

# CIS Bottlerocket Benchmark

v1.0.0 - 08-11-2022

# 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

<b>Terms of Use.....</b>	<b>1</b>
<b>Table of Contents .....</b>	<b>2</b>
<b>Overview .....</b>	<b>5</b>
Intended Audience .....	6
Consensus Guidance.....	7
Typographical Conventions .....	8
<b>Recommendation Definitions.....</b>	<b>9</b>
Title .....	9
Assessment Status .....	9
Automated .....	9
Manual .....	9
Profile .....	9
Description.....	9
Rationale Statement.....	9
Impact Statement .....	10
Audit Procedure .....	10
Remediation Procedure .....	10
Default Value.....	10
References .....	10
CIS Critical Security Controls® (CIS Controls®).....	10
Additional Information .....	10
Profile Definitions.....	11
Acknowledgements.....	12
<b>Recommendations .....</b>	<b>13</b>
<b>1 Initial Setup .....</b>	<b>13</b>
<b>1.1 Filesystem Configuration.....</b>	<b>13</b>
<b>1.1.1 Disable unused filesystems .....</b>	<b>14</b>
1.1.1.1 Ensure mounting of udf filesystems is disabled (Automated).....	15
<b>1.2 Configure Software Updates .....</b>	<b>17</b>
1.2.1 Ensure software update repositories are configured (Manual).....	18
<b>1.3 Filesystem Integrity Checking.....</b>	<b>20</b>
1.3.1 Ensure dm-verity is configured (Automated) .....	21
<b>1.4 Additional Process Hardening .....</b>	<b>23</b>
1.4.1 Ensure setuid programs do not create core dumps (Automated).....	24
1.4.2 Ensure address space layout randomization (ASLR) is enabled (Automated).....	25
1.4.3 Ensure unprivileged eBPF is disabled (Automated).....	26

1.4.4 Ensure user namespaces are disabled (Automated) .....	27
<b>1.5 Mandatory Access Control .....</b>	<b>28</b>
1.5.1 Ensure SELinux is configured (Automated).....	29
1.5.2 Ensure Lockdown is configured (Automated).....	31
1.6 Ensure updates, patches, and additional security software are installed (Manual).....	32
<b>2 Services.....</b>	<b>33</b>
<b>2.1 Special Purpose Services .....</b>	<b>33</b>
<b>2.1.1 Time Synchronization .....</b>	<b>34</b>
2.1.1.1 Ensure chrony is configured (Automated) .....	35
<b>3 Network Configuration.....</b>	<b>36</b>
<b>3.1 Network Parameters (Host Only).....</b>	<b>37</b>
3.1.1 Ensure packet redirect sending is disabled (Automated) .....	38
<b>3.2 Network Parameters (Host and Router).....</b>	<b>40</b>
3.2.1 Ensure source routed packets are not accepted (Automated) .....	41
3.2.2 Ensure ICMP redirects are not accepted (Automated).....	43
3.2.3 Ensure secure ICMP redirects are not accepted (Automated) .....	45
3.2.4 Ensure suspicious packets are logged (Automated) .....	47
3.2.5 Ensure broadcast ICMP requests are ignored (Automated).....	49
3.2.6 Ensure bogus ICMP responses are ignored (Automated).....	51
3.2.7 Ensure TCP SYN Cookies is enabled (Automated) .....	53
<b>3.3 Uncommon Network Protocols .....</b>	<b>55</b>
3.3.1 Ensure SCTP is disabled (Automated).....	56
<b>3.4 Firewall Configuration.....</b>	<b>57</b>
<b>3.4.1 Configure IPv4 iptables .....</b>	<b>58</b>
3.4.1.1 Ensure IPv4 default deny firewall policy (Automated) .....	59
3.4.1.2 Ensure IPv4 loopback traffic is configured (Automated).....	61
3.4.1.3 Ensure IPv4 outbound and established connections are configured (Manual) .....	63
<b>3.4.2 Configure IPv6 ip6tables .....</b>	<b>65</b>
3.4.2.1 Ensure IPv6 default deny firewall policy (Automated) .....	66
3.4.2.2 Ensure IPv6 loopback traffic is configured (Automated).....	68
3.4.2.3 Ensure IPv6 outbound and established connections are configured (Manual) .....	70
<b>4 Logging and Auditing .....</b>	<b>71</b>
<b>4.1 Configure Logging.....</b>	<b>72</b>
<b>4.1.1 Configure journald .....</b>	<b>73</b>
4.1.1.1 Ensure journald is configured to write logs to persistent disk (Automated).....	74
4.1.2 Ensure permissions on journal files are configured (Automated).....	76
<b>Appendix: Summary Table.....</b>	<b>77</b>
<b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>	<b>80</b>
<b>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</b>	<b>82</b>
<b>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</b>	<b>84</b>
<b>Appendix: CIS Controls v7 Unmapped Recommendations .....</b>	<b>86</b>
<b>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</b>	<b>87</b>
<b>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</b>	<b>89</b>
<b>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</b>	<b>91</b>
<b>Appendix: CIS Controls v8 Unmapped Recommendations .....</b>	<b>93</b>



# 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 configuration posture for Linux systems based on Bottlerocket.

Bottlerocket does not include any facilities for interactive use. This means that shells, user accounts, console gettys for local access, and an SSH daemon for remote access are not available. However, Bottlerocket does allow additional host-level services to be defined and executed, provided they are packaged as containers. These additional services are referred to as host containers. It is possible to configure a host container to provide the necessary access to complete this benchmark.

Bottlerocket defines an "admin" host container that supports SSH sessions and includes a static shell for running commands directly on the host. It is disabled by default and only intended for break-glass access to troubleshoot production systems, but it can be enabled and used to perform the audit and remediation steps in this guide.

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 <http://workbench.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@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 Bottlerocket.

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

# 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 a clear security benefit; and
- not inhibit 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 paramount.
- acts as defense in depth measure.
- may negatively inhibit the utility or performance of the technology.

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.

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.

# 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.

Bottlerocket has a specialized partition layout that provides two logical sets of partitions to support image-based updates. Modifications to the partition layout are not recommended and could interfere with software updates.

Bottlerocket makes extensive use of temporary, memory-backed filesystems in addition to the immutable root filesystem and the mutable data filesystem. Filesystems are automatically mounted with secure options such as `nosuid`, `nodev`, and `noexec` where possible. Additional mitigations against the execution of arbitrary code are applied through the mandatory SELinux policy. Modifications to filesystem mount options are not recommended and could interfere with system functionality.

### 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

# grep -Fw udf /proc/modules
<No output>
```

#### Remediation:




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

```
# apiclient set kernel.modules.udf.allowed=false
```




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

```
# rmmod udf
```

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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.			



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

## 1.2 Configure Software Updates

Update management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of the distribution servers, whereas a single deployment of a system may prefer to get updates directly. Updates can be performed automatically or manually, depending on the site's policy for update management. Many large enterprises prefer to test updates on a non-production system before rolling out to production.

For the purpose of this benchmark, the requirement is to ensure that an update management system is configured and maintained. The specifics on update procedures are left to the organization.

## 1.2.1 Ensure software update repositories are configured (Manual)

### Profile Applicability:

- Level 1 - Server

### Description:

Systems need to have software update repositories configured to ensure they receive the latest updates.

### Rationale:

If a system's software update repositories are misconfigured, important updates may not be identified.

### Audit:










Verify software update repositories are configured correctly. This command should display a list of available updates and return without error:


```
# apiclient update check
```

### Remediation:

Configure your software update repositories according to site policy.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.3 <u>Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v8	<b>7.4 <u>Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><u>3.5 Deploy Automated Software Patch Management Tools</u></p> <p>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.</p>			

## 1.3 Filesystem Integrity Checking

dm-verity provides transparent integrity checking of an underlying block device using a cryptographic digest.

Bottlerocket uses dm-verity for its root filesystem image. The root filesystem is marked as read-only and cannot be directly modified by userspace processes. The kernel is configured to restart if corruption is detected. That allows the system to fail closed if the underlying block device is unexpectedly modified.

### 1.3.1 Ensure dm-verity is configured (Automated)

#### Profile Applicability:

- Level 1 - Server

#### Description:

dm-verity provides transparent integrity checking of block devices using a cryptographic digest. Because dm-verity devices are read-only, filesystems mounted from the devices are also read-only.

#### Rationale:

Using dm-verity prevents direct modification of the root filesystem. Indirect modifications, whether accidental or malicious, can be detected by rebooting the system if corrupt blocks are found.

#### Audit:

Verify that the root filesystem is using dm-verity, and that the kernel is configured to restart if corruption is detected.

```
# grep -Fw "dm-mod.create=root,,,ro,0" /proc/cmdline
# grep -Fw "root=/dev/dm-0" /proc/cmdline
# grep -Fw "restart_on_corruption" /proc/cmdline
```







#### Remediation:

Replace the system or reinstall the distribution.

#### References:

1. dm-verity: <https://www.kernel.org/doc/html/latest/admin-guide/device-mapper/verity.html>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			



## 1.4 Additional Process Hardening



## 1.4.1 Ensure setuid programs do not create core dumps (Automated)

### Profile Applicability:

- Level 1 - 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.

### Rationale:

Setting the `fs.suid_dumpable` variable to 0 will prevent setuid programs from dumping core.

### Audit:

Run the following command and verify output matches:







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

### Remediation:

Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"fs.suid_dumpable" = "0"
EOF
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 1.4.2 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
```

### Remediation:

Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"kernel.randomize_va_space" = "2"
EOF
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>10.5 <u>Enable Anti-Exploitation Features</u></b> 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	<b>8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u></b> 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 unprivileged eBPF is disabled (Automated)

#### Profile Applicability:

- Level 1 - Server

#### Description:

Unprivileged users should not have access to eBPF.

#### Rationale:

eBPF requires complex verification and JIT compilation procedures, and any bugs in this logic can compromise kernel security. Access to eBPF can also facilitate speculative execution attacks.

#### Audit:

Run the following command and verify output matches:







```
# sysctl kernel.unprivileged_bpf_disabled
kernel.unprivileged_bpf_disabled = 1
```

#### Remediation:

Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"kernel.unprivileged_bpf_disabled" = "1"
EOF
```

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> 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	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 1.4.4 Ensure user namespaces are disabled (Automated)

### Profile Applicability:

- Level 2 - Server

### Description:

User namespaces should be disabled unless required.

Note that user namespaces can be necessary in environments where containers running as unprivileged users are meant to run other containers. These are often referred to as "rootless" containers.

### Rationale:

If user namespaces are enabled, then an unprivileged user can create a new user namespace where their processes have capabilities such as `CAP_SYS_ADMIN`. This opens a large attack surface within the kernel that would otherwise be unreachable.

### Audit:

Run the following command and verify output matches:







```
# sysctl user.max_user_namespaces
user.max_user_namespaces = 0
```

### Remediation:

Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"user.max_user_namespaces" = "0"
EOF
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 1.5 Mandatory Access Control

SELinux is a Linux Security Module (LSM) that provides a mechanism for Mandatory Access Control (MAC). Processes that run as root with full capabilities are still subject to the mandatory policy restrictions.

Lockdown is an additional LSM that attempts to protect against unauthorized modification of the running kernel.

Bottlerocket enables SELinux by default, sets it to enforcing mode, and loads the policy during boot. There is no way to disable it.

Bottlerocket enables Lockdown by default in most configurations. It can be disabled if necessary to allow unsigned kernel modules to be loaded.

### 1.5.1 Ensure SELinux is configured (Automated)

#### Profile Applicability:

- Level 1 - Server

#### Description:

SELinux must be enabled and in enforcing mode.

#### Rationale:

The mandatory access controls provided by the default SELinux policy are a critical mechanism to prevent containers from accessing sensitive data or modifying system files that belong to the host or to other containers.

#### Audit:

Verify that SELinux is enabled, that it is set to enforcing mode, and that the expected policy is loaded.

```
# sestatus
SELinux status:           enabled
Loaded policy name:       fortified
Current mode:             enforcing
Mode from config file:    enforcing
Policy MLS status:        enabled
Policy deny_unknown status: denied
Memory protection checking: actual (secure)
```




#### Remediation:




Replace the system or reinstall the distribution.

#### References:

1. SELinux Project: <https://github.com/SELinuxProject>

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> 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	<p><b>14.6 <u>Protect Information through Access Control Lists</u></b></p> <p>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.</p>			

## 1.5.2 Ensure Lockdown is configured (Automated)

### Profile Applicability:

- Level 2 - Server

### Description:

Lockdown must be enabled in integrity mode.

Note that this prevents unsigned kernel modules from being loaded. This could interfere with the operation of hardware or third-party software that depends on these modules.

### Rationale:

Many security mechanisms ultimately depend on the kernel for enforcement. This includes access controls such as capabilities and SELinux, and integrity checks such as dm-verity. Modifications to the running kernel could bypass or subvert these mechanisms.

### Audit:

Verify that Lockdown is enabled in integrity mode.







```
# grep -Fw '[integrity]' /sys/kernel/security/lockdown
none [integrity] confidentiality
```

### Remediation:

Run the following command to enable Lockdown in integrity mode:

```
# apiclient set kernel.lockdown=integrity
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			



## 1.6 Ensure updates, patches, and additional security software are installed (Manual)

### Profile Applicability:

- Level 1 - Server

### Description:

Periodically updates are released for included software either due to security flaws or to include additional functionality.

### Rationale:

It is recommended that the latest software updates be used to take advantage of the latest functionality and security enhancements. As with any software installation, organizations need to determine if a given update meets their requirements and verify the compatibility and supportability of any additional software against the update revision that is selected.

### Audit:

Verify there are no updates to install. This command should display a list of available updates and return without error:

```
# apiclient update check
```

### Remediation:

Update the software on the system according to site policy.




This command will apply the latest available update and reboot the system to apply it if necessary:










```
# apiclient update apply --check --reboot
```

### Additional Information:

Site policy may mandate a testing period before install onto production systems for available updates.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.4 <u>Perform Automated Application Patch Management</u></b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			
v7	<b>3.5 <u>Deploy Automated Software Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.			

## 2 Services

Bottlerocket system images are customized for specific combinations of execution platforms and container orchestrator agents. Only services required for normal system operation are included and enabled. The actions in this section of the document provide guidance for secure configuration of these services.

### 2.1 Special Purpose Services

This section describes services that are installed on systems that specifically need to run these services.

### **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 chrony is configured (Automated)

#### Profile Applicability:

- Level 1 - Server

#### Description:

`chrony` is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate.

#### Rationale:

Proper configuration of `chrony` is vital to ensuring time synchronization is working properly.

#### Audit:

Run the following command and verify that time servers are configured:

```
# apiclient get settings.ntp.time-servers
{
  "settings": {
    "ntp": {
      "time-servers": [
        "..."
      ]
    }
  }
}
```

Run the following command and verify that `chrony` is active:

```
# systemctl is-active chronyd
active
```

#### Remediation:

Configure additional time servers as needed.

The following command would add "2.pool.ntp.org" to the list of time servers.





```
# apiclient apply <<EOF
[settings.ntp]
time-servers = [ "2.pool.ntp.org" ]
EOF
```

If `chrony` is not running, update to a version of the OS with the correct service configuration.

#### References:

1. chrony: <http://chrony.tuxfamily.org>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.4 <u>Standardize Time Synchronization</u></b> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.			
v7	<b>6.1 <u>Utilize Three Synchronized Time Sources</u></b> 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.			

## 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 2 - 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
```

#### Remediation:




Run the following command to set the active kernel parameters and persist the settings:




```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.conf.all.send_redirects" = "0"
"net.ipv4.conf.default.send_redirects" = "0"
EOF
```

Run the following command to flush the routing cache:

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

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>5.1 Establish Secure Configurations</b> 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 command to set the active kernel parameters and persist the settings:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.conf.all.accept_source_route" = "0"
"net.ipv4.conf.default.accept_source_route" = "0"
"net.ipv6.conf.all.accept_source_route" = "0"
"net.ipv6.conf.default.accept_source_route" = "0"
EOF
```

Run the following command to flush the routing caches:

```
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> 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	<b>5.1 <u>Establish Secure Configurations</u></b> 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 command to set the active kernel parameters and persist the settings:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.conf.all.accept_redirects" = "0"
"net.ipv4.conf.default.accept_redirects" = "0"
"net.ipv6.conf.all.accept_redirects" = "0"
"net.ipv6.conf.default.accept_redirects" = "0"
EOF
```

Run the following commands to flush the routing caches:

```
# sysctl -w net.ipv4.route.flush=1
# sysctl -w net.ipv6.route.flush=1
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 <u>Establish and Maintain a Secure Configuration Process</u></b> 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	<b>5.1 <u>Establish Secure Configurations</u></b> 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 command to set the active kernel parameters and persist the settings:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.conf.all.secure_redirects" = "0"
"net.ipv4.conf.default.secure_redirects" = "0"
EOF
```

Run the following command to flush the routing cache:

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

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> 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 command to set the active kernel parameters and persist the settings:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.conf.all.log_martians" = "1"
"net.ipv4.conf.default.log_martians" = "1"
EOF
```






Run the following command to flush the routing cache:

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

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 Collect Detailed Audit Logs</b> 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	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> 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 command and verify output matches:

```
# sysctl net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

#### Remediation:




Run the following command to set the active kernel parameter and persist the setting:




```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.icmp_echo_ignore_broadcasts" = "1"
EOF
```

Run the following command to flush the routing cache:

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

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>5.1 Establish Secure Configurations</b> 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 command and verify output matches:

```
# sysctl net.ipv4.icmp_ignore_bogus_error_responses
net.ipv4.icmp_ignore_bogus_error_responses = 1
```

#### Remediation:







Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.icmp_ignore_bogus_error_responses" = "1"
EOF
```

Run the following command to flush the routing cache:

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

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			



### 3.2.7 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 attack 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 command and verify output matches:

```
# sysctl net.ipv4.tcp_syncookies
net.ipv4.tcp_syncookies = 1
```

#### Remediation:







Run the following command to set the active kernel parameter and persist the setting:

```
# apiclient apply <<EOF
[settings.kernel.sysctl]
"net.ipv4.tcp_syncookies" = "1"
EOF
```

Run the following command to flush the routing cache:

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

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>4.1 Establish and Maintain a Secure Configuration Process</u></b> 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	<b><u>5.1 Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### 3.3 Uncommon Network Protocols

The Linux kernel modules support several network protocols that are not commonly used. If these protocols are not needed, it is recommended that they be disabled in the kernel.

**Note:** This should not be considered a comprehensive list of uncommon network protocols, you may wish to consider additions to those listed here for your environment.



### 3.3.1 Ensure SCTP is disabled (Automated)

#### Profile Applicability:

- Level 2 - Server

#### Description:

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP.

#### Rationale:

If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

#### Audit:

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

```
# modprobe -n -v sctp
install /bin/true







# grep -w sctp /proc/modules
<No output>
```

#### Remediation:

Run the following command to disable the `sctp` module:

```
# apiclient set kernel.modules.sctp.allowed=false
```

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

### 3.4 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.

### 3.4.1 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. Configuring the firewall of a live system 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:

```
#!/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
```

The above script can be deployed through a bootstrap container, which is the mechanism that Bottlerocket provides for running custom code during the boot process.

### 3.4.1.1 Ensure IPv4 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 allow list acceptable usage than to deny 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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.			

### 3.4.1.2 Ensure IPv4 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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.			

### 3.4.1.3 Ensure IPv4 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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.			

### 3.4.2 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.

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. Configuring the firewall of a live system 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:

```
#!/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
```

The above script can be deployed through a bootstrap container, which is the mechanism that Bottlerocket provides for running custom code during the boot process.

### 3.4.2.1 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 allow list acceptable usage than to deny 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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.			

### 3.4.2.2 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 DROP        all  *  *       *      ::1

# 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
```

#### 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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.			

### 3.4.2.3 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	<b>4.4 <u>Implement and Manage a Firewall on Servers</u></b> 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	<b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b> 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	<b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b> 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 using tools included in the distribution.

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.

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.



## 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.

Bottlerocket ensures that all of its own logs are stored in the systemd journal. However, it does not provide direct support for shipping these logs to a remote server.

Log aggregation agents must be deployed through containers instead. You should configure your preferred log aggregation agent to read from the systemd journal, along with any other directories where container logs might be stored. The specific agent to deploy, and the details of its configuration, are a matter of site policy and will vary across organizations.

### 4.1.1 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.

### 4.1.1.1 Ensure journald is configured to write logs to persistent disk (Automated)

#### Profile Applicability:

- Level 1 - Server

#### Description:

Data from the journal 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 `/usr/lib/systemd/journald.conf.d/journald.conf` and verify that logs are persisted to disk:



```
# grep -Fw Storage /usr/lib/systemd/journald.conf.d/journald.conf
Storage=persistent
```

#### Remediation:

Update to a version of the OS with the correct journald configuration.

#### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> 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	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>6.3 <u>Enable Detailed Logging</u></b> 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 Ensure permissions on journal files are configured (Automated)

### Profile Applicability:

- Level 1 - Server

### Description:

The journal is stored in `/var/log/journal`, and contains logged information from all services on the system.

### 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/journal -type f -perm /g+wx,o+rw
```

### Remediation:

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

```
# find /var/log/journal -type f -perm /g+wx,o+rw -exec chmod g-wx,o-rwx "{}" +
```

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> 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	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Initial Setup</b>		
<b>1.1</b>	<b>Filesystem Configuration</b>		
<b>1.1.1</b>	<b>Disable unused filesystems</b>		
1.1.1.1	Ensure mounting of udf filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.2</b>	<b>Configure Software Updates</b>		
1.2.1	Ensure software update repositories are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.3</b>	<b>Filesystem Integrity Checking</b>		
1.3.1	Ensure dm-verity is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.4</b>	<b>Additional Process Hardening</b>		
1.4.1	Ensure setuid programs do not create core dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure address space layout randomization (ASLR) is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.5</b>	<b>Mandatory Access Control</b>		
1.5.1	Ensure SELinux is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>2</b>	<b>Services</b>		
<b>2.1</b>	<b>Special Purpose Services</b>		
<b>2.1.1</b>	<b>Time Synchronization</b>		
2.1.1.1	Ensure chrony is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3</b>	<b>Network Configuration</b>		
<b>3.1</b>	<b>Network Parameters (Host Only)</b>		
3.1.1	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.2</b>	<b>Network Parameters (Host and Router)</b>		
3.2.1	Ensure source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.3</b>	<b>Uncommon Network Protocols</b>		
3.3.1	Ensure SCTP is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.4</b>	<b>Firewall Configuration</b>		
<b>3.4.1</b>	<b>Configure IPv4 iptables</b>		
3.4.1.1	Ensure IPv4 default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4.1.2	Ensure IPv4 loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>3.4.2</b>	<b>Configure IPv6 ip6tables</b>		
3.4.2.1	Ensure IPv6 default deny firewall policy (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure IPv6 outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Logging and Auditing</b>		
<b>4.1</b>	<b>Configure Logging</b>		
<b>4.1.1</b>	<b>Configure journald</b>		
4.1.1.1	Ensure journald is configured to write logs to persistent disk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>



# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7.0	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>



Recommendation		Set Correctly	
		Yes	No
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Ensure mounting of udf filesystems is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.2.1	Ensure software update repositories are configured	<input type="checkbox"/>	<input type="checkbox"/>
1.3.1	Ensure dm-verity is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.4.1	Ensure setuid programs do not create core dumps	<input type="checkbox"/>	<input type="checkbox"/>
1.4.2	Ensure address space layout randomization (ASLR) is enabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.3	Ensure unprivileged eBPF is disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.4.4	Ensure user namespaces are disabled	<input type="checkbox"/>	<input type="checkbox"/>
1.5.1	Ensure SELinux is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.5.2	Ensure Lockdown is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure updates, patches, and additional security software are installed	<input type="checkbox"/>	<input type="checkbox"/>
2.1.1.1	Ensure chrony is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1	Ensure packet redirect sending is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.2.1	Ensure source routed packets are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	Ensure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Ensure secure ICMP redirects are not accepted	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Ensure suspicious packets are logged	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Ensure broadcast ICMP requests are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Ensure bogus ICMP responses are ignored	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Ensure TCP SYN Cookies is enabled	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1	Ensure SCTP is disabled	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.1	Ensure IPv4 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.2	Ensure IPv4 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.1.3	Ensure IPv4 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.1	Ensure IPv6 default deny firewall policy	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2.2	Ensure IPv6 loopback traffic is configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
3.4.2.3	Ensure IPv6 outbound and established connections are configured	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Ensure journald is configured to write logs to persistent disk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure permissions on journal files are configured	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8.0	<input type="checkbox"/>	<input type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version