensure that any such logfile is removed but standard rotation settings are not overridden.

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.		●	●

5 Access, Authentication and Authorization

5.1 SSH Server Configuration

SSH is a secure, encrypted replacement for common login services such as `telnet`, `ftp`, `rlogin`, `rsh`, and `rcp`. It is strongly recommended that sites abandon older clear-text login protocols and use SSH to prevent session hijacking and sniffing of sensitive data off the network.

Note: The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is not required the SSH daemon can be removed and this section skipped.

Note: Once all configuration changes have been made to `/etc/ssh/sshd_config`, the sshd configuration must be reloaded:

```
# systemctl reload sshd
```

Note: `/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make configuration changes persistent across reboots. After a reboot, configuration changes need to be reapplied.

5.1.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/etc/ssh/sshd_config` file contains configuration specifications for `sshd`. The command below sets the owner and group of the file to root.

Rationale:

The `/etc/ssh/sshd_config` file needs to be protected from unauthorized changes by non-privileged users.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` does not grant permissions to `group` or `other`:

```
# stat /etc/ssh/sshd_config
Access: (0600/-rw-------)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following commands to set ownership and permissions on `/etc/ssh/sshd_config`:

```
# chown root:root /etc/ssh/sshd_config
# chmod og-rwx /etc/ssh/sshd_config
```

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

5.1.2 Ensure permissions on SSH private host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

An SSH private key is one of two files used in SSH public key authentication. In this authentication method, the possession of the private key is proof of identity. Only a private key that corresponds to a public key will be able to authenticate successfully. The private keys need to be stored and handled carefully, and no copies of the private key should be distributed.

Rationale:

If an unauthorized user obtains the private SSH host key file, the host could be impersonated

Audit:

Run the following command and verify Uid is 0/root and Gid is 0/root. Ensure group and other do not have permissions

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec stat {} \;

  File: '/etc/ssh/ssh_host_rsa_key'
  Size: 1679           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8628138      Links: 1
Access: (0600/-rw-------)  Uid: (     0/    root)  Gid: (  0/root)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.873750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ecdsa_key'
  Size: 227            Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631760      Links: 1
Access: (0600/-rw-------)  Uid: (     0/    root)  Gid: (  0/root)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.905750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ed25519_key'
  Size: 387            Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631762      Links: 1
Access: (0600/-rw-------)  Uid: (     0/    root)  Gid: ( 0/root)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.957750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set ownership and permissions on the private SSH host key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:root {} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod 0600 {} \;
```

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

5.1.3 Ensure permissions on SSH public host key files are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.

Rationale:

If a public host key file is modified by an unauthorized user, the SSH service may be compromised.

Audit:

Run the following command and verify Access does not grant write or execute permissions to group or other for all returned files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec stat {} \;

  File: '/etc/ssh/ssh_host_rsa_key.pub'
  Size: 382           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631758     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.881750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ecdsa_key.pub'
  Size: 162           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631761     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.917750616 +0000
 Birth: -
  File: '/etc/ssh/ssh_host_ed25519_key.pub'
  Size: 82            Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d    Inode: 8631763     Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.961750616 +0000
 Birth: -
```

Remediation:

Run the following commands to set permissions and ownership on the SSH host public key files

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chmod 0644 {}
\;
#find /etc/ssh -xdev -type f -name 'ssh_host_*_key.pub' -exec chown root:root
{} \;
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.4 Ensure SSH Protocol is set to 2 (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Older versions of SSH support two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

Run the following command and verify that output matches:

```
# grep ^Protocol /etc/ssh/sshd_config

Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

Additional Information:

This command not longer exists in newer versions of SSH. This check is still being included for systems that may be running an older version of SSH. As of openSSH version 7.4 this parameter will not cause an issue when included.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> 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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.5 <u>Use Multifactor Authentication For All Administrative Access</u> Use multi-factor authentication and encrypted channels for all administrative account access.		🟠	🔵
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		🟠	🔵

5.1.5 Ensure SSH LogLevel is appropriate (Automated)

Profile Applicability:

- Level 1 - Server

Description:

`INFO` level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field.

`VERBOSE` level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments.

Rationale:

SSH provides several logging levels with varying amounts of verbosity. `DEBUG` is specifically **not** recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep loglevel
LogLevel VERBOSE

OR

loglevel INFO
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LogLevel VERBOSE
```

OR

```
LogLevel INFO
```

Default Value:

LogLevel INFO

References:

1. https://www.ssh.com/ssh/sshd_config/

CIS Controls:

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

5.1.6 Ensure SSH X11 forwarding is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections.

Rationale:

Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep x11forwarding

X11Forwarding no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
X11Forwarding no
```

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.	●	●	●
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

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

5.1.7 Ensure SSH MaxAuthTries is set to 4 or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the `journald` logs detailing the login failure.

Rationale:

Setting the `MaxAuthTries` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Audit:

Run the following command and verify that output `MaxAuthTries` is 4 or less:

```
# sshd -T | grep maxauthtries

MaxAuthTries 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxAuthTries 4
```

Default Value:

MaxAuthTries 6

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	16.13 <u>Alert on Account Login Behavior Deviation</u> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

5.1.8 Ensure SSH IgnoreRhosts is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not be used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

Rationale:

Setting this parameter forces users to enter a password when authenticating with ssh.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep ignorerhosts

IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
IgnoreRhosts yes
```

Default Value:

IgnoreRhosts yes

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

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.		🟠	🔵

5.1.9 Ensure SSH HostbasedAuthentication is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `HostbasedAuthentication` parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

Rationale:

Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep hostbasedauthentication

HostbasedAuthentication no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
HostbasedAuthentication no
```

Default Value:

HostbasedAuthentication no

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	**16.3 Require Multi-factor Authentication** Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.1.10 Ensure SSH root login is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using ssh. The default is no.

Rationale:

Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo` or `su`. This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep permitrootlogin

PermitRootLogin no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitRootLogin no
```

Default Value:

PermitRootLogin without-password

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.	●	●	●

5.1.11 Ensure SSH PermitEmptyPasswords is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `PermitEmptyPasswords` parameter specifies if the SSH server allows login to accounts with empty password strings.

Rationale:

Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep permitemptypasswords

PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitEmptyPasswords no
```

Default Value:

PermitEmptyPasswords no

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.3 <u>Require MFA for Externally-Exposed Applications</u>** Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	**16.3 <u>Require Multi-factor Authentication</u>** Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

5.1.12 Ensure SSH PermitUserEnvironment is disabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `PermitUserEnvironment` option allows users to present environment options to the `ssh` daemon.

Rationale:

Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has `ssh` executing trojan'd programs)

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep permituserenvironment

PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
PermitUserEnvironment no
```

Default Value:

PermitUserEnvironment no

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

5.1.13 Ensure only strong Ciphers are used (Automated)

Profile Applicability:

- Level 1 - Server

Description:

This variable limits the ciphers that SSH can use during communication.

Rationale:

Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised

The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue

The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session

Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

The mm_newkeys_from_blob function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

Audit:

Run the following command and verify that output does not contain any of the listed weak ciphers

```
# sshd -T | grep ciphers
```

Weak Ciphers:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
```

Remediation:

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers
Example:

```
Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-
gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr
```

Default Value:

ciphers aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr

References:

1. https://nvd.nist.gov/vuln/detail/CVE-2016-2183
2. https://nvd.nist.gov/vuln/detail/CVE-2015-2808
3. https://www.kb.cert.org/vuls/id/565052
4. https://www.openssh.com/txt/cbc.adv
5. https://nvd.nist.gov/vuln/detail/CVE-2008-5161
6. https://nvd.nist.gov/vuln/detail/CVE-2013-4548
7. https://www.kb.cert.org/vuls/id/565052
8. https://www.openssh.com/txt/cbc.adv
9. SSHD_CONFIG(5)

Additional Information:

Some organizations may have stricter requirements for approved ciphers. Ensure that ciphers used are in compliance with site policy.

The only "strong" ciphers currently FIPS 140-2 compliant are: aes256-ctr,aes192-ctr,aes128-ctr

CVE-2013-4548 referenced above applies to OpenSSH versions 6.2 and 6.3. If running these versions of Open SSH, Please upgrade to version 6.4 or later to fix the vulnerability, or disable AES-GCM in the server configuration.

The Following are the supported ciphers in openSSH:

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
aes128-gcm@openssh.com
aes256-gcm@openssh.com
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se
chacha20-poly1305@openssh.com
```

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.		●	●

5.1.14 Ensure only strong MAC algorithms are used (Automated)

Profile Applicability:

- Level 2 - Server

Description:

This variable limits the types of MAC algorithms that SSH can use during communication.

Rationale:

MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Audit:

Run the following command and verify that output does not contain any of the listed weak MAC algorithms:

```
# sshd -T | grep -i "MACs"
```

Weak MAC algorithms:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the MACs line to contain a comma separated list of the site approved MACs
Example:

```
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-
512,hmac-sha2-256
```

Default Value:

macs umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-
etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-
256,hmac-sha2-512,hmac-sha1

References:

1. More information on SSH downgrade attacks can be found here:
   http://www.mitls.org/pages/attacks/SLOTH
2. SSHD_CONFIG(5)

Additional Information:

Some organizations may have stricter requirements for approved MACs. Ensure that
MACs used are in compliance with site policy.

The only "strong" MACs currently FIPS 140-2 approved are hmac-sha2-256 and hmac-
sha2-512

The Supported MACs are:

```
hmac-md5
hmac-md5-96
hmac-ripemd160
hmac-sha1
hmac-sha1-96
hmac-sha2-256
hmac-sha2-512
umac-64@openssh.com
umac-128@openssh.com
hmac-md5-etm@openssh.com
hmac-md5-96-etm@openssh.com
hmac-ripemd160-etm@openssh.com
hmac-sha1-etm@openssh.com
hmac-sha1-96-etm@openssh.com
hmac-sha2-256-etm@openssh.com
hmac-sha2-512-etm@openssh.com
umac-64-etm@openssh.com
umac-128-etm@openssh.com
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.10 <u>Encrypt Sensitive Data in Transit</u>** Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	**14.4 <u>Encrypt All Sensitive Information in Transit</u>** Encrypt all sensitive information in transit.		●	●
v7	**16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u>** Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

5.1.15 Ensure only strong Key Exchange algorithms are used (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received

Rationale:

Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Audit:

Run the following command and verify that output does not contain any of the listed weak Key Exchange algorithms

```
# sshd -T | grep kexalgorithms
```

Weak Key Exchange Algorithms:

```
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
```

Remediation:

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms
Example:

```
KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256
```

Default Value:

kexalgorithms curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

Additional Information:

Kex algorithms have a higher preference the earlier they appear in the list

Some organizations may have stricter requirements for approved Key exchange algorithms. Ensure that Key exchange algorithms used are in compliance with site policy.

The only Key Exchange Algorithms currently FIPS 140-2 approved are: ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

The Key Exchange algorithms supported by OpenSSH 7 are:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
```

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.		●	●

5.1.16 Ensure SSH Idle Timeout Interval is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions. When the `ClientAliveInterval` variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the `ClientAliveCountMax` variable is set, `sshd` will send client alive messages at every `ClientAliveInterval` interval. When the number of consecutive client alive messages are sent with no response from the client, the `ssh` session is terminated. For example, if the `ClientAliveInterval` is set to 15 seconds and the `ClientAliveCountMax` is set to 3, the client `ssh` session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's `ssh` session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening..

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for `ClientAliveCountMax` is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Audit:

Run the following commands and verify `ClientAliveInterval` is between 1 and 300 and `ClientAliveCountMax` is 3 or less:

```
# sshd -T | grep clientaliveinterval

ClientAliveInterval 300

# sshd -T | grep clientalivecountmax

ClientAliveCountMax 0
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameters according to site policy:

```
ClientAliveInterval 300

ClientAliveCountMax 0
```

Default Value:

ClientAliveInterval 420

ClientAliveCountMax 3

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.	●	●	●

5.1.17 Ensure SSH LoginGraceTime is set to one minute or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `LoginGraceTime` parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access.

Rationale:

Setting the `LoginGraceTime` parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Audit:

Run the following command and verify that output `LoginGraceTime` is between 1 and 60:

```
# sshd -T | grep logingracetime

LoginGraceTime 60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
LoginGraceTime 60
```

Default Value:

LoginGraceTime 120

CIS Controls:

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.	●	●	●

5.1.18 Ensure SSH warning banner is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `Banner` parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale:

Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep banner

Banner /etc/issue.net
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Banner /etc/issue.net
```

CIS Controls:

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.	●	●	●

5.1.19 Ensure SSH PAM is enabled (Automated)

Profile Applicability:

- Level 1 - Server

Description:

UsePAM Enables the Pluggable Authentication Module interface. If set to "yes" this will enable PAM authentication using ChallengeResponseAuthentication and PasswordAuthentication in addition to PAM account and session module processing for all authentication types

Rationale:

When usePAM is set to yes, PAM runs through account and session types properly. This is important if you want to restrict access to services based off of IP, time or other factors of the account. Additionally, you can make sure users inherit certain environment variables on login or disallow access to the server

Impact:

If UsePAM is enabled, you will not be able to run sshd(8) as a non-root user.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep -i usepam

usepam yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
UsePAM yes
```

Default Value:

usePAM yes

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.8** <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	**5.1** <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.1.20 Ensure SSH AllowTcpForwarding is disabled (Automated)

Profile Applicability:

- Level 2 - Server

Description:

SSH port forwarding is a mechanism in SSH for tunneling application ports from the client to the server, or servers to clients. It can be used for adding encryption to legacy applications, going through firewalls, and some system administrators and IT professionals use it for opening backdoors into the internal network from their home machines

Rationale:

Leaving port forwarding enabled can expose the organization to security risks and back-doors.

SSH connections are protected with strong encryption. This makes their contents invisible to most deployed network monitoring and traffic filtering solutions. This invisibility carries considerable risk potential if it is used for malicious purposes such as data exfiltration. Cybercriminals or malware could exploit SSH to hide their unauthorized communications, or to exfiltrate stolen data from the target network

Impact:

SSH tunnels are widely used in many corporate environments that employ mainframe systems as their application backends. In those environments the applications themselves may have very limited native support for security. By utilizing tunneling, compliance with SOX, HIPAA, PCI-DSS, and other standards can be achieved without having to modify the applications.

Audit:

Run the following command and verify that output matches:

```
# sshd -T | grep -i allowtcpforwarding

AllowTcpForwarding no
```

Remediation:

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

```
AllowTcpForwarding no
```

Default Value:

AllowTcpForwarding yes

References:

1. https://www.ssh.com/ssh/tunneling/example

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.	●	●	●
v8	**4.5 Implement and Manage a Firewall on End-User Devices** Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
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.		●	●

5.1.21 Ensure SSH MaxStartups is configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `MaxStartups` parameter specifies the maximum number of concurrent unauthenticated connections to the SSH daemon.

Rationale:

To protect a system from denial of service due to a large number of pending authentication connection attempts, use the rate limiting function of MaxStartups to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxStartups` is `10:30:60` or matches site policy:

```
# sshd -T | grep -i maxstartups
# maxstartups 10:30:60
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
maxstartups 10:30:60
```

CIS Controls:

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

5.1.22 Ensure SSH MaxSessions is set to 4 or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `MaxSessions` parameter specifies the maximum number of open sessions permitted from a given connection.

Rationale:

To protect a system from denial of service due to a large number of concurrent sessions, use the rate limiting function of MaxSessions to protect availability of sshd logins and prevent overwhelming the daemon.

Audit:

Run the following command and verify that output `MaxSessions` is 4 or less, or matches site policy:

```
# sshd -T | grep -i maxsessions
# maxsessions 4
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
MaxSessions 4
```

CIS Controls:

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

5.2 Configure PAM

PAM (Pluggable Authentication Modules) is a service that implements modular authentication modules on UNIX systems. PAM is implemented as a set of shared objects that are loaded and executed when a program needs to authenticate a user. Files for PAM are typically located in the `/etc/pam.d` directory. PAM must be carefully configured to secure system authentication. While this section covers some of PAM, please consult other PAM resources to fully understand the configuration capabilities.

Note: `/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make configuration changes persistent across reboots. After a reboot, configuration changes need to be reapplied.

5.2.1 Ensure password creation requirements are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `pam_passwdqc.so` module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more based on the following options set in the `/etc/security/passwdqc.conf`:

- `min=disabled,disabled,disabled,disabled,14` - The password must be 14 characters or more and consists of four character classes.
- `max=40` - The maximum allowed password length is 40.
- `passphrase=3` - The number of words required for a passphrase is at least 3.
- `match=4` - The length of common substring required to conclude that a password is at least partially based on information found in a character string is 4.
- `similar=deny` - The password that is similar to the old one is going to be denied.
- `random=47` - The size of randomly-generated passphrases in bits is 47.
- `enforce=everyone` - Warn everyone for weak passwords.
- `retry=3` - Let the user provide a password 3 times if the user fails to provide a sufficiently strong password and enter it twice the first time.

For more details, refer to pam_passwdqc module documentation. The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.

Rationale:

Strong passwords protect systems from being hacked through brute force methods.

Audit:

Verify password creation requirements conform to organization policy in `/etc/security/passwdqc.conf` with the following command.

```
# cat /etc/security/passwdqc.conf

min=disabled,disabled,disabled,disabled,14
max=40
passphrase=3
match=4
similar=deny
random=47
enforce=everyone
retry=3
```

Run the following command and verify that the output is similar to:

```
grep  pam_passwdqc.so /etc/pam.d/system-auth
password        required        pam_passwdqc.so
config=/etc/security/passwdqc.conf
```

Remediation:

Edit the file /etc/security/passwdqc.conf and add or modify the following lines for password length and complexity to conform to site policy:

```
min=disabled,disabled,disabled,disabled,14
max=40
passphrase=3
match=4
similar=deny
random=47
enforce=everyone
retry=3
```

Edit the /etc/pam.d/system-auth files to include the appropriate options for pam_passwdqc.so and to conform to site policy:

```
password        required        pam_passwdqc.so
config=/etc/security/passwdqc.conf
```

Additional Information:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation requirements only cover including try_first_pass and minlen set to 14 or more.

Settings in /etc/security/pwquality.conf must use spaces around the = symbol.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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.	●	●	●

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.		●	●

5.2.2 Ensure password reuse is limited (Manual)

Profile Applicability:

- Level 2 - Server

Description:

The `/etc/security/opasswd` file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords.

Rationale:

Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password.

Note that these change only apply to accounts configured on the local system.

Audit:

Verify remembered password history is 5 or more. This setting is commonly configured with the `pam_unix.so` or `pam_pwhistory.so remember` options found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` . Examples:

```
password required pam_pwhistory.so remember=5
password required pam_unix.so remember=5
```

Remediation:

Set remembered password history to conform to site policy. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_pwhistory.so` or `pam_unix.so` lines to include the `remember` option:

```
password required pam_pwhistory.so remember=5
password required pam_unix.so remember=5
```

Additional Information:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

5.2.3 Ensure password hashing algorithm is SHA-512 (Manual)

Profile Applicability:

- Level 2 - Server

Description:

The commands below change password encryption from `md5` to `sha512` (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.

Rationale:

The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

Note that these changes only apply to accounts configured on the local system.

Audit:

Verify password hashing algorithm is sha512. This setting is commonly configured with the `pam_unix.so sha512` option found in `/etc/pam.d/common-password` or `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth` . Example:

```
password required pam_unix.so sha512
```

Remediation:

Set password hashing algorithm to sha512. Many distributions provide tools for updating PAM configuration, consult your documentation for details. If no tooling is provided edit the appropriate `/etc/pam.d/` configuration file and add or modify the `pam_unix.so` lines to include the sha512 option:

```
password required pam_unix.so sha512
```

Additional Information:

Consult your documentation for the appropriate PAM file and module.

Additional module options may be set, recommendation only covers those listed here.

If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login. To accomplish that, the following commands can be used. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# cat /etc/passwd | awk -F: '( $3 >= 500 && $1 != "nfsnobody" ) { print $1 }'
| xargs -n 1 chage -d 0
```

This command assumes a system UID split at 500. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 <u>Encrypt Sensitive Data at Rest</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.3 User Accounts and Environment

This section provides guidance on setting up secure defaults for system and user accounts and their environment.

5.3.1 Set Shadow Password Suite Parameters

While a majority of the password control parameters have been moved to PAM, some parameters are still available through the shadow password suite. Any changes made to `/etc/login.defs` will only be applied if the `usermod` command is used. If user IDs are added a different way, use the `chage` command to effect changes to individual user IDs.

Note: `/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make configuration changes persistent across reboots. After a reboot, configuration changes need to be reapplied.

5.3.1.1 Ensure password expiration is 365 days or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `PASS_MAX_DAYS` parameter in `/etc/login.defs` allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the `PASS_MAX_DAYS` parameter be set to less than or equal to 365 days.

Rationale:

The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Audit:

Run the following command and verify `PASS_MAX_DAYS` conforms to site policy (no more than 365 days):

```
# grep PASS_MAX_DAYS /etc/login.defs

PASS_MAX_DAYS 365
```

Run the following command and Review list of users and PASS_MAX_DAYS to verify that all users' PASS_MAX_DAYS conforms to site policy (no more than 365 days):

```
# grep -E '^[^:]+:[^!*]' /etc/shadow | cut -d: -f1,5

<user>:<PASS_MAX_DAYS>
```

Remediation:

Set the `PASS_MAX_DAYS` parameter to conform to site policy in `/etc/login.defs` :

```
PASS_MAX_DAYS 365
```

Modify user parameters for all users with a password set to match:

```
# chage --maxdays 365 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 5th field should be 365 or less for all users with a password.

Note: A value of -1 will disable password expiration. Additionally the password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

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.		●	●

5.3.1.2 Ensure minimum days between password changes is 7 or more (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `PASS_MIN_DAYS` parameter in `/etc/login.defs` allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that `PASS_MIN_DAYS` parameter be set to 7 or more days.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

Run the following command and verify `PASS_MIN_DAYS` conforms to site policy (no less than 7 days):

```
# grep PASS_MIN_DAYS /etc/login.defs

PASS_MIN_DAYS 7
```

Run the following command and Review list of users and PAS_MIN_DAYS to Verify that all users' PAS_MIN_DAYS conform s to site policy (no less than 7 days):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,4

<user>:<PASS_MIN_DAYS>
```

Remediation:

Set the `PASS_MIN_DAYS` parameter to 7 in `/etc/login.defs` :

```
PASS_MIN_DAYS 7
```

Modify user parameters for all users with a password set to match:

```
# chage --mindays 7 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 4th field should be 7 or more for all users with a password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> 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** <u>Use Unique Passwords</u> 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.		●	●

5.3.1.3 Ensure password expiration warning days is 7 or more (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `PASS_WARN_AGE` parameter in `/etc/login.defs` allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the `PASS_WARN_AGE` parameter be set to 7 or more days.

Rationale:

Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.

Audit:

Run the following command and verify `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep PASS_WARN_AGE /etc/login.defs

PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:
Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,6

<user>:<PASS_WARN_AGE>
```

Remediation:

Set the `PASS_WARN_AGE` parameter to 7 in `/etc/login.defs` :

```
PASS_WARN_AGE 7
```

Modify user parameters for all users with a password set to match:

```
# chage --warndays 7 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 6th field should be 7 or more for all users with a password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2 <u>Use Unique Passwords</u>** 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 <u>Use Unique Passwords</u>** 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.		●	●

5.3.1.4 Ensure inactive password lock is 30 days or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled.

Rationale:

Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Audit:

Run the following command and verify `INACTIVE` conforms to sire policy (no more than 30 days):

```
# useradd -D | grep INACTIVE

INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires:
Run the following command and Review list of users and INACTIVE to verify that all users' INACTIVE conforms to site policy (no more than 30 days):

```
# grep -E ^[^:]+:[^\!*] /etc/shadow | cut -d: -f1,7

<user>:<INACTIVE>
```

Remediation:

Run the following command to set the default password inactivity period to 30 days:

```
# useradd -D -f 30
```

Modify user parameters for all users with a password set to match:

```
# chage --inactive 30 <user>
```

Additional Information:

You can also check this setting in `/etc/shadow` directly. The 7th field should be 30 or less for all users with a password.

Note: A value of -1 would disable this setting.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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 <u>Use Unique Passwords</u> 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.		●	●

5.3.1.5 Ensure all users last password change date is in the past (Automated)

Profile Applicability:

- Level 1 - Server

Description:

All users should have a password change date in the past.

Rationale:

If a users recorded password change date is in the future then they could bypass any set password expiration.

Audit:

Run the following command and verify nothing is returned

```
# for usr in $(cut -d: -f1 /etc/shadow); do [[ $(chage --list $usr | grep
'^Last password change' | cut -d: -f2) > $(date) ]] && echo "$usr :$(chage --
list $usr | grep '^Last password change' | cut -d: -f2)"; done
```

Remediation:

Investigate any users with a password change date in the future and correct them. Locking the account, expiring the password, or resetting the password manually may be appropriate.

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.		●	●

5.3.2 Ensure system accounts are secured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

There are a number of accounts provided with most distributions that are used to manage applications and are not intended to provide an interactive shell.

Rationale:

It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default, most distributions set the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to the `nologin` shell. This prevents the account from potentially being used to run any commands.

Audit:

Run the following commands and verify no results are returned:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" &&
$1!~/^\+/ && $3>='"$(awk '/^\s*SYS_UID_MIN/{print $2}' /etc/login.defs)"' &&
$3<='"$(awk '/^\s*SYS_UID_MAX/{print $2}' /etc/login.defs)"' &&
$7!="'"$(which nologin)"'" && $7!="/bin/false") {print}' /etc/passwd
awk -F: '($1!="root" && $1!~/^\+/ && $3>='"$(awk '/^\s*SYS_UID_MIN/{print
$2}' /etc/login.defs)"' && $3<='"$(awk '/^\s*SYS_UID_MAX/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

Remediation:

Run the commands appropriate for your distribution:
Set the shell for any accounts returned by the audit to nologin:

```
# usermod -s $(which nologin) <user>
```

Lock any non root accounts returned by the audit:

```
# usermod -L <user>
```

The following command will set all system accounts to a non login shell:

```
awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" &&
$1!~/^\+/ && $3>='"$(awk '/^\s*SYS_UID_MIN/{print $2}' /etc/login.defs)"' &&
$3<='"$(awk '/^\s*SYS_UID_MAX/{print $2}' /etc/login.defs)"' &&
$7!="'"$(which nologin)"'" && $7!="/bin/false") {print $1}' /etc/passwd |
while read user; do usermod -s $(which nologin) $user; done
```

The following command will automatically lock not root system accounts:

```
awk -F: '($1!="root" && $1!~/^\+/ && $3>='"$(awk '/^\s*SYS_UID_MIN/{print
$2}' /etc/login.defs)"' && $3<='"$(awk '/^\s*SYS_UID_MAX/{print $2}'
/etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}' | while read user; do usermod -L
$user; done
```

Additional Information:

The `root`, `sync`, `shutdown`, and `halt` users are exempted from requiring a non-login shell.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**6.1 Establish an Access Granting Process** Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●

5.3.3 Ensure default group for the root account is GID 0 (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.

Rationale:

Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.

Audit:

Run the following command and verify the result is 0 :

```
# grep "^root:" /etc/passwd | cut -f4 -d:
0
```

Remediation:

Run the following command to set the root user default group to GID 0 :

```
# usermod -g 0 root
```

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

5.3.4 Ensure default user umask is 027 or more restrictive (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The default `umask` determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the `umask` command into the standard shell configuration files (`.profile` , `.bashrc` , etc.) in their home directories.

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of `077` causes files and directories created by users to not be readable by any other user on the system. A `umask` of `027` would make files and directories readable by users in the same Unix group, while a `umask` of `022` would make files readable by every user on the system.

Audit:

Run the following commands and verify all umask lines returned are 027 or more restrictive.

```
# grep "umask" /etc/bash/bashrc
umask 027
# grep "umask" /etc/profile /etc/profile.d/*.sh
umask 027
```

Remediation:

Edit the `/etc/bash/bashrc`, `/etc/profile` and `/etc/profile.d/*.sh` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
umask 027
```

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

Other methods of setting a default user umask exist however the shell configuration files are the last run and will override other settings if they exist therefor our recommendation is to configure in the shell configuration files. If other methods are in use in your environment they should be audited and the shell configs should be verified to not override.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.3.5 Ensure default user shell timeout is 900 seconds or less (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The default `TMOUT` determines the shell timeout for users. The TMOUT value is measured in seconds.

Rationale:

Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Audit:

Run the following commands and verify all TMOUT lines returned are 900 or less and at least one exists in each file.

```
# grep "^TMOUT" /etc/bash/bashrc
TMOUT=900

# grep "^TMOUT" /etc/profile
TMOUT=900
```

Remediation:

Edit the `/etc/bash/bashrc` and `/etc/profile` files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:

```
TMOUT=900
```

Additional Information:

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

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.	●	●	●

5.4 Ensure root login is restricted to system console (Manual)

Profile Applicability:

- Level 1 - Server

Description:

The file `/etc/securetty` contains a list of valid terminals that may be logged in directly as root.

Rationale:

Since the system console has special properties to handle emergency situations, it is important to ensure that the console is in a physically secure location and that unauthorized consoles have not been defined.

Audit:

```
# cat /etc/securetty
```

Remediation:

Remove entries for any consoles that are not in a physically secure location.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

5.5 Ensure access to the su command is restricted (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in the wheel group to execute `su`.

Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

Audit:

Run the following command and verify output includes matching line:

```
# grep pam_wheel.so /etc/pam.d/su
auth required pam_wheel.so use_uid
```

Run the following command and verify users in `wheel` group match site policy:

```
# grep wheel /etc/group
wheel:!:10:root,<user list>
```

Remediation:

Add the following line to the `/etc/pam.d/su` file:

```
auth required pam_wheel.so use_uid
```

Create a comma separated list of users in the wheel statement in the `/etc/group` file:

```
wheel:!:10:root,<user list>
```

`/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make these changes persistent across reboots. The steps mentioned above needs to be performed after every boot.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

6 System Maintenance

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

Note: `/etc` is stateless on Container-Optimized OS. Therefore, `/etc` cannot be used to make configuration changes persistent across reboots. After a reboot, configuration changes need to be reapplied.

6.1 System File Permissions

This section provides guidance on securing aspects of system files and directories.

6.1.1 Ensure permissions on /etc/passwd are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

Rationale:

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` :

```
# stat /etc/passwd
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd` :

```
# chown root:root /etc/passwd
# chmod 644 /etc/passwd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.2 Ensure permissions on /etc/shadow are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

Audit:

Run the following command and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow,` and `Access` is `640` or more restrictive:

```
# stat /etc/shadow
Access: (0640/-rw-r-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/shadow` :

```
# chown root:root /etc/shadow
# chown root:shadow /etc/shadow

# chmod o-rwx,g-wx /etc/shadow
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.3 Ensure permissions on /etc/group are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

Rationale:

The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

Audit:

Run the following command and verify Uid and Gid are both 0/root and Access is 644 :

```
# stat /etc/group
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on /etc/group :

```
# chown root:root /etc/group
# chmod 644 /etc/group
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.4 Ensure permissions on /etc/gshadow are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

Audit:

Run the following command and verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow,` and `Access` is `640` or more restrictive:

```
# stat /etc/gshadow
Access: (0640/-rw-r-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/gshadow` :

```
# chown root:root /etc/gshadow
# chown root:shadow /etc/gshadow

# chmod o-rwx,g-rw /etc/gshadow
```

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	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.5 Ensure permissions on /etc/passwd- are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `/etc/passwd-` file contains backup user account information.

Rationale:

It is critical to ensure that the `/etc/passwd-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/passwd-
Access: (0644/-rw-r--r--)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/passwd-` :

```
# chown root:root /etc/passwd-

# chmod u-x,go-wx /etc/passwd-
```

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	**16.4 Encrypt or Hash all Authentication Credentials** Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.6 Ensure permissions on /etc/shadow- are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow`, and `Access` is `640` or more restrictive:

```
# stat /etc/shadow-
Access: (0640/-rw-r-----)  Uid: (     0/     root)  Gid: (     0/     root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/shadow-` :

```
# chown root:root /etc/shadow-
# chown root:shadow /etc/shadow-

# chmod o-rwx,g-rw /etc/shadow-
```

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	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.7 Ensure permissions on /etc/group- are configured (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

Rationale:

It is critical to ensure that the `/etc/group-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify `Uid` and `Gid` are both `0/root` and `Access` is `644` or more restrictive:

```
# stat /etc/group-
Access: (0644/-rw-------)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the following command to set permissions on `/etc/group-` :

```
# chown root:root /etc/group-
# chmod u-x,go-wx /etc/group-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> 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	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.1.8 Ensure permissions on /etc/gshadow- are configured (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

Rationale:

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

Audit:

Run the following command and verify verify `Uid` is `0/root`, `Gid` is `0/root` or `<gid>/shadow,` and `Access` is `640` or more restrictive:

```
# stat /etc/gshadow-
Access: (0640/-rw-r-----)  Uid: (    0/    root)  Gid: (    0/    root)
```

Remediation:

Run the one of the following chown commands as appropriate and the chmod to set permissions on `/etc/gshadow-` :

```
# chown root:root /etc/gshadow-
# chown root:shadow /etc/gshadow-

# chmod o-rwx,g-rw /etc/gshadow-
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**3.3** <u>Configure Data Access Control Lists</u> 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	**16.4** <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.2 User and Group Settings

This section provides guidance on securing aspects of the users and groups.

Note: The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

6.2.1 Ensure password fields are not empty (Automated)

Profile Applicability:

- Level 1 - Server

Description:

An account with an empty password field means that anybody may log in as that user without providing a password.

Rationale:

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

Audit:

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow
```

Remediation:

If any accounts in the /etc/shadow file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**5.2** <u>Use Unique Passwords</u> 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** <u>Use Unique Passwords</u> 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.		●	●

6.2.2 Ensure no legacy "+" entries exist in /etc/passwd (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep '^\+:' /etc/passwd
```

Remediation:

Remove any legacy '+' entries from `/etc/passwd` if they exist.

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.		●	●

6.2.3 Ensure no legacy "+" entries exist in /etc/shadow (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep '^\+:' /etc/shadow
```

Remediation:

Remove any legacy '+' entries from /etc/shadow if they exist.

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.		●	●

6.2.4 Ensure no legacy "+" entries exist in /etc/group (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.

Rationale:

These entries may provide an avenue for attackers to gain privileged access on the system.

Audit:

Run the following command and verify that no output is returned:

```
# grep '^\+:' /etc/group
```

Remediation:

Remove any legacy '+' entries from `/etc/group` if they exist.

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.		●	●

6.2.5 Ensure root is the only UID 0 account (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Any account with UID 0 has superuser privileges on the system.

Rationale:

This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.

Audit:

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd

root
```

Remediation:

Remove any users other than root with UID 0 or assign them a new UID if appropriate.

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

6.2.6 Ensure root PATH Integrity (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.

Rationale:

Including the current working directory (.) or other writable directory in root 's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.

Audit:

Run the following script and verify no results are returned:

```bash
#!/bin/bash

PATH="$(sudo -Hiu root env | grep '^PATH' | cut -d= -f2)"
echo "$PATH" | grep -q "::" && echo "Empty directory in PATH (::)"
echo "$PATH" | grep -q ":$" && echo "Trailing : in PATH"
for dir in $(echo "$PATH" | tr ":" " "); do
   if [ -d "$dir" ]; then
      ls -ldH "$dir" | awk 'substr($1,6,1) != "-" {print $9, "is group
writable"}
      substr($1,9,1) != "-" {print $9, "is world writable"}
      $3 != "root" {print $9, "is not owned by root"}'
   else
      base_dir=$(echo "$dir" | cut -d "/" -f2)
      # Ignore if directory is on read-only partition
      rw=$(findmnt -T "/$base_dir" | sed '1d' | grep -v "\sro,")
      if [ -n "$rw" ]; then
         echo "$dir is not a directory"
      fi
   fi
done
```

Remediation:

Correct or justify any items discovered in the Audit step.

CIS Controls:

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

6.2.7 Ensure all users' home directories exist (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

Rationale:

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read -r user
dir; do
        if [ ! -d "$dir" ]; then
                echo "The home directory ($dir) of user $user does not exist."
        fi
done
```

Remediation:

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Additional Information:

The audit script checks all users UID 500 and above except nfsnobody. Some distributions split at `UID 1000` instead, consult your documentation and/or the `UID_MIN` setting in `/etc/login.defs` to determine which is appropriate for you.

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

CIS Controls:

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

6.2.8 Ensure users' home directories permissions are 750 or more restrictive (Automated)

Profile Applicability:

- Level 2 - Server

Description:

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash
grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    dirperm=$(ls -ld $dir | cut -f1 -d" ")
    if [ $(echo $dirperm | cut -c6) != "-" ]; then
      echo "Group Write permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c8) != "-" ]; then
      echo "Other Read permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c9) != "-" ]; then
      echo "Other Write permission set on the home directory ($dir) of user
$user"
    fi
    if [ $(echo $dirperm | cut -c10) != "-" ]; then
      echo "Other Execute permission set on the home directory ($dir) of user
$user"
    fi
  fi
done
```

Remediation:

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Additional Information:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

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	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.	●	●	●

6.2.9 Ensure users own their home directories (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

Rationale:

Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
   owner=$(stat -L -c "%U" "$dir")
   if [ "$owner" != "$user" ]; then
     echo "The home directory ($dir) of user $user is owned by $owner."
   fi
 fi
done
```

Remediation:

Change the ownership of any home directories that are not owned by the defined user to the correct user.

Additional Information:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

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	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.	●	●	●

6.2.10 Ensure users' dot files are not group or world writable (Automated)

Profile Applicability:

- Level 2 - Server

Description:

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which
nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user
dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.[A-Za-z0-9]*; do
      if [ ! -h "$file" -a -f "$file" ]; then
        fileperm=$(ls -ld $file | cut -f1 -d" ")

        if [ $(echo $fileperm | cut -c6)  != "-" ]; then
          echo "Group Write permission set on file $file"
        fi
        if [ $(echo $fileperm | cut -c9)  != "-" ]; then
          echo "Other Write permission set on file $file"
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

Additional Information:

On some distributions the `/sbin/nologin` should be replaced with
`/usr/sbin/nologin`.

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	**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.	●	●	●

6.2.11 Ensure no users have .forward files (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `.forward` file specifies an email address to forward the user's mail to.

Rationale:

Use of the `.forward` file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The `.forward` file also poses a risk as it can be used to execute commands that may perform unintended actions.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then
      echo ".forward file $dir/.forward exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.forward` files and determine the action to be taken in accordance with site policy.

Additional Information:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

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.	●	●	●

6.2.12 Ensure no users have .netrc files (Automated)

Profile Applicability:

- Level 2 - Server

Description:

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

Rationale:

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then
      echo ".netrc file $dir/.netrc exists"
    fi
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user `.netrc` files and determine the action to be taken in accordance with site policy.

Additional Information:

On some distributions the `/sbin/nologin` should be replaced with `/usr/sbin/nologin`.

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	**16.4 Encrypt or Hash all Authentication Credentials** Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.2.13 Ensure users' .netrc Files are not group or world accessible (Automated)

Profile Applicability:

- Level 2 - Server

Description:

While the system administrator can establish secure permissions for users' `.netrc` files, the users can easily override these.

Rationale:

`.netrc` files may contain unencrypted passwords that may be used to attack other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.netrc; do
      if [ ! -h "$file" -a -f "$file" ]; then
        fileperm=$(ls -ld $file | cut -f1 -d" ")
        if [ $(echo $fileperm | cut -c5)  != "-" ]; then
          echo "Group Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c6)  != "-" ]; then
          echo "Group Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c7)  != "-" ]; then
          echo "Group Execute set on $file"
        fi
        if [ $(echo $fileperm | cut -c8)  != "-" ]; then
          echo "Other Read set on $file"
        fi
        if [ $(echo $fileperm | cut -c9)  != "-" ]; then
          echo "Other Write set on $file"
        fi
        if [ $(echo $fileperm | cut -c10)  != "-" ]; then
          echo "Other Execute set on $file"
        fi
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc file permissions and determine the action to be taken in accordance with site policy.

Additional Information:

While the complete removal of .netrc files is recommended if any are required on the system secure permissions must be applied.

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

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	**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.	●	●	●

6.2.14 Ensure no users have .rhosts files (Automated)

Profile Applicability:

- Level 2 - Server

Description:

While no .rhosts files are shipped by default, users can easily create them.

Rationale:

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 !=
"'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while
read user dir; do
  if [ ! -d "$dir" ]; then
    echo "The home directory ($dir) of user $user does not exist."
  else
    for file in $dir/.rhosts; do
      if [ ! -h "$file" -a -f "$file" ]; then
        echo ".rhosts file in $dir"
      fi
    done
  fi
done
```

Remediation:

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.

Additional Information:

On some distributions the /sbin/nologin should be replaced with /usr/sbin/nologin.

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	**16.4 Encrypt or Hash all Authentication Credentials** Encrypt or hash with a salt all authentication credentials when stored.		●	●

6.2.15 Ensure all groups in /etc/passwd exist in /etc/group (Automated)

Profile Applicability:

- Level 2 - Server

Description:

Over time, system administration errors and changes can lead to groups being defined in `/etc/passwd` but not in `/etc/group` .

Rationale:

Groups defined in the `/etc/passwd` file but not in the `/etc/group` file pose a threat to system security since group permissions are not properly managed.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
  grep -q ":$i:" /etc/group
  if [ $? -ne 0 ]; then
    echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
  fi
done
```

Remediation:

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

6.2.16 Ensure no duplicate UIDs exist (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

Rationale:

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    users=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs)
    echo "Duplicate UID ($2): $users"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

6.2.17 Ensure no duplicate GIDs exist (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

Rationale:

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f3 -d":" /etc/group | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    groups=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/group | xargs)
    echo "Duplicate GID ($2): $groups"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

Additional Information:

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

6.2.18 Ensure no duplicate user names exist (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

Rationale:

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd` . For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f1 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    uids=$(awk -F: '($1 == n) { print $3 }' n=$2 /etc/passwd | xargs)
    echo "Duplicate User Name ($2): $uids"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

6.2.19 Ensure no duplicate group names exist (Automated)

Profile Applicability:

- Level 1 - Server

Description:

Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.

Rationale:

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group . Effectively, the GID is shared, which is a security problem.

Audit:

Run the following script and verify no results are returned:

```bash
#!/bin/bash

cut -f1 -d":" /etc/group | sort -n | uniq -c | while read x ; do
  [ -z "$x" ] && break
  set - $x
  if [ $1 -gt 1 ]; then
    gids=$(gawk -F: '($1 == n) { print $3 }' n=$2 /etc/group | xargs)
    echo "Duplicate Group Name ($2): $gids"
  fi
done
```

Remediation:

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

6.2.20 Ensure shadow group is empty (Automated)

Profile Applicability:

- Level 1 - Server

Description:

The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group.

Rationale:

Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert additional user accounts.

Audit:

Run the following commands and verify no results are returned:

```
# grep ^shadow:[^:]*:[^:]*:[^:]+ /etc/group
# awk -F: '($4 == "<shadow-gid>") { print }' /etc/passwd
```

Remediation:

Remove all users from the shadow group, and change the primary group of any users with shadow as their primary group.

CIS Controls:

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.	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Initial Setup**		
1.1	**Filesystem Configuration**		
1.1.1	**Disable unused filesystems**		
1.1.1.1	Ensure mounting of udf filesystems is disabled (Automated)	☐	☐
1.1.2	Ensure /tmp is configured (Automated)	☐	☐
1.1.3	Ensure nodev option set on /tmp partition (Automated)	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition (Automated)	☐	☐
1.1.5	Ensure noexec option set on /tmp partition (Automated)	☐	☐
1.1.6	Ensure nosuid option set on /var partition (Automated)	☐	☐
1.1.7	Ensure noexec option set on /var partition (Automated)	☐	☐
1.1.8	Ensure nodev option set on /var partition (Automated)	☐	☐
1.1.9	Ensure nodev option set on /home partition (Automated)	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition (Automated)	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition (Automated)	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition (Automated)	☐	☐
1.1.13	Disable Automounting (Automated)	☐	☐
1.2	**Filesystem Integrity Checking**		
1.2.1	Ensure dm-verity is enabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.3	**Secure Boot Settings**		
1.3.1	Ensure authentication required for single user mode (Automated)	☐	☐
1.4	**Additional Process Hardening**		
1.4.1	Ensure core dumps are restricted (Automated)	☐	☐
1.4.2	Ensure XD/NX support is enabled (Automated)	☐	☐
1.4.3	Ensure address space layout randomization (ASLR) is enabled (Automated)	☐	☐
1.5	**Warning Banners**		
1.5.1	**Command Line Warning Banners**		
1.5.1.1	Ensure message of the day is configured properly (Automated)	☐	☐
1.5.1.2	Ensure local login warning banner is configured properly (Automated)	☐	☐
1.5.1.3	Ensure remote login warning banner is configured properly (Automated)	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured (Automated)	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured (Automated)	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured (Automated)	☐	☐
1.6	Ensure AppArmor is installed (Automated)	☐	☐
2	**Services**		
2.1	**Special Purpose Services**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.1	**Time Synchronization**		
2.1.1.1	Ensure time synchronization is in use (Manual)	☐	☐
2.1.1.2	Ensure chrony is configured (Automated)	☐	☐
2.1.2	Ensure X Window System is not installed (Automated)	☐	☐
2.1.3	Ensure NFS and RPC are not enabled (Automated)	☐	☐
2.1.4	Ensure rsync service is not enabled (Automated)	☐	☐
3	**Network Configuration**		
3.1	**Network Parameters (Host Only)**		
3.1.1	Ensure packet redirect sending is disabled (Automated)	☐	☐
3.2	**Network Parameters (Host and Router)**		
3.2.1	Ensure source routed packets are not accepted (Automated)	☐	☐
3.2.2	Ensure ICMP redirects are not accepted (Automated)	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted (Automated)	☐	☐
3.2.4	Ensure suspicious packets are logged (Automated)	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored (Automated)	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored (Automated)	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled (Automated)	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled (Automated)	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.3	**Firewall Configuration**		
3.3.1	**Configure IPv6 ip6tables**		
3.3.1.1	Ensure IPv6 default deny firewall policy (Automated)	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured (Automated)	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured (Manual)	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports (Manual)	☐	☐
3.3.2	**Configure IPv4 iptables**		
3.3.2.1	Ensure default deny firewall policy (Automated)	☐	☐
3.3.2.2	Ensure loopback traffic is configured (Automated)	☐	☐
3.3.2.3	Ensure outbound and established connections are configured (Manual)	☐	☐
3.3.3	Ensure iptables is installed (Automated)	☐	☐
4	**Logging and Auditing**		
4.1	**Configure Logging**		
4.1.1	**Configure logging agent**		
4.1.1.1	Ensure correct container image is set for stackdriver logging agent (Automated)	☐	☐
4.1.1.2	Ensure Logging Service is Running (Manual)	☐	☐
4.1.1.3	Ensure logging is configured (Manual)	☐	☐
4.1.2	**Configure journald**		
4.1.2.1	Ensure journald is configured to compress large log files (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk (Automated)	☐	☐
4.1.3	Ensure permissions on all logfiles are configured (Automated)	☐	☐
4.2	Ensure logrotate is configured (Manual)	☐	☐
5	**Access, Authentication and Authorization**		
5.1	**SSH Server Configuration**		
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured (Automated)	☐	☐
5.1.3	Ensure permissions on SSH public host key files are configured (Automated)	☐	☐
5.1.4	Ensure SSH Protocol is set to 2 (Automated)	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate (Automated)	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled (Automated)	☐	☐
5.1.7	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled (Automated)	☐	☐
5.1.9	Ensure SSH HostbasedAuthentication is disabled (Automated)	☐	☐
5.1.10	Ensure SSH root login is disabled (Automated)	☐	☐
5.1.11	Ensure SSH PermitEmptyPasswords is disabled (Automated)	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.13	Ensure only strong Ciphers are used (Automated)	☐	☐
5.1.14	Ensure only strong MAC algorithms are used (Automated)	☐	☐
5.1.15	Ensure only strong Key Exchange algorithms are used (Automated)	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured (Automated)	☐	☐
5.1.17	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	☐	☐
5.1.18	Ensure SSH warning banner is configured (Automated)	☐	☐
5.1.19	Ensure SSH PAM is enabled (Automated)	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled (Automated)	☐	☐
5.1.21	Ensure SSH MaxStartups is configured (Automated)	☐	☐
5.1.22	Ensure SSH MaxSessions is set to 4 or less (Automated)	☐	☐
5.2	**Configure PAM**		
5.2.1	Ensure password creation requirements are configured (Automated)	☐	☐
5.2.2	Ensure password reuse is limited (Manual)	☐	☐
5.2.3	Ensure password hashing algorithm is SHA-512 (Manual)	☐	☐
5.3	**User Accounts and Environment**		
5.3.1	**Set Shadow Password Suite Parameters**		
5.3.1.1	Ensure password expiration is 365 days or less (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3.1.2	Ensure minimum days between password changes is 7 or more (Automated)	☐	☐
5.3.1.3	Ensure password expiration warning days is 7 or more (Automated)	☐	☐
5.3.1.4	Ensure inactive password lock is 30 days or less (Automated)	☐	☐
5.3.1.5	Ensure all users last password change date is in the past (Automated)	☐	☐
5.3.2	Ensure system accounts are secured (Automated)	☐	☐
5.3.3	Ensure default group for the root account is GID 0 (Automated)	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive (Automated)	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less (Automated)	☐	☐
5.4	Ensure root login is restricted to system console (Manual)	☐	☐
5.5	Ensure access to the su command is restricted (Automated)	☐	☐
6	**System Maintenance**		
6.1	**System File Permissions**		
6.1.1	Ensure permissions on /etc/passwd are configured (Automated)	☐	☐
6.1.2	Ensure permissions on /etc/shadow are configured (Automated)	☐	☐
6.1.3	Ensure permissions on /etc/group are configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1.4	Ensure permissions on /etc/gshadow are configured (Automated)	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured (Automated)	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured (Automated)	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured (Automated)	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured (Automated)	☐	☐
6.2	**User and Group Settings**		
6.2.1	Ensure password fields are not empty (Automated)	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd (Automated)	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow (Automated)	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group (Automated)	☐	☐
6.2.5	Ensure root is the only UID 0 account (Automated)	☐	☐
6.2.6	Ensure root PATH Integrity (Automated)	☐	☐
6.2.7	Ensure all users' home directories exist (Automated)	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive (Automated)	☐	☐
6.2.9	Ensure users own their home directories (Automated)	☐	☐
6.2.10	Ensure users' dot files are not group or world writable (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2.11	Ensure no users have .forward files (Automated)	☐	☐
6.2.12	Ensure no users have .netrc files (Automated)	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible (Automated)	☐	☐
6.2.14	Ensure no users have .rhosts files (Automated)	☐	☐
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	☐	☐
6.2.16	Ensure no duplicate UIDs exist (Automated)	☐	☐
6.2.17	Ensure no duplicate GIDs exist (Automated)	☐	☐
6.2.18	Ensure no duplicate user names exist (Automated)	☐	☐
6.2.19	Ensure no duplicate group names exist (Automated)	☐	☐
6.2.20	Ensure shadow group is empty (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure core dumps are restricted	☐	☐
1.5.1.1	Ensure message of the day is configured properly	☐	☐
1.5.1.2	Ensure local login warning banner is configured properly	☐	☐
1.5.1.3	Ensure remote login warning banner is configured properly	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
3.1.1	Ensure packet redirect sending is disabled	☐	☐
3.2.1	Ensure source routed packets are not accepted	☐	☐
3.2.2	Ensure ICMP redirects are not accepted	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
3.2.4	Ensure suspicious packets are logged	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐
4.1.3	Ensure permissions on all logfiles are configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.17	Ensure SSH LoginGraceTime is set to one minute or less	☐	☐
5.1.18	Ensure SSH warning banner is configured	☐	☐
5.1.19	Ensure SSH PAM is enabled	☐	☐
5.1.21	Ensure SSH MaxStartups is configured	☐	☐
5.1.22	Ensure SSH MaxSessions is set to 4 or less	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.6	Ensure root PATH Integrity	☐	☐
6.2.7	Ensure all users' home directories exist	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐
6.2.20	Ensure shadow group is empty	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	☐	☐
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure core dumps are restricted	☐	☐
1.4.2	Ensure XD/NX support is enabled	☐	☐
1.4.3	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.5.1.1	Ensure message of the day is configured properly	☐	☐
1.5.1.2	Ensure local login warning banner is configured properly	☐	☐
1.5.1.3	Ensure remote login warning banner is configured properly	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐
2.1.1.1	Ensure time synchronization is in use	☐	☐

Recommendation		Set Correctly	
		Yes	No
2.1.1.2	Ensure chrony is configured	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
2.1.3	Ensure NFS and RPC are not enabled	☐	☐
2.1.4	Ensure rsync service is not enabled	☐	☐
3.1.1	Ensure packet redirect sending is disabled	☐	☐
3.2.1	Ensure source routed packets are not accepted	☐	☐
3.2.2	Ensure ICMP redirects are not accepted	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted	☐	☐
3.2.4	Ensure suspicious packets are logged	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.1	Ensure journald is configured to compress large log files	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐
4.1.3	Ensure permissions on all logfiles are configured	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
4.2	Ensure logrotate is configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.4	Ensure SSH Protocol is set to 2	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled	☐	☐
5.1.9	Ensure SSH HostbasedAuthentication is disabled	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.11	Ensure SSH PermitEmptyPasswords is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.13	Ensure only strong Ciphers are used	☐	☐
5.1.14	Ensure only strong MAC algorithms are used	☐	☐
5.1.15	Ensure only strong Key Exchange algorithms are used	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐
5.1.17	Ensure SSH LoginGraceTime is set to one minute or less	☐	☐
5.1.18	Ensure SSH warning banner is configured	☐	☐
5.1.19	Ensure SSH PAM is enabled	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled	☐	☐
5.1.21	Ensure SSH MaxStartups is configured	☐	☐
5.1.22	Ensure SSH MaxSessions is set to 4 or less	☐	☐
5.2.1	Ensure password creation requirements are configured	☐	☐
5.2.3	Ensure password hashing algorithm is SHA-512	☐	☐
5.3.1.1	Ensure password expiration is 365 days or less	☐	☐
5.3.1.2	Ensure minimum days between password changes is 7 or more	☐	☐
5.3.1.3	Ensure password expiration warning days is 7 or more	☐	☐
5.3.1.4	Ensure inactive password lock is 30 days or less	☐	☐

	Recommendation	Set Correctly	
		Yes	**No**
5.3.1.5	Ensure all users last password change date is in the past	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.2.1	Ensure password fields are not empty	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.6	Ensure root PATH Integrity	☐	☐
6.2.7	Ensure all users' home directories exist	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.12	Ensure no users have .netrc files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐
6.2.14	Ensure no users have .rhosts files	☐	☐
6.2.20	Ensure shadow group is empty	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	☐	☐
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.2.1	Ensure dm-verity is enabled	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.4.1	Ensure core dumps are restricted	☐	☐
1.4.2	Ensure XD/NX support is enabled	☐	☐
1.4.3	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.5.1.1	Ensure message of the day is configured properly	☐	☐
1.5.1.2	Ensure local login warning banner is configured properly	☐	☐
1.5.1.3	Ensure remote login warning banner is configured properly	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
2.1.1.1	Ensure time synchronization is in use	☐	☐
2.1.1.2	Ensure chrony is configured	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
2.1.3	Ensure NFS and RPC are not enabled	☐	☐
2.1.4	Ensure rsync service is not enabled	☐	☐
3.1.1	Ensure packet redirect sending is disabled	☐	☐
3.2.1	Ensure source routed packets are not accepted	☐	☐
3.2.2	Ensure ICMP redirects are not accepted	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted	☐	☐
3.2.4	Ensure suspicious packets are logged	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.1	Ensure journald is configured to compress large log files	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.3	Ensure permissions on all logfiles are configured	☐	☐
4.2	Ensure logrotate is configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.4	Ensure SSH Protocol is set to 2	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled	☐	☐
5.1.7	Ensure SSH MaxAuthTries is set to 4 or less	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled	☐	☐
5.1.9	Ensure SSH HostbasedAuthentication is disabled	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.11	Ensure SSH PermitEmptyPasswords is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.13	Ensure only strong Ciphers are used	☐	☐
5.1.14	Ensure only strong MAC algorithms are used	☐	☐
5.1.15	Ensure only strong Key Exchange algorithms are used	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐
5.1.17	Ensure SSH LoginGraceTime is set to one minute or less	☐	☐
5.1.18	Ensure SSH warning banner is configured	☐	☐
5.1.19	Ensure SSH PAM is enabled	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled	☐	☐
5.1.21	Ensure SSH MaxStartups is configured	☐	☐
5.1.22	Ensure SSH MaxSessions is set to 4 or less	☐	☐
5.2.1	Ensure password creation requirements are configured	☐	☐
5.2.3	Ensure password hashing algorithm is SHA-512	☐	☐
5.3.1.1	Ensure password expiration is 365 days or less	☐	☐
5.3.1.2	Ensure minimum days between password changes is 7 or more	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.3.1.3	Ensure password expiration warning days is 7 or more	☐	☐
5.3.1.4	Ensure inactive password lock is 30 days or less	☐	☐
5.3.1.5	Ensure all users last password change date is in the past	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.2.1	Ensure password fields are not empty	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.6	Ensure root PATH Integrity	☐	☐
6.2.7	Ensure all users' home directories exist	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.12	Ensure no users have .netrc files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐
6.2.14	Ensure no users have .rhosts files	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2.20	Ensure shadow group is empty	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
5.2.2	Ensure password reuse is limited	☐	☐
5.3.2	Ensure system accounts are secured	☐	☐
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group	☐	☐
6.2.16	Ensure no duplicate UIDs exist	☐	☐
6.2.17	Ensure no duplicate GIDs exist	☐	☐
6.2.18	Ensure no duplicate user names exist	☐	☐
6.2.19	Ensure no duplicate group names exist	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
2.1.3	Ensure NFS and RPC are not enabled	☐	☐
2.1.4	Ensure rsync service is not enabled	☐	☐
3.2.4	Ensure suspicious packets are logged	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.1	Ensure journald is configured to compress large log files	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐
4.1.3	Ensure permissions on all logfiles are configured	☐	☐
4.2	Ensure logrotate is configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.4	Ensure SSH Protocol is set to 2	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled	☐	☐
5.1.7	Ensure SSH MaxAuthTries is set to 4 or less	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled	☐	☐
5.2.1	Ensure password creation requirements are configured	☐	☐
5.3.1.1	Ensure password expiration is 365 days or less	☐	☐
5.3.1.2	Ensure minimum days between password changes is 7 or more	☐	☐
5.3.1.3	Ensure password expiration warning days is 7 or more	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
5.3.1.4	Ensure inactive password lock is 30 days or less	☐	☐
5.3.1.5	Ensure all users last password change date is in the past	☐	☐
5.3.2	Ensure system accounts are secured	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.2.1	Ensure password fields are not empty	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	☐	☐
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.2.1	Ensure dm-verity is enabled	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.4.2	Ensure XD/NX support is enabled	☐	☐
1.4.3	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐
2.1.1.1	Ensure time synchronization is in use	☐	☐
2.1.1.2	Ensure chrony is configured	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
2.1.3	Ensure NFS and RPC are not enabled	☐	☐
2.1.4	Ensure rsync service is not enabled	☐	☐

	Recommendation	Set Correctly	
		Yes	No
3.1.1	Ensure packet redirect sending is disabled	☐	☐
3.2.1	Ensure source routed packets are not accepted	☐	☐
3.2.2	Ensure ICMP redirects are not accepted	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted	☐	☐
3.2.4	Ensure suspicious packets are logged	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.1	Ensure journald is configured to compress large log files	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐
4.1.3	Ensure permissions on all logfiles are configured	☐	☐
4.2	Ensure logrotate is configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.4	Ensure SSH Protocol is set to 2	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled	☐	☐
5.1.7	Ensure SSH MaxAuthTries is set to 4 or less	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled	☐	☐
5.1.9	Ensure SSH HostbasedAuthentication is disabled	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.11	Ensure SSH PermitEmptyPasswords is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.13	Ensure only strong Ciphers are used	☐	☐
5.1.14	Ensure only strong MAC algorithms are used	☐	☐
5.1.15	Ensure only strong Key Exchange algorithms are used	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled	☐	☐
5.2.1	Ensure password creation requirements are configured	☐	☐
5.2.3	Ensure password hashing algorithm is SHA-512	☐	☐
5.3.1.1	Ensure password expiration is 365 days or less	☐	☐
5.3.1.2	Ensure minimum days between password changes is 7 or more	☐	☐
5.3.1.3	Ensure password expiration warning days is 7 or more	☐	☐
5.3.1.4	Ensure inactive password lock is 30 days or less	☐	☐
5.3.1.5	Ensure all users last password change date is in the past	☐	☐
5.3.2	Ensure system accounts are secured	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐
6.1.2	Ensure permissions on /etc/shadow are configured	☐	☐

Recommendation		Set Correctly	
		Yes	**No**
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.2.1	Ensure password fields are not empty	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.12	Ensure no users have .netrc files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐
6.2.14	Ensure no users have .rhosts files	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	☐	☐
1.1.2	Ensure /tmp is configured	☐	☐
1.1.3	Ensure nodev option set on /tmp partition	☐	☐
1.1.4	Ensure nosuid option set on /tmp partition	☐	☐
1.1.5	Ensure noexec option set on /tmp partition	☐	☐
1.1.6	Ensure nosuid option set on /var partition	☐	☐
1.1.7	Ensure noexec option set on /var partition	☐	☐
1.1.8	Ensure nodev option set on /var partition	☐	☐
1.1.9	Ensure nodev option set on /home partition	☐	☐
1.1.10	Ensure nodev option set on /dev/shm partition	☐	☐
1.1.11	Ensure nosuid option set on /dev/shm partition	☐	☐
1.1.12	Ensure noexec option set on /dev/shm partition	☐	☐
1.1.13	Disable Automounting	☐	☐
1.2.1	Ensure dm-verity is enabled	☐	☐
1.3.1	Ensure authentication required for single user mode	☐	☐
1.4.2	Ensure XD/NX support is enabled	☐	☐
1.4.3	Ensure address space layout randomization (ASLR) is enabled	☐	☐
1.5.1.4	Ensure permissions on /etc/motd are configured	☐	☐
1.5.1.5	Ensure permissions on /etc/issue are configured	☐	☐
1.5.1.6	Ensure permissions on /etc/issue.net are configured	☐	☐
1.6	Ensure AppArmor is installed	☐	☐
2.1.1.1	Ensure time synchronization is in use	☐	☐
2.1.1.2	Ensure chrony is configured	☐	☐
2.1.2	Ensure X Window System is not installed	☐	☐
2.1.3	Ensure NFS and RPC are not enabled	☐	☐
2.1.4	Ensure rsync service is not enabled	☐	☐

	Recommendation	Set Correctly	
		Yes	No
3.1.1	Ensure packet redirect sending is disabled	☐	☐
3.2.1	Ensure source routed packets are not accepted	☐	☐
3.2.2	Ensure ICMP redirects are not accepted	☐	☐
3.2.3	Ensure secure ICMP redirects are not accepted	☐	☐
3.2.4	Ensure suspicious packets are logged	☐	☐
3.2.5	Ensure broadcast ICMP requests are ignored	☐	☐
3.2.6	Ensure bogus ICMP responses are ignored	☐	☐
3.2.7	Ensure Reverse Path Filtering is enabled	☐	☐
3.2.8	Ensure TCP SYN Cookies is enabled	☐	☐
3.2.9	Ensure IPv6 router advertisements are not accepted	☐	☐
3.3.1.1	Ensure IPv6 default deny firewall policy	☐	☐
3.3.1.2	Ensure IPv6 loopback traffic is configured	☐	☐
3.3.1.3	Ensure IPv6 outbound and established connections are configured	☐	☐
3.3.1.4	Ensure IPv6 firewall rules exist for all open ports	☐	☐
3.3.2.1	Ensure default deny firewall policy	☐	☐
3.3.2.2	Ensure loopback traffic is configured	☐	☐
3.3.2.3	Ensure outbound and established connections are configured	☐	☐
3.3.3	Ensure iptables is installed	☐	☐
4.1.1.1	Ensure correct container image is set for stackdriver logging agent	☐	☐
4.1.1.2	Ensure Logging Service is Running	☐	☐
4.1.1.3	Ensure logging is configured	☐	☐
4.1.2.1	Ensure journald is configured to compress large log files	☐	☐
4.1.2.2	Ensure journald is configured to write logfiles to persistent disk	☐	☐
4.1.3	Ensure permissions on all logfiles are configured	☐	☐
4.2	Ensure logrotate is configured	☐	☐
5.1.1	Ensure permissions on /etc/ssh/sshd_config are configured	☐	☐
5.1.2	Ensure permissions on SSH private host key files are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.3	Ensure permissions on SSH public host key files are configured	☐	☐
5.1.4	Ensure SSH Protocol is set to 2	☐	☐
5.1.5	Ensure SSH LogLevel is appropriate	☐	☐
5.1.6	Ensure SSH X11 forwarding is disabled	☐	☐
5.1.7	Ensure SSH MaxAuthTries is set to 4 or less	☐	☐
5.1.8	Ensure SSH IgnoreRhosts is enabled	☐	☐
5.1.9	Ensure SSH HostbasedAuthentication is disabled	☐	☐
5.1.10	Ensure SSH root login is disabled	☐	☐
5.1.11	Ensure SSH PermitEmptyPasswords is disabled	☐	☐
5.1.12	Ensure SSH PermitUserEnvironment is disabled	☐	☐
5.1.13	Ensure only strong Ciphers are used	☐	☐
5.1.14	Ensure only strong MAC algorithms are used	☐	☐
5.1.15	Ensure only strong Key Exchange algorithms are used	☐	☐
5.1.16	Ensure SSH Idle Timeout Interval is configured	☐	☐
5.1.19	Ensure SSH PAM is enabled	☐	☐
5.1.20	Ensure SSH AllowTcpForwarding is disabled	☐	☐
5.2.1	Ensure password creation requirements are configured	☐	☐
5.2.3	Ensure password hashing algorithm is SHA-512	☐	☐
5.3.1.1	Ensure password expiration is 365 days or less	☐	☐
5.3.1.2	Ensure minimum days between password changes is 7 or more	☐	☐
5.3.1.3	Ensure password expiration warning days is 7 or more	☐	☐
5.3.1.4	Ensure inactive password lock is 30 days or less	☐	☐
5.3.1.5	Ensure all users last password change date is in the past	☐	☐
5.3.2	Ensure system accounts are secured	☐	☐
5.3.3	Ensure default group for the root account is GID 0	☐	☐
5.3.4	Ensure default user umask is 027 or more restrictive	☐	☐
5.3.5	Ensure default user shell timeout is 900 seconds or less	☐	☐
5.4	Ensure root login is restricted to system console	☐	☐
5.5	Ensure access to the su command is restricted	☐	☐
6.1.1	Ensure permissions on /etc/passwd are configured	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.1.2	Ensure permissions on /etc/shadow are configured	☐	☐
6.1.3	Ensure permissions on /etc/group are configured	☐	☐
6.1.4	Ensure permissions on /etc/gshadow are configured	☐	☐
6.1.5	Ensure permissions on /etc/passwd- are configured	☐	☐
6.1.6	Ensure permissions on /etc/shadow- are configured	☐	☐
6.1.7	Ensure permissions on /etc/group- are configured	☐	☐
6.1.8	Ensure permissions on /etc/gshadow- are configured	☐	☐
6.2.1	Ensure password fields are not empty	☐	☐
6.2.2	Ensure no legacy "+" entries exist in /etc/passwd	☐	☐
6.2.3	Ensure no legacy "+" entries exist in /etc/shadow	☐	☐
6.2.4	Ensure no legacy "+" entries exist in /etc/group	☐	☐
6.2.5	Ensure root is the only UID 0 account	☐	☐
6.2.8	Ensure users' home directories permissions are 750 or more restrictive	☐	☐
6.2.9	Ensure users own their home directories	☐	☐
6.2.10	Ensure users' dot files are not group or world writable	☐	☐
6.2.11	Ensure no users have .forward files	☐	☐
6.2.12	Ensure no users have .netrc files	☐	☐
6.2.13	Ensure users' .netrc Files are not group or world accessible	☐	☐
6.2.14	Ensure no users have .rhosts files	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.4.1	Ensure core dumps are restricted	☐	☐
1.5.1.1	Ensure message of the day is configured properly	☐	☐
1.5.1.2	Ensure local login warning banner is configured properly	☐	☐
1.5.1.3	Ensure remote login warning banner is configured properly	☐	☐
5.1.17	Ensure SSH LoginGraceTime is set to one minute or less	☐	☐
5.1.18	Ensure SSH warning banner is configured	☐	☐
5.1.21	Ensure SSH MaxStartups is configured	☐	☐
5.1.22	Ensure SSH MaxSessions is set to 4 or less	☐	☐
5.2.2	Ensure password reuse is limited	☐	☐
6.2.6	Ensure root PATH Integrity	☐	☐
6.2.7	Ensure all users' home directories exist	☐	☐
6.2.15	Ensure all groups in /etc/passwd exist in /etc/group	☐	☐
6.2.16	Ensure no duplicate UIDs exist	☐	☐
6.2.17	Ensure no duplicate GIDs exist	☐	☐
6.2.18	Ensure no duplicate user names exist	☐	☐
6.2.19	Ensure no duplicate group names exist	☐	☐
6.2.20	Ensure shadow group is empty	☐	☐

Appendix: Change History

Date	Version	Changes for this version
May 16, 2024	1.2.0	UPDATE - Ensure Logging Service is running - wording clarification, change to manual (Ticket 21594)
May 17, 2024	1.2.0	Delete - Ensure SSH access is limited (Ticket 21097)
May 17, 2024	1.2.0	UPDATE - Ensure system accounts are secured - Change to use SYS_UID_MIN and SYS_UID_MAX in auditing and remediation (Ticket 20054)
May 20, 2024	1.2.0	UPDATE - Ensure System Accounts are Secured - Update CLI (Ticket 21598)
Jan 12, 2023	1.1.0	UPDATE - Ensure /tmp is configured - Fix typo misspelling utilizing. (Ticket 16968)
Jan 12, 2023	1.1.0	UPDATE - Ensure dm-verity is enabled - Add further explanation as to what ensuring dm-verity is enabled will do. (Ticket 17149)
Jan 12, 2023	1.1.0	UPDATE - Ensure XD/NX support is enabled - expand description to address NX bit in the ARM architecture (Ticket 17165)
Jan 12, 2023	1.1.0	UPDATE - Configure stackdriver logging agent - update section name and description (Ticket 17326)
Jan 12, 2023	1.1.0	UPDATE - Ensure correct container image is set for stackdriver logging agent - Add note about fluent-bit logging (Ticket 17166)
Jan 12, 2023	1.1.0	UPDATE - Filesystem Integrity Checking - fix wording to be relevant for the section content (Ticket 17328)
Jan 19, 2023	1.1.0	UPDATE - Ensure logging is configured - change language to address fluent-bit logging (Ticket 17167)
Jan 19, 2023	1.1.0	UPDATE - Ensure stackdriver Service is running - change wording to include checking for fluent-bit logging (Ticket 17168)
Dec 28, 2021	1.0.0	Initial Release - Document Created