

# CIS Rocky Linux 8 Benchmark

v1.0.0 - 03-29-2022

# 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

Terms of Use.....	1
Overview.....	15
Intended Audience .....	15
Consensus Guidance.....	15
Assessment Status.....	16
Profile Definitions.....	17
Acknowledgements.....	18
Recommendations.....	20
1 Initial Setup.....	20
1.1 Filesystem Configuration .....	21
1.1.1 Disable unused filesystems.....	22
1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated) .....	23
1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated) .....	25
1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated).....	28
1.1.2 Configure /tmp .....	31
1.1.2.1 Ensure /tmp is a separate partition (Automated).....	32
1.1.2.2 Ensure nodev option set on /tmp partition (Automated) .....	35
1.1.2.3 Ensure noexec option set on /tmp partition (Automated) .....	37
1.1.2.4 Ensure nosuid option set on /tmp partition (Automated).....	39
1.1.3 Configure /var.....	41
1.1.3.1 Ensure separate partition exists for /var (Automated).....	42
1.1.3.2 Ensure nodev option set on /var partition (Automated) .....	44
1.1.3.3 Ensure noexec option set on /var partition (Automated) .....	46
1.1.3.4 Ensure nosuid option set on /var partition (Automated).....	48
1.1.4 Configure /var/tmp.....	50
1.1.4.1 Ensure separate partition exists for /var/tmp (Automated).....	51
1.1.4.2 Ensure noexec option set on /var/tmp partition (Automated) .....	54
1.1.4.3 Ensure nosuid option set on /var/tmp partition (Automated) .....	56
1.1.4.4 Ensure nodev option set on /var/tmp partition (Automated) .....	58

1.1.5 Configure /var/log.....	60
1.1.5.1 Ensure separate partition exists for /var/log (Automated).....	61
1.1.5.2 Ensure nodev option set on /var/log partition (Automated).....	63
1.1.5.3 Ensure noexec option set on /var/log partition (Automated).....	65
1.1.5.4 Ensure nosuid option set on /var/log partition (Automated).....	67
1.1.6 Configure /var/log/audit .....	69
1.1.6.1 Ensure separate partition exists for /var/log/audit (Automated) .....	70
1.1.6.2 Ensure noexec option set on /var/log/audit partition (Automated).....	72
1.1.6.3 Ensure nodev option set on /var/log/audit partition (Automated) .....	74
1.1.6.4 Ensure nosuid option set on /var/log/audit partition (Automated) .....	76
1.1.7 Configure /home.....	78
1.1.7.1 Ensure separate partition exists for /home (Automated).....	79
1.1.7.2 Ensure nodev option set on /home partition (Automated).....	81
1.1.7.3 Ensure nosuid option set on /home partition (Automated).....	83
1.1.7.4 Ensure usrquota option set on /home partition (Automated).....	85
1.1.7.5 Ensure grpquota option set on /home partition (Automated) .....	88
1.1.8 Configure /dev/shm .....	91
1.1.8.1 Ensure nodev option set on /dev/shm partition (Automated).....	92
1.1.8.2 Ensure noexec option set on /dev/shm partition (Automated) .....	94
1.1.8.3 Ensure nosuid option set on /dev/shm partition (Automated) .....	96
1.1.9 Disable Automounting (Automated).....	98
1.1.10 Disable USB Storage (Automated).....	100
1.2 Configure Software Updates .....	102
1.2.1 Ensure GPG keys are configured (Manual) .....	103
1.2.2 Ensure gpgcheck is globally activated (Automated) .....	106
1.2.3 Ensure package manager repositories are configured (Manual) .....	108
1.3 Filesystem Integrity Checking.....	110
1.3.1 Ensure AIDE is installed (Automated) .....	111
1.3.2 Ensure filesystem integrity is regularly checked (Automated) .....	113
1.4 Secure Boot Settings .....	116

1.4.1 Ensure bootloader password is set (Automated).....	117
1.4.2 Ensure permissions on bootloader config are configured (Automated).....	120
1.4.3 Ensure authentication is required when booting into rescue mode (Automated) .....	123
1.5 Additional Process Hardening .....	125
1.5.1 Ensure core dump storage is disabled (Automated).....	126
1.5.2 Ensure core dump backtraces are disabled (Automated) .....	127
1.5.3 Ensure address space layout randomization (ASLR) is enabled (Automated) .....	129
1.6 Mandatory Access Control .....	131
1.6.1 Configure SELinux.....	132
1.6.1.1 Ensure SELinux is installed (Automated) .....	134
1.6.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated) .....	136
1.6.1.3 Ensure SELinux policy is configured (Automated) .....	138
1.6.1.4 Ensure the SELinux mode is not disabled (Automated) .....	140
1.6.1.5 Ensure the SELinux mode is enforcing (Automated) .....	143
1.6.1.6 Ensure no unconfined services exist (Automated) .....	146
1.6.1.7 Ensure SETroubleshoot is not installed (Automated) .....	148
1.6.1.8 Ensure the MCS Translation Service (mcstrans) is not installed (Automated) .....	150
1.7 Command Line Warning Banners .....	152
1.7.1 Ensure message of the day is configured properly (Automated) .....	153
1.7.2 Ensure local login warning banner is configured properly (Automated)....	155
1.7.3 Ensure remote login warning banner is configured properly (Automated) .....	157
1.7.4 Ensure permissions on /etc/motd are configured (Automated) .....	159
1.7.5 Ensure permissions on /etc/issue are configured (Automated) .....	161
1.7.6 Ensure permissions on /etc/issue.net are configured (Automated) .....	163
1.8 GNOME Display Manager .....	165
1.8.1 Ensure GNOME Display Manager is removed (Manual) .....	166
1.8.2 Ensure GDM login banner is configured (Automated) .....	168

1.8.3 Ensure last logged in user display is disabled (Automated) .....	171
1.8.4 Ensure XDMCP is not enabled (Automated).....	173
1.8.5 Ensure automatic mounting of removable media is disabled (Automated) .....	175
1.9 Ensure updates, patches, and additional security software are installed (Manual).....	177
1.10 Ensure system-wide crypto policy is not legacy (Automated).....	179
2 Services.....	181
2.1 Time Synchronization.....	182
2.1.1 Ensure time synchronization is in use (Automated).....	183
2.1.2 Ensure chrony is configured (Automated).....	185
2.2 Special Purpose Services .....	187
2.2.1 Ensure xinetd is not installed (Automated).....	188
2.2.2 Ensure xorg-x11-server-common is not installed (Automated) .....	190
2.2.3 Ensure Avahi Server is not installed (Automated).....	192
2.2.4 Ensure CUPS is not installed (Automated).....	194
2.2.5 Ensure DHCP Server is not installed (Automated).....	196
2.2.6 Ensure DNS Server is not installed (Automated).....	198
2.2.7 Ensure FTP Server is not installed (Automated) .....	200
2.2.8 Ensure VSFTP Server is not installed (Automated) .....	202
2.2.9 Ensure TFTP Server is not installed (Automated) .....	204
2.2.10 Ensure a web server is not installed (Automated) .....	206
2.2.11 Ensure IMAP and POP3 server is not installed (Automated) .....	208
2.2.12 Ensure Samba is not installed (Automated).....	210
2.2.13 Ensure HTTP Proxy Server is not installed (Automated) .....	212
2.2.14 Ensure net-snmp is not installed (Automated).....	214
2.2.15 Ensure NIS server is not installed (Automated) .....	216
2.2.16 Ensure telnet-server is not installed (Automated) .....	218
2.2.17 Ensure mail transfer agent is configured for local-only mode (Automated) .....	220

2.2.18 Ensure nfs-utils is not installed or the nfs-server service is masked (Automated) .....	222
2.2.19 Ensure rpcbind is not installed or the rpcbind services are masked (Automated) .....	224
2.2.20 Ensure rsync is not installed or the rsyncd service is masked (Automated) .....	226
2.3 Service Clients.....	228
2.3.1 Ensure NIS Client is not installed (Automated) .....	229
2.3.2 Ensure rsh client is not installed (Automated) .....	231
2.3.3 Ensure talk client is not installed (Automated) .....	233
2.3.4 Ensure telnet client is not installed (Automated).....	235
2.3.5 Ensure LDAP client is not installed (Automated) .....	237
2.3.6 Ensure TFTP client is not installed (Automated).....	239
2.4 Ensure nonessential services are removed or masked (Manual).....	241
3 Network Configuration .....	243
3.1 Disable unused network protocols and devices.....	245
3.1.1 Verify if IPv6 is enabled on the system (Manual) .....	246
3.1.2 Ensure SCTP is disabled (Automated) .....	250
3.1.3 Ensure DCCP is disabled (Automated).....	252
3.1.4 Ensure wireless interfaces are disabled (Automated) .....	254
3.2 Network Parameters (Host Only).....	257
3.2.1 Ensure IP forwarding is disabled (Automated) .....	258
3.2.2 Ensure packet redirect sending is disabled (Automated) .....	262
3.3 Network Parameters (Host and Router).....	265
3.3.1 Ensure source routed packets are not accepted (Automated).....	266
3.3.2 Ensure ICMP redirects are not accepted (Automated) .....	273
3.3.3 Ensure secure ICMP redirects are not accepted (Automated) .....	280
3.3.4 Ensure suspicious packets are logged (Automated) .....	284
3.3.5 Ensure broadcast ICMP requests are ignored (Automated).....	287
3.3.6 Ensure bogus ICMP responses are ignored (Automated).....	290
3.3.7 Ensure Reverse Path Filtering is enabled (Automated) .....	292

3.3.8 Ensure TCP SYN Cookies is enabled (Automated) .....	296
3.3.9 Ensure IPv6 router advertisements are not accepted (Automated) .....	299
3.4 Firewall Configuration.....	303
3.4.1 Configure firewalld .....	304
3.4.1.1 Ensure firewalld is installed (Automated) .....	305
3.4.1.2 Ensure iptables-services not installed with firewalld (Automated).....	307
3.4.1.3 Ensure nftables either not installed or masked with firewalld (Automated) .....	309
3.4.1.4 Ensure firewalld service enabled and running (Automated).....	311
3.4.1.5 Ensure firewalld default zone is set (Automated) .....	313
3.4.1.6 Ensure network interfaces are assigned to appropriate zone (Manual) ..	315
3.4.1.7 Ensure firewalld drops unnecessary services and ports (Manual).....	317
3.4.2 Configure nftables .....	320
3.4.2.1 Ensure nftables is installed (Automated) .....	323
3.4.2.2 Ensure firewalld is either not installed or masked with nftables (Automated) .....	325
3.4.2.3 Ensure iptables-services not installed with nftables (Automated).....	327
3.4.2.4 Ensure iptables are flushed with nftables (Manual).....	329
3.4.2.5 Ensure an nftables table exists (Automated) .....	331
3.4.2.6 Ensure nftables base chains exist (Automated).....	333
3.4.2.7 Ensure nftables loopback traffic is configured (Automated) .....	335
3.4.2.8 Ensure nftables outbound and established connections are configured (Manual) .....	338
3.4.2.9 Ensure nftables default deny firewall policy (Automated) .....	340
3.4.2.10 Ensure nftables service is enabled (Automated).....	342
3.4.2.11 Ensure nftables rules are permanent (Automated) .....	344
3.4.3 Configure iptables .....	347
3.4.3.1.1 Ensure iptables packages are installed (Automated).....	349
3.4.3.1.2 Ensure nftables is not installed with iptables (Automated) .....	351
3.4.3.1.3 Ensure firewalld is either not installed or masked with iptables (Automated) .....	353

3.4.3.2.1 Ensure iptables loopback traffic is configured (Automated).....	356
3.4.3.2.2 Ensure iptables outbound and established connections are configured (Manual).....	358
3.4.3.2.3 Ensure iptables rules exist for all open ports (Automated).....	360
3.4.3.2.4 Ensure iptables default deny firewall policy (Automated).....	363
3.4.3.2.5 Ensure iptables rules are saved (Automated) .....	365
3.4.3.2.6 Ensure iptables is enabled and active (Automated) .....	368
3.4.3.3.1 Ensure ip6tables loopback traffic is configured (Automated).....	371
3.4.3.3.2 Ensure ip6tables outbound and established connections are configured (Manual) .....	374
3.4.3.3.3 Ensure ip6tables firewall rules exist for all open ports (Automated)....	377
3.4.3.3.4 Ensure ip6tables default deny firewall policy (Automated) .....	380
3.4.3.3.5 Ensure ip6tables rules are saved (Automated).....	383
3.4.3.3.6 Ensure ip6tables is enabled and active (Automated) .....	387
4 Logging and Auditing .....	390
4.1 Configure System Accounting (auditd).....	391
4.1.1 Ensure auditing is enabled.....	393
4.1.1.1 Ensure auditd is installed (Automated).....	394
4.1.1.2 Ensure auditd service is enabled (Automated).....	396
4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated) .....	398
4.1.1.4 Ensure audit_backlog_limit is sufficient (Automated).....	400
4.1.2 Configure Data Retention .....	402
4.1.2.1 Ensure audit log storage size is configured (Automated) .....	403
4.1.2.2 Ensure audit logs are not automatically deleted (Automated) .....	405
4.1.2.3 Ensure system is disabled when audit logs are full (Automated).....	407
4.1.3 Configure auditd rules .....	410
4.1.3.1 Ensure changes to system administration scope (sudoers) is collected (Automated) .....	411
4.1.3.2 Ensure actions as another user are always logged (Automated).....	415
4.1.3.3 Ensure events that modify the sudo log file are collected (Automated)...	419

4.1.3.4 Ensure events that modify date and time information are collected (Automated) .....	423
4.1.3.5 Ensure events that modify the system's network environment are collected (Automated).....	427
4.1.3.6 Ensure use of privileged commands are collected (Automated).....	431
4.1.3.7 Ensure unsuccessful file access attempts are collected (Automated) .....	435
4.1.3.8 Ensure events that modify user/group information are collected (Automated).....	439
4.1.3.9 Ensure discretionary access control permission modification events are collected (Automated).....	443
4.1.3.10 Ensure successful file system mounts are collected (Automated).....	448
4.1.3.11 Ensure session initiation information is collected (Automated).....	452
4.1.3.12 Ensure login and logout events are collected (Automated).....	456
4.1.3.13 Ensure file deletion events by users are collected (Automated) .....	460
4.1.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated).....	464
4.1.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated).....	468
4.1.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated).....	472
4.1.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated).....	476
4.1.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated) .....	480
4.1.3.19 Ensure kernel module loading unloading and modification is collected (Automated) .....	484
4.1.3.20 Ensure the audit configuration is immutable (Automated).....	489
4.1.3.21 Ensure the running and on disk configuration is the same (Manual) ....	492
<b>4.2 Configure Logging.....</b>	<b>494</b>
Security principals for logging.....	494
What is covered .....	494
What is not covered.....	494
<b>4.2.1 Configure rsyslog.....</b>	<b>495</b>

4.2.1.1 Ensure rsyslog is installed (Automated) .....	496
4.2.1.2 Ensure rsyslog service is enabled (Automated) .....	498
4.2.1.3 Ensure journald is configured to send logs to rsyslog (Manual) .....	500
4.2.1.4 Ensure rsyslog default file permissions are configured (Automated).....	503
4.2.1.5 Ensure logging is configured (Manual) .....	505
4.2.1.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)	507
4.2.1.7 Ensure rsyslog is not configured to receive logs from a remote client (Automated) .....	509
4.2.2 Configure journald .....	512
4.2.2.1.1 Ensure systemd-journal-remote is installed (Manual) .....	514
4.2.2.1.2 Ensure systemd-journal-remote is configured (Manual).....	516
4.2.2.1.3 Ensure systemd-journal-remote is enabled (Manual).....	518
4.2.2.1.4 Ensure journald is not configured to receive logs from a remote client (Automated) .....	520
4.2.2.2 Ensure journald service is enabled (Automated) .....	522
4.2.2.3 Ensure journald is configured to compress large log files (Automated) ..	524
4.2.2.4 Ensure journald is configured to write logfiles to persistent disk (Automated) .....	526
4.2.2.5 Ensure journald is not configured to send logs to rsyslog (Manual) .....	528
4.2.2.6 Ensure journald log rotation is configured per site policy (Manual) .....	530
4.2.2.7 Ensure journald default file permissions configured (Manual) .....	532
4.2.3 Ensure permissions on all logfiles are configured (Automated) .....	534
4.3 Ensure logrotate is configured (Manual).....	536
5 Access, Authentication and Authorization.....	538
5.1 Configure time-based job schedulers.....	539
5.1.1 Ensure cron daemon is enabled (Automated).....	540
5.1.2 Ensure permissions on /etc/crontab are configured (Automated).....	541
5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated) .....	543
5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated).....	545
5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated) .....	547
5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)....	549

5.1.7 Ensure permissions on /etc/cron.d are configured (Automated).....	551
5.1.8 Ensure cron is restricted to authorized users (Automated).....	553
5.1.9 Ensure at is restricted to authorized users (Automated) .....	556
5.2 Configure SSH Server .....	559
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured (Automated).....	560
5.2.2 Ensure permissions on SSH private host key files are configured (Automated) .....	562
5.2.3 Ensure permissions on SSH public host key files are configured (Automated).....	565
5.2.4 Ensure SSH access is limited (Automated) .....	568
5.2.5 Ensure SSH LogLevel is appropriate (Automated) .....	571
5.2.6 Ensure SSH PAM is enabled (Automated) .....	573
5.2.7 Ensure SSH root login is disabled (Automated) .....	575
5.2.8 Ensure SSH HostbasedAuthentication is disabled (Automated) .....	577
5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Automated) .....	579
5.2.10 Ensure SSH PermitUserEnvironment is disabled (Automated).....	581
5.2.11 Ensure SSH IgnoreRhosts is enabled (Automated).....	583
5.2.12 Ensure SSH X11 forwarding is disabled (Automated).....	585
5.2.13 Ensure SSH AllowTcpForwarding is disabled (Automated).....	587
5.2.14 Ensure system-wide crypto policy is not over-ridden (Automated).....	590
5.2.15 Ensure SSH warning banner is configured (Automated) .....	592
5.2.16 Ensure SSH MaxAuthTries is set to 4 or less (Automated).....	594
5.2.17 Ensure SSH MaxStartups is configured (Automated) .....	596
5.2.18 Ensure SSH MaxSessions is set to 10 or less (Automated).....	598
5.2.19 Ensure SSH LoginGraceTime is set to one minute or less (Automated) ...	600
5.2.20 Ensure SSH Idle Timeout Interval is configured (Automated) .....	602
5.3 Configure privilege escalation .....	605
5.3.1 Ensure sudo is installed (Automated).....	606
5.3.2 Ensure sudo commands use pty (Automated) .....	608
5.3.3 Ensure sudo log file exists (Automated) .....	610

5.3.4 Ensure users must provide password for escalation (Automated) .....	612
5.3.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated) .....	614
5.3.6 Ensure sudo authentication timeout is configured correctly (Automated) .....	616
5.3.7 Ensure access to the su command is restricted (Automated) .....	618
5.4 Configure authselect .....	620
5.4.1 Ensure custom authselect profile is used (Manual) .....	621
5.4.2 Ensure authselect includes with-faillock (Automated) .....	624
5.5 Configure PAM .....	626
5.5.1 Ensure password creation requirements are configured (Automated) .....	627
5.5.2 Ensure lockout for failed password attempts is configured (Automated) ..	631
5.5.3 Ensure password reuse is limited (Automated).....	635
5.5.4 Ensure password hashing algorithm is SHA-512 (Automated).....	638
5.6 User Accounts and Environment.....	642
5.6.1 Set Shadow Password Suite Parameters .....	643
5.6.1.1 Ensure password expiration is 365 days or less (Automated).....	644
5.6.1.2 Ensure minimum days between password changes is 7 or more (Automated).....	646
5.6.1.3 Ensure password expiration warning days is 7 or more (Automated)....	648
5.6.1.4 Ensure inactive password lock is 30 days or less (Automated).....	650
5.6.1.5 Ensure all users last password change date is in the past (Automated) ..	652
5.6.2 Ensure system accounts are secured (Automated) .....	654
5.6.3 Ensure default user shell timeout is 900 seconds or less (Automated).....	657
5.6.4 Ensure default group for the root account is GID 0 (Automated).....	660
5.6.5 Ensure default user umask is 027 or more restrictive (Automated) .....	662
6 System Maintenance.....	667
6.1 System File Permissions .....	668
6.1.1 Audit system file permissions (Manual) .....	669
6.1.2 Ensure sticky bit is set on all world-writable directories (Automated) .....	672
6.1.3 Ensure permissions on /etc/passwd are configured (Automated) .....	674
6.1.4 Ensure permissions on /etc/shadow are configured (Automated) .....	676

6.1.5 Ensure permissions on /etc/group are configured (Automated) .....	678
6.1.6 Ensure permissions on /etc/gshadow are configured (Automated) .....	680
6.1.7 Ensure permissions on /etc/passwd- are configured (Automated) .....	682
6.1.8 Ensure permissions on /etc/shadow- are configured (Automated).....	684
6.1.9 Ensure permissions on /etc/group- are configured (Automated).....	686
6.1.10 Ensure permissions on /etc/gshadow- are configured (Automated).....	688
6.1.11 Ensure no world writable files exist (Automated) .....	690
6.1.12 Ensure no unowned files or directories exist (Automated).....	692
6.1.13 Ensure no ungrouped files or directories exist (Automated) .....	694
6.1.14 Audit SUID executables (Manual) .....	696
6.1.15 Audit SGID executables (Manual) .....	698
<b>6.2 User and Group Settings .....</b>	<b>700</b>
6.2.1 Ensure password fields are not empty (Automated).....	701
6.2.2 Ensure all groups in /etc/passwd exist in /etc/group (Automated).....	703
6.2.3 Ensure no duplicate UIDs exist (Automated) .....	705
6.2.4 Ensure no duplicate GIDs exist (Automated).....	707
6.2.5 Ensure no duplicate user names exist (Automated) .....	709
6.2.6 Ensure no duplicate group names exist (Automated).....	711
6.2.7 Ensure root PATH Integrity (Automated) .....	713
6.2.8 Ensure root is the only UID 0 account (Automated) .....	715
6.2.9 Ensure all users' home directories exist (Automated).....	717
6.2.10 Ensure users own their home directories (Automated).....	720
6.2.11 Ensure users' home directories permissions are 750 or more restrictive (Automated) .....	722
6.2.12 Ensure users' dot files are not group or world writable (Automated).....	724
6.2.13 Ensure users' .netrc Files are not group or world accessible (Automated) .....	726
6.2.14 Ensure no users have .forward files (Automated).....	729
6.2.15 Ensure no users have .netrc files (Automated) .....	731
6.2.16 Ensure no users have .rhosts files (Automated).....	733
<b>Appendix: Recommendation Summary Table .....</b>	<b>735</b>

Appendix: Change History.....	746
-------------------------------	-----

# Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Rocky Linux 8 systems running on x86\_64 platforms.

The guidance within broadly assumes that operations are being performed as the root user, and executed under the default bash version for the applicable distribution. Operations performed using sudo instead of the root user, or executed under another shell, 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 Rocky Linux 8 on x86\_64 platforms.

## Consensus Guidance

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

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

## 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 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.

- **Level 1 - Workstation**

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 workstations.

- **Level 2 - Workstation**

This profile extends the "Level 1 - Workstation" 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 workstations.

## Acknowledgements

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

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

### **Contributor**

Rael Daruszka  
Ron Colvin  
Bill Erickson  
Dave Billing  
Dominic Pace  
Elliot Anderson  
Ely Pinto  
Fredrik Silverskär  
Joy Latten  
Kirill Antonenko  
Koen Laevens  
Marcelo Cerri  
Mark Birch  
Martynas Brijunas  
Michel Verbraak  
Mike Thompson  
Pradeep R B  
Rakesh Jain  
Robert Thomas  
Tom Pietschmann  
Vineetha Hari Pai  
William E. Triest III  
Anurag Pal  
Bradley Hieber  
Thomas Sjögren  
James Trigg  
Kenneth Karlsson  
Mark Hesse  
Martinus Nel

Matthew Burket , IBM

Mike Cross

Marcus Burghardt

Graham Eames

Simon John

Robert McSulla

Chad Streck

Ryan Jaynes

**Editor**

Jonathan Lewis Christopherson

Eric Pinnell

Justin Brown

# Recommendations

## ***1 Initial Setup***

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

## **1.1 Filesystem Configuration**

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

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

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

### **1.1.1 Disable unused filesystems**

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

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

**Note:** This should not be considered a comprehensive list of filesystems. You may wish to consider additions to those listed here for your environment. For the current available file system modules on the system see `/usr/lib/modules/$(uname -r)/kernel/fs`

#### **Start up scripts**

Kernel modules loaded directly via `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/* .conf` files. If modules are still being loaded after a reboot whilst having the correctly configured `blacklist` and `install` command, check for `insmod` entries in start up scripts such as `.bashrc`.

You may also want to check `/usr/lib/modprobe.d/`. Please note that this directory should not be used for user defined module loading. Ensure that all such entries resides in `/etc/modprobe.d/* .conf` files.

#### **Return values**

By using `/bin/false` as the command in disabling a particular module service two purposes; to convey the meaning of the entry to the user and cause a non-zero return value. The latter can be tested for in scripts. Please note that `insmod` will ignore what is configured in the relevant `/etc/modprobe.d/* .conf` files. The preferred way to load modules is with `modprobe`.

### *1.1.1.1 Ensure mounting of cramfs filesystems is disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `cramfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `cramfs` image can be used without having to first decompress the image.

#### **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.

- How will the module be loaded.

```
# modprobe -n -v cramfs | grep "install"
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep cramfs
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist\s+cramfs" /etc/modprobe.d/*
blacklist      cramfs
```

## **Remediation:**

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with a line that reads `install cramfs /bin/false` and a line that reads `blacklist cramfs`.

*Example:*

```
# printf "install cramfs /bin/false\nblacklist cramfs\n" >> /etc/modprobe.d/cramfs.conf
```

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

```
# modprobe -r cramfs
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-7

## **CIS Controls:**

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

### *1.1.1.2 Ensure mounting of squashfs filesystems is disabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `squashfs` filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A `squashfs` image can be used without having to first decompress the image.

#### **Rationale:**

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

#### **Impact:**

As Snap packages utilizes `squashfs` as a compressed filesystem, disabling `squashfs` will cause Snap packages to fail.

Snap application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment.

## Audit:

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

- How will the module be loaded.

```
# modprobe -n -v squashfs | grep "^install"
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep squashfs
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist\s+squashfs" /etc/modprobe.d/*
/etc/modprobe.d/squashfs.conf:blacklist      squashfs
```

## Remediation:

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with the lines that reads `install squashfs /bin/false` and `blacklist squashfs`.

*Example:*

```
# printf "install squashfs /bin/false
blacklist squashfs
" >> /etc/modprobe.d/squashfs.conf
```

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

```
# modprobe -r squashfs
```

**CIS Controls:**

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

### *1.1.1.3 Ensure mounting of udf filesystems is disabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **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.

#### **Impact:**

Microsoft Azure requires the usage of `udf`.

`udf` should not be disabled on systems run on Microsoft Azure.

## **Audit:**

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

- How will the module be loaded.

```
# modprobe -n -v udf | grep "^install"
install /bin/false
```

- Is the module currently loaded.

```
# lsmod | grep udf
<No output>
```

- Is the module blacklisted.

```
# grep -E "^blacklist[[:blank:]]*udf" /etc/modprobe.d/*
/etc/modprobe.d/udf.conf:blacklist      udf
```

## **Remediation:**

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf` with a line that reads `install udf /bin/false`.

Example:

```
# printf "install udf /bin/false
blacklist udf
" >> /etc/modprobe.d/udf.conf
```

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

```
# modprobe -r udf
```

**CIS Controls:**

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

### **1.1.2 Configure /tmp**

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

### *1.1.2.1 Ensure /tmp is a separate partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

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

#### **Impact:**

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

Running out of `/tmp` space is a problem regardless of what kind of filesystem lies under it, but in a configuration where `/tmp` is not a separate file system it will essentially have the whole disk available, as the default installation only creates a single `/` partition. On the other hand, a RAM-based `/tmp` (as with `tmpfs`) will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily. Another alternative is to create a dedicated partition for `/tmp` from a separate volume or disk. One of the downsides of a disk-based dedicated partition is that it will be slower than `tmpfs` which is RAM-based.

`/tmp` utilizing `tmpfs` can be resized using the `size={size}` parameter in the relevant entry in `/etc/fstab`.

## Audit:

Run the following command and verify the output shows that `/tmp` is mounted. Particular requirements pertaining to mount options are covered in ensuing sections.

```
# findmnt --kernel /tmp  
  
TARGET SOURCE FSTYPE OPTIONS  
/tmp tmpfs tmpfs rw,nosuid,nodev,noexec,relatime,seclabel
```

Ensure that systemd will mount the `/tmp` partition at boot time.

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

Note that by default systemd will output generated if there is an entry in `/etc/fstab` for `/tmp`. This just means systemd will use the entry in `/etc/fstab` instead of it's default unit file configuration for `/tmp`.

## Remediation:

First ensure that systemd is correctly configured to ensure that `/tmp` will be mounted at boot time.

```
# systemctl unmask tmp.mount
```

For specific configuration requirements of the `/tmp` mount for your environment, modify `/etc/fstab`.

Example of using `tmpfs` with specific mount options:

```
tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime,size=2G 0  
0
```

Example of using a volume or disk with specific mount options. The source location of the volume or disk will vary depending on your environment.

```
<device> /tmp <fstype> defaults,nodev,nosuid,noexec 0 0
```

## References:

1. <https://www.freedesktop.org/wiki/Software/systemd/APIFileSystems/>
2. <https://www.freedesktop.org/software/systemd/man/systemd-fstab-generator.html>

### **Additional Information:**

If an entry for `/tmp` exists in `/etc/fstab` it will take precedence over entries in `systemd` default unit file located at `/usr/lib/systemd/system/tmp.mount`.

### **NIST SP 800-53 Rev. 5:**

- CM-7

### **CIS Controls:**

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

### *1.1.2.2 Ensure nodev option set on /tmp partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set for the `/tmp` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep nodev
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

### *1.1.2.3 Ensure noexec option set on /tmp partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `noexec` option is set for the `/tmp` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep noexec
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### *1.1.2.4 Ensure nosuid option set on /tmp partition (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

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

##### **Audit:**

Verify that the `nosuid` option is set for the `/tmp` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /tmp | grep nosuid
/tmp    tmpfs    tmpfs    rw,nosuid,nodev,noexec,relatime,seclabel
```

##### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/tmp` partition.

Example:

```
<device> /tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/tmp` with the configured options:

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

##### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### **1.1.3 Configure /var**

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

### *1.1.3.1 Ensure separate partition exists for /var (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `/var` directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable.

#### **Rationale:**

The reasoning for mounting `/var` on a separate partition is as follow.

##### **Protection from resource exhaustion**

The default installation only creates a single `/` partition. Since the `/var` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var` and cause unintended behavior across the system as the disk is full. See `man auditd.conf` for details.

##### **Fine grained control over the mount**

Configuring `/var` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behaviour. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

##### **Protection from exploitation**

An example of exploiting `/var` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

Run the following command and verify output shows `/var` is mounted.

Example:

```
# findmnt --kernel /var  
  
TARGET SOURCE FSTYPE OPTIONS  
/var /dev/sdb ext4 rw,relatime,seclabel,data=ordered
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

## Additional Information:

When modifying `/var` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

## 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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.3.2 Ensure nodev option set on /var partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set for the `/var` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var | grep nodev
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.3.3 Ensure noexec option set on /var partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

Since the `/var` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot run executable binaries from `/var`.

#### **Audit:**

Verify that the `noexec` option is set for the `/var` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var | grep noexec
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### *1.1.3.4 Ensure nosuid option set on /var partition (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

Since the `/var` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var`.

##### **Audit:**

Verify that the `nosuid` option is set for the `/var` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var | grep nosuid
/var    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

##### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var` with the configured options:

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

##### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### **1.1.4 Configure /var/tmp**

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary file residing in `/var/tmp` is to be preserved between reboots.

#### *1.1.4.1 Ensure separate partition exists for /var/tmp (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The `/var/tmp` directory is a world-writable directory used for temporary storage by all users and some applications. Temporary file residing in `/var/tmp` is to be preserved between reboots.

##### **Rationale:**

The reasoning for mounting `/var/tmp` on a separate partition is as follow.

###### **Protection from resource exhaustion**

The default installation only creates a single `/` partition. Since the `/var/tmp` directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/tmp` and cause the potential disruption to daemons as the disk is full.

###### **Fine grained control over the mount**

Configuring `/var/tmp` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

###### **Protection from exploitation**

An example of exploiting `/var/tmp` may be an attacker establishing a hard-link to a system `setuid` program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

## **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## **Audit:**

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

Example:

```
# findmnt --kernel /var/tmp  
  
TARGET SOURCE      FSTYPE OPTIONS  
/var/tmp  /dev/sdb  ext4    rw,relatime,seclabel,data=ordered
```

## **Remediation:**

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/tmp`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## **References:**

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

## **Additional Information:**

When modifying `/var/tmp` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.4.2 Ensure noexec option set on /var/tmp partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `noexec` option is set for the `/var/tmp` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep noexec
/var/tmp    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.4.3 Ensure nosuid option set on /var/tmp partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nosuid` option is set for the `/var/tmp` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep nosuid
/var/tmp    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### *1.1.4.4 Ensure nodev option set on /var/tmp partition (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

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

##### **Audit:**

Verify that the `nodev` option is set for the `/var/tmp` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/tmp | grep nodev
/var/tmp    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

##### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/tmp` partition.

Example:

```
<device> /var/tmp      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/tmp` with the configured options:

```
# mount -o remount /var/tmp
```

##### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### **1.1.5 Configure /var/log**

The `/var/log` directory is used by system services to store log data.

### *1.1.5.1 Ensure separate partition exists for /var/log (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `/var/log` directory is used by system services to store log data.

#### **Rationale:**

The reasoning for mounting `/var/log` on a separate partition is as follow.

##### **Protection from resource exhaustion**

The default installation only creates a single `/` partition. Since the `/var/log` directory contain the log files that can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole.

##### **Fine grained control over the mount**

Configuring `/var/log` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

##### **Protection of log data**

As `/var/log` contains log files, care should be taken to ensure the security and integrity of the data and mount point.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

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

```
# findmnt --kernel /var/log
TARGET      SOURCE   FSTYPE OPTIONS
/var/log    /dev/sdb ext4    rw,relatime,seclabel,data=ordered
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

## Additional Information:

When modifying `/var/log` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multiuser mode.

## CIS Controls:

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

### *1.1.5.2 Ensure nodev option set on /var/log partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set for the `/var/log` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep nodev
/var/log    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.5.3 Ensure noexec option set on /var/log partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

Since the `/var/log` filesystem is only intended for log files, set this option to ensure that users cannot run executable binaries from `/var/log`.

#### **Audit:**

Verify that the `noexec` option is set for the `/var/log` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep noexec
/var/log    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.5.4 Ensure nosuid option set on /var/log partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nosuid` option is set for the `/var/log` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/log | grep nosuid
/var/log    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log` partition.

Example:

```
<device> /var/log      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/var/log` with the configured options:

```
# mount -o remount /var/log
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### ***1.1.6 Configure /var/log/audit***

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

### *1.1.6.1 Ensure separate partition exists for /var/log/audit (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The auditing daemon, `auditd`, stores log data in the `/var/log/audit` directory.

#### **Rationale:**

The reasoning for mounting `/var/log/audit` on a separate partition is as follow.

##### **Protection from resource exhaustion**

The default installation only creates a single `/` partition. Since the `/var/log/audit` directory contain the `audit.log` file that can grow quite large, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/var/log/audit` and cause `auditd` to trigger it's `space_left_action` as the disk is full. See `man auditd.conf` for details.

##### **Fine grained control over the mount**

Configuring `/var/log/audit` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

##### **Protection of audit data**

As `/var/log/audit` contains audit logs, care should be taken to ensure the security and integrity of the data and mount point.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

Run the following command and verify output shows `/var/log/audit` is mounted:

```
# findmnt --kernel /var/log/audit  
  
TARGET      SOURCE   FSTYPE OPTIONS  
/var/log/audit /dev/sdb ext4    rw,relatime,seclabel,data=ordered
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for `/var/log/audit`.

For systems that were previously installed, create a new partition and configure `/etc/fstab` as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

## Additional Information:

When modifying `/var/log/audit` it is advisable to bring the system to emergency mode (so `auditd` is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

## CIS Controls:

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

## *1.1.6.2 Ensure noexec option set on /var/log/audit partition (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

Since the `/var/log/audit` filesystem is only intended for audit logs, set this option to ensure that users cannot run executable binaries from `/var/log/audit`.

### **Audit:**

Verify that the `noexec` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep noexec
/var/log/audit    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/var` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

### **References:**

1. See the `fstab(5)` manual page for more information.

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### *1.1.6.3 Ensure nodev option set on /var/log/audit partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep nodev
/var/log/audit  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/var/log/audit` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.6.4 Ensure nosuid option set on /var/log/audit partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

Since the `/var/log/audit` filesystem is only intended for variable files such as logs, set this option to ensure that users cannot create `setuid` files in `/var/log/audit`.

#### **Audit:**

Verify that the `nosuid` option is set for the `/var/log/audit` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /var/log/audit | grep nosuid
/var/log/audit  /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/var/log/audit` partition.

Example:

```
<device> /var/log/audit    <fstype>
defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/var/log/audit` with the configured options:

```
# mount -o remount /var/log/audit
```

#### **References:**

1. See the `fstab(5)` manual page for more information.

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### **1.1.7 Configure /home**

Please note that home directories could be mounted anywhere and is not necessarily restricted to `/home` nor restricted to a single location nor is the name restricted in any way.

Checks can be made by looking in `/etc/passwd`, looking over the mounted file systems with `mount` or queering the relevant database with `getent`.

### *1.1.7.1 Ensure separate partition exists for /home (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The `/home` directory is used to support disk storage needs of local users.

#### **Rationale:**

The reasoning for mounting `/home` on a separate partition is as follow.

#### **Protection from resource exhaustion**

The default installation only creates a single `/` partition. Since the `/home` directory contains user generated data, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to `/home` and impact all local users.

#### **Fine grained control over the mount**

Configuring `/home` as its own file system allows an administrator to set additional mount options such as `noexec/nosuid/nodev`. These options limits an attackers ability to create exploits on the system. In the case of `/home` options such as `usrquota/grpquota` may be considered to limit the impact that users can have on each other with regards to disk resource exhaustion. Other options allow for specific behavior. See `man mount` for exact details regarding filesystem-independent and filesystem-specific options.

#### **Protection of user data**

As `/home` contains user data, care should be taken to ensure the security and integrity of the data and mount point.

#### **Impact:**

Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

## Audit:

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

```
# findmnt --kernel /home  
  
TARGET SOURCE FSTYPE OPTIONS  
/home /dev/sdb ext4 rw,relatime,seclabel
```

## Remediation:

For new installations, during installation create a custom partition setup and specify a separate partition for /home.

For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate.

## References:

1. AJ Lewis, "LVM HOWTO", <http://tldp.org/HOWTO/LVM-HOWTO/>

## Additional Information:

When modifying /home it is advisable to bring the system to emergency mode (so auditd is not running), rename the existing directory, mount the new file system, and migrate the data over before returning to multi-user mode.

## 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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.7.2 Ensure nodev option set on /home partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set for the `/home` mount.

Run the following command to verify that the `nodev` mount option is set.

Example:

```
# findmnt --kernel /home | grep nodev
/home    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.7.3 Ensure nosuid option set on /home partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nosuid` option is set for the `/home` mount.

Run the following command to verify that the `nosuid` mount option is set.

Example:

```
# findmnt --kernel /home | grep nosuid
/home    /dev/sdb ext4  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0 0
```

Run the following command to remount `/home` with the configured options:

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

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### *1.1.7.4 Ensure usrquota option set on /home partition (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `usrquota` mount option allows for the filesystem to have disk quotas configured.

##### **Rationale:**

To ensure the availability of disk space on `/home`, it is important to limit the impact a single user or group can cause for other users (or the wider system) by accidentally filling up the partition. Quotas can also be applied to inodes for filesystems where inode exhaustion is a concern.

##### **Audit:**

Verify that the `usrquota` option is set for the `/home` mount, that quotas is enabled and configured.

Run the following command to verify that the `usrquota` mount option is set.

Example:

```
# findmnt --kernel /home | grep usrquota
/home    /dev/sdb ext4  rw,quota,usrquota,grpquota,nodev,relatime,seclabel
```

Run the following command to verify that the user quotas are enabled.

```
# quotaon -p /home | grep user
user quota on /home (/dev/sdb) is on
```

## **Remediation:**

Edit the `/etc/fstab` file and add `usrquota` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,usrquota,grpquota,nodev,relatime  
0 0
```

Run the following command to remount `/home` with the configured options:

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

Create the quota database. This example will ignore any existing quota files.

```
# quotacheck -cugv /home  
  
quotacheck: Your kernel probably supports journaled quota but you are not  
using it. Consider switching to journaled quota to avoid running quotacheck  
after an unclean shutdown.  
quotacheck: Scanning /dev/sdb [/home] done  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Checked 8 directories and 0 files  
quotacheck: Old file not found.  
quotacheck: Old file not found.
```

Restore SELinux context on the quota database files. Order of operations is important as `quotaon` will set the immutable attribute on the files and thus `restorecon` will fail.

```
# restorecon /home/aquota.user
```

Enable quotas on the partition:

```
# quotaon -vug /home  
  
/dev/sdb [/home]: group quotas turned on  
/dev/sdb [/home]: user quotas turned on
```

## **References:**

1. See the `fstab(5)` and `edquota(8)` manual pages for more information.

## **Additional Information:**

### **Journal filesystems**

If the destination filesystem is journaled, it is recommended to investigate the relevant documentation for the filesystem and use journaled quotas instead of the above example.

### **Setting quotas**

Set the relevant quotas with `edquota`. See `man edquota` for more information.

### **Reporting**

To see the current usage use `repquota -a`.

## **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## **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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.7.5 Ensure grpquota option set on /home partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `grpquota` mount option allows for the filesystem to have disk quotas configured.

#### **Rationale:**

To ensure the availability of disk space on `/home`, it is important to limit the impact a single user or group can cause for other users (or the wider system) by accidentally filling up the partition. Quotas can also be applied to inodes for filesystems where inode exhaustion is a concern.

#### **Audit:**

Verify that the `grpquota` option is set for the `/home` mount, that quotas is enabled and configured.

Run the following command to verify that the `grpquota` mount option is set.

Example:

```
# findmnt --kernel /home | grep grpquota  
/home  /dev/sdb ext4  rw,quota,usrquota,grpquota,nodev,relatime,seclabel
```

Run the following command to verify that the user quotas are enabled.

```
# quotaon -p /home | grep group  
user quota on /home (/dev/sdb) is on
```

## **Remediation:**

Edit the `/etc/fstab` file and add `grpquota` to the fourth field (mounting options) for the `/home` partition.

Example:

```
<device> /home      <fstype>      defaults,rw,usrquota,grpquota,nodev,relatime  
0 0
```

Run the following command to remount `/home` with the configured options:

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

Create the quota database. This example will ignore any existing quota files.

```
# quotacheck -cugv /home  
  
quotacheck: Your kernel probably supports journaled quota but you are not  
using it. Consider switching to journaled quota to avoid running quotacheck  
after an unclean shutdown.  
quotacheck: Scanning /dev/sdb [/home] done  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old user quota file /home/aquota.user: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Cannot stat old group quota file /home/aquota.group: No such file  
or directory. Usage will not be subtracted.  
quotacheck: Checked 8 directories and 0 files  
quotacheck: Old file not found.  
quotacheck: Old file not found.
```

Restore SELinux context on the quota database files. Order of operations is important as `quotaon` will set the immutable attribute on the files and thus `restorecon` will fail.

```
# restorecon /home/aquota.group
```

Enable quotas on the partition:

```
# quotaon -vug /home  
  
/dev/sdb [/home]: group quotas turned on  
/dev/sdb [/home]: user quotas turned on
```

## **References:**

1. See the `fstab(5)` and `edquota(8)` manual pages for more information.

## **Additional Information:**

### **Journal filesystems**

If the destination filesystem is journaled, it is recommended to investigate the relevant documentation for the filesystem and use journaled quotas instead of the above example.

### **Setting quotas**

Set the relevant quotas with `edquota`. See `man edquota` for more information.

### **Reporting**

To see the current usage use `repquota -a`.

## **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## **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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### ***1.1.8 Configure /dev/shm***

### *1.1.8.1 Ensure nodev option set on /dev/shm partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nodev` option is set if a `/dev/shm` partition exists.

Run the following command and verify that nothing is returned:

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

#### **Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/dev/shm` using the updated options from `/etc/fstab`:

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

#### **Additional Information:**

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.8.2 Ensure noexec option set on /dev/shm partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `noexec` option is set for the `/dev/shm` mount.

Run the following command to verify that the `noexec` mount option is set.

Example:

```
# findmnt --kernel /dev/shm | grep noexec
/dev/shm  tmpfs  tmpfs  rw,nosuid,nodev,noexec,relatime,seclabel
```

#### **Remediation:**

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition.

Example:

```
<device> /dev/shm      <fstype>      defaults,rw,nosuid,nodev,noexec,relatime  0
0
```

Run the following command to remount `/dev/shm` with the configured options:

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

**NOTE** It is recommended to use `tmpfs` as the device/filesystem type as `/dev/shm` is used as shared memory space by applications.

#### **References:**

1. See the `fstab(5)` manual page for more information.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.1.8.3 Ensure nosuid option set on /dev/shm partition (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Verify that the `nosuid` option is set if a `/dev/shm` partition exists.

Run the following command and verify that nothing is returned:

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

#### **Remediation:**

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.

Run the following command to remount `/dev/shm` using the updated options from `/etc/fstab`:

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

#### **Additional Information:**

Some distributions mount `/dev/shm` through other means and require `/dev/shm` to be added to `/etc/fstab` even though it is already being mounted on boot. Others may configure `/dev/shm` in other locations and may override `/etc/fstab` configuration. Consult the documentation appropriate for your distribution.

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### *1.1.9 Disable Automounting (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Impact:**

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

#### **Audit:**

As a preference `autofs` should not be installed unless other packages depend on it.

Run the following command to verify `autofs` is not installed:

```
# systemctl is-enabled autofs  
Failed to get unit file state for autofs.service: No such file or directory
```

Run the following command to verify `autofs` is not enabled if installed:

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

Verify result is not "enabled".

## **Remediation:**

If there are no other packages that depends on `autofs`, remove the package with:

```
# dnf remove autofs
```

Run the following command to disable `autofs` if it is required:

```
# systemctl --now disable autofs
```

## **Additional Information:**

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

## **NIST SP 800-53 Rev. 5:**

- SC-18(4)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<a href="#">10.3 Disable Autorun and Autoplay for Removable Media</a> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<a href="#">8.5 Configure Devices Not To Auto-run Content</a> Configure devices to not auto-run content from removable media.	●	●	●

### **1.1.10 Disable USB Storage (Automated)**

#### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

#### **Description:**

USB storage provides a means to transfer and store files insuring persistence and availability of the files independent of network connection status. Its popularity and utility has led to USB-based malware being a simple and common means for network infiltration and a first step to establishing a persistent threat within a networked environment.

#### **Rationale:**

Restricting USB access on the system will decrease the physical attack surface for a device and diminish the possible vectors to introduce malware.

#### **Audit:**

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

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

#### **Remediation:**

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf

Example: vim /etc/modprobe.d/usb\_storage.conf

and add the following line:

```
install usb-storage /bin/true
```

Run the following command to unload the usb-storage module:

```
rmmod usb-storage
```

### **Additional Information:**

An alternative solution to disabling the usb-storage module may be found in USBGuard.

Use of USBGuard and construction of USB device policies should be done in alignment with site policy.

### **NIST SP 800-53 Rev. 5:**

- SC-18(4)

### **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>10.3 Disable Autorun and Autoplay for Removable Media</b> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<b>13.7 Manage USB Devices</b> If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.		●	●

## ***1.2 Configure Software Updates***

Rocky Linux 8 uses dnf (previously yum) to install and update software packages. Patch management procedures may vary widely between enterprises. Large enterprises may choose to install a local updates server that can be used in place of their distributions 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 patch management. Many large enterprises prefer to test patches on a non-production system before rolling out to production.

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

### *1.2.1 Ensure GPG keys are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The RPM Package Manager implements GPG key signing to verify package integrity during and after installation.

#### **Rationale:**

It is important to ensure that updates are obtained from a valid source to protect against spoofing that could lead to the inadvertent installation of malware on the system. To this end, verify that GPG keys are configured correctly for your system.

#### **Audit:**

##### **List all GPG key URLs**

Each repository should have a `gpgkey` with a URL pointing to the location of the GPG key, either local or remote.

```
# grep -r gpgkey /etc/yum.repos.d/* /etc/dnf/dnf.conf
```

##### **List installed GPG keys**

Run the following command to list the currently installed keys. These are the active keys used for verification and installation of RPMs. The packages are fake, they are generated on the fly by `dnf` or `rpm` during the import of keys from the URL specified in the repository configuration.

Example:

```

# for RPM_PACKAGE in $(rpm -q gpg-pubkey); do
echo "RPM: ${RPM_PACKAGE}"
RPM_SUMMARY=$(rpm -q --queryformat "%{SUMMARY}" "${RPM_PACKAGE}")
RPM_PACKAGER=$(rpm -q --queryformat "%{PACKAGER}" "${RPM_PACKAGE}")
RPM_DATE=$(date +%Y-%m-%d -d "1970-1-1+$((0x$(rpm -q --queryformat
"%{RELEASE}" "${RPM_PACKAGE}") ))sec")
RPM_KEY_ID=$(rpm -q --queryformat "%{VERSION}" "${RPM_PACKAGE}")
echo "Packager: ${RPM_PACKAGER}"
Summary: ${RPM_SUMMARY}
Creation date: ${RPM_DATE}
Key ID: ${RPM_KEY_ID}
"
done

RPM: gpg-pubkey-9db62fb1-59920156
Packager: Fedora 28 (28) <fedora-28@fedoraproject.org>
Summary: gpg(Fedora 28 (28) <fedora-28@fedoraproject.org>)
Creation date: 2017-08-14
Key ID: 9db62fb1

RPM: gpg-pubkey-09eab3f2-595fbba3
Packager: RPM Fusion free repository for Fedora (28) <rpmfusion-
buildsys@lists.rpmfusion.org>
Summary: gpg(RPM Fusion free repository for Fedora (28) <rpmfusion-
buildsys@lists.rpmfusion.org>)
Creation date: 2017-07-07
Key ID: 09eab3f2

```

The format of the package (gpg-pubkey-9db62fb1-59920156) is important to understand for verification. Using the above example, it consists of three parts:

1. The general prefix name for all imported GPG keys: gpg-pubkey-
2. The version, which is the GPG key ID: 9db62fb1
3. The release is the date of the key in UNIX timestamp in hexadecimal: 59920156

With both the date and the GPG key ID, check the relevant repositories public key page to confirm that the keys are indeed correct.

### **Query locally available GPG keys**

Repositories that store their respective GPG keys on disk should do so in /etc/pki/rpm-gpg/. These keys are available for immediate import either when dnf is asked to install a relevant package from the repository or when an administrator imports the key directly with the rpm --import command.

To find where these keys comes from run:

```

# for PACKAGE in $(find /etc/pki/rpm-gpg/ -type f -exec rpm -qf {} \; | sort
-u); do rpm -q --queryformat "%{NAME}-%{VERSION} %{PACKAGER} %{SUMMARY}\n"
"${PACKAGE}"; done

```

**Remediation:**

Update your package manager GPG keys in accordance with site policy.

**Additional Information:**

Fedora public keys: <https://getfedora.org/security/>

**NIST SP 800-53 Rev. 5:**

- SI-2

**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.	●	●	●
v8	<u>7.4 Perform Automated Application Patch Management</u> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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	<u>3.5 Deploy Automated Software Patch Management Tools</u> 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.	●	●	●

## *1.2.2 Ensure gpgcheck is globally activated (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `gpgcheck` option, found in the main section of the `/etc/dnf/dnf.conf` and individual `/etc/yum.repos.d/*` files, determines if an RPM package's signature is checked prior to its installation.

### **Rationale:**

It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.

### **Audit:**

Global configuration. Run the following command and verify that `gpgcheck` is set to 1:

```
# grep ^gpgcheck /etc/dnf/dnf.conf  
gpgcheck=1
```

Configuration in `/etc/yum.repos.d/` takes precedence over the global configuration. Run the following command and verify that there are no instances of entries starting with `gpgcheck` returned set to 0. Nor should there be any invalid (non-boolean) values. When `dnf` encounters such invalid entries they are ignored and the global configuration is applied.

```
# grep -P "^\gpgcheck\h*=\\h*[^\n].*\h*\$" /etc/yum.repos.d/*
```

## **Remediation:**

Edit `/etc/dnf/dnf.conf` and set `gpgcheck=1` in the `[main]` section.

Example:

```
# sed -i 's/^gpgcheck\s*=.*$/gpgcheck=1/' /etc/dnf/dnf.conf
```

Edit any failing files in `/etc/yum.repos.d/*` and set all instances starting with `gpgcheck` to 1.

Example:

```
# find /etc/yum.repos.d/ -name "*.repo" -exec echo "Checking:" {} \; -exec sed -i 's/^gpgcheck\s*=.*$/gpgcheck=1/' {} \;
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- SI-2

### **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.	●	●	●
v7	<u>3.4 Deploy Automated Operating System Patch Management Tools</u> 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.	●	●	●

### *1.2.3 Ensure package manager repositories are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Systems need to have the respective package manager repositories configured to ensure that the system is able to receive the latest patches and updates.

#### **Rationale:**

If a system's package repositories are misconfigured, important patches may not be identified or a rogue repository could introduce compromised software.

#### **Audit:**

Run the following command to verify repositories are configured correctly. The output may vary depending on which repositories is currently configured on the system.

Example:

```
# dnf repolist
Last metadata expiration check: 1:00:00 ago on Mon 1 Jan 2021 00:00:00 BST.
repo id          repo name           status
*fedora          Fedora 28 - x86_64      57,327
*updates         Fedora 28 - x86_64 - Updates 22,133
```

For the repositories in use, inspect the configuration file to ensure all settings are correctly applied according to site policy.

Example:

```
# cat /etc/yum.repos.d/fedora.repo
```

#### **Remediation:**

Configure your package manager repositories according to site policy.

## **Additional Information:**

For further information about Fedora repositories see: <https://docs.fedoraproject.org/en-US/quick-docs/repositories/>

## **NIST SP 800-53 Rev. 5:**

- SI-2

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>7.3 Perform Automated Operating System Patch Management</b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	<b>7.4 Perform Automated Application Patch Management</b> Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	<b>3.4 Deploy Automated Operating System Patch Management Tools</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 Deploy Automated Software Patch Management Tools</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.	●	●	●

## ***1.3 Filesystem Integrity Checking***

AIDE is a file integrity checking tool, similar in nature to Tripwire. While it cannot prevent intrusions, it can detect unauthorized changes to configuration files by alerting when the files are changed. When setting up AIDE, decide internally what the site policy will be concerning integrity checking. Review the AIDE quick start guide and AIDE documentation before proceeding.

### *1.3.1 Ensure AIDE is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Advanced Intrusion Detection Environment (AIDE) is a intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories.

AIDE takes a snapshot of files and directories including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

#### **Rationale:**

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

#### **Audit:**

Run the following command and verify `aide` is installed:

```
# rpm -q aide  
aide-<version>
```

#### **Remediation:**

Run the following command to install AIDE:

```
# dnf install aide
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE:

Run the following commands:

```
# aide --init  
# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

## **References:**

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

## **Additional Information:**

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

## **NIST SP 800-53 Rev. 5:**

- AU-2

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.14 Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	<u>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

### *1.3.2 Ensure filesystem integrity is regularly checked (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Periodic checking of the filesystem integrity is needed to detect changes to the filesystem.

#### **Rationale:**

Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

#### **Audit:**

Run the following commands to verify a cron job scheduled to run the aide check.

```
# grep -Ers '^([^\#]+\s+)?(/usr\s?bin\//|^[\s]*)aide(\.wrapper)?\s(--?\s+\s)*(-  
-(check|update)|\$AIDEARGS)\b' /etc/cron.* /etc/crontab /var/spool/cron/
```

Ensure a cron job in compliance with site policy is returned.

OR run the following commands to verify that aidcheck.service and aidcheck.timer are enabled and aidcheck.timer is running

```
# systemctl is-enabled aidecheck.service  
  
# systemctl is-enabled aidecheck.timer  
# systemctl status aidecheck.timer
```

## **Remediation:**

*If cron will be used to schedule and run aide check*

Run the following command:

```
# crontab -u root -e
```

Add the following line to the crontab:

```
0 5 * * * /usr/sbin/aide --check
```

*OR if aidecheck.service and aidecheck.timer will be used to schedule and run aide check:*

Create or edit the file `/etc/systemd/system/aidecheck.service` and add the following lines:

```
[Unit]
Description=Aide Check

[Service]
Type=simple
ExecStart=/usr/sbin/aide --check

[Install]
WantedBy=multi-user.target
```

Create or edit the file `/etc/systemd/system/aidecheck.timer` and add the following lines:

```
[Unit]
Description=Aide check every day at 5AM

[Timer]
OnCalendar=*-*-* 05:00:00
Unit=aidecheck.service

[Install]
WantedBy=multi-user.target
```

Run the following commands:

```
# chown root:root /etc/systemd/system/aidecheck.*
# chmod 0644 /etc/systemd/system/aidecheck.*

# systemctl daemon-reload

# systemctl enable aidecheck.service
# systemctl --now enable aidecheck.timer
```

## References:

1. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.service>
2. <https://github.com/konstruktoid/hardening/blob/master/config/aidecheck.timer>

## Additional Information:

The checking in this recommendation occurs every day at 5am. Alter the frequency and time of the checks in compliance with site policy.

## NIST SP 800-53 Rev. 5:

- AU-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.14 Log Sensitive Data Access</u> Log sensitive data access, including modification and disposal.			●
v7	<u>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</u> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

## ***1.4 Secure Boot Settings***

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

### *1.4.1 Ensure bootloader password is set (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters.

#### **Rationale:**

Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

#### **Impact:**

If password protection is enabled, only the designated superuser can edit a Grub 2 menu item by pressing "e" or access the GRUB 2 command line by pressing "c"

If GRUB 2 is set up to boot automatically to a password-protected menu entry the user has no option to back out of the password prompt to select another menu entry. Holding the SHIFT key will not display the menu in this case. The user must enter the correct username and password. If unable, the configuration files will have to be edited via the LiveCD or other means to fix the problem

You can add `--unrestricted` to the menu entries to allow the system to boot without entering a password. Password will still be required to edit menu items.

## Audit:

Run the following script to verify the bootloader password has been set:

```
#!/usr/bin/env bash

{
    tst1="" tst2="" output=""
    grubdir=$(dirname "$(find /boot -type f \(\ -name 'grubenv' -o -name
'grub.conf' -o -name 'grub.cfg' \) -exec grep -El
'^\s*(kernelopts=|linux|kernel)' {} \;)")
    if [ -f "$grubdir/user.cfg" ]; then
        grep -Pq '^h*GRUB2_PASSWORD\h*=\h*.' "$grubdir/user.cfg" &&
output="bootloader password set in \"$grubdir/user.cfg\""
    fi
    if [ -z "$output" ]; then
        grep -Piq '^h*set\h+superusers\h*=\h*?'[^"\n\r]+?(\h+.*?)$'
"$grubdir/grub.cfg" && tst1=pass
        grep -Piq '^h*password(_pbkdf2)?\h+\H+\h+.' "$grubdir/grub.cfg" &&
tst2=pass
        [ "$tst1" = pass ] && [ "$tst2" = pass ] && output="bootloader password
set in \"$grubdir/grub.cfg\""
    fi
    [ -n "$output" ] && echo -e "\n\n PASSED! $output\n\n"
}
```

## Remediation:

Create an encrypted password with `grub2-setpassword`:

```
# grub2-setpassword

Enter password: <password>
Confirm password: <password>
```

Run the following command to update the `grub2` configuration:

```
# grub2-mkconfig -o "$(dirname "$(find /boot -type f \(\ -name 'grubenv' -o -
-name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl
'^\h*(kernelopts=|linux|kernel)' {} \;)/grub.cfg"
```

## Additional Information:

This recommendation is designed around the `grub2` bootloader, if Lilo or another bootloader is in use in your environment enact equivalent settings.

## NIST SP 800-53 Rev. 5:

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

## *1.4.2 Ensure permissions on bootloader config are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The grub files contain information on boot settings and passwords for unlocking boot options.

The grub2 configuration is usually `grub.cfg`. On newer grub2 systems the encrypted bootloader password is contained in `user.cfg`.

If the system uses UEFI, `/boot/efi` is a vfat filesystem. The vfat filesystem itself doesn't have the concept of permissions but can be mounted under Linux with whatever permissions desired.

### **Rationale:**

Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.

## Audit:

Run the following script to verify correct permissions, ownership, and group for the grub files:

```
#!/usr/bin/env bash

{
    output="" output2="" output3="" output4=""
    grubdir=$(dirname $(find /boot -type f \(\ -name 'grubenv' -o -name
'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl
'^\h*(kernelopts=linux|kernel)\{\} ;;"))
    for grubfile in $grubdir/user.cfg $grubdir/grubenv $grubdir/grub.cfg; do
        if [ -f "$grubfile" ]; then
            if stat -c "%a" "$grubfile" | grep -Pq '^h*[0-7]00$'; then
                output="$output\npermissions on \"$grubfile\" are \"$(stat -c
"%a" "$grubfile")\""
            else
                output3="$output3\npermissions on \"$grubfile\" are \"$(stat -c
"%a" "$grubfile")\""
            fi
            if stat -c "%u:%g" "$grubfile" | grep -Pq '^h*0:0$'; then
                output2="$output2\n\"$grubfile\" is owned by \"$(stat -c \"%U\""
"$grubfile\")\" and belongs to group \"$(stat -c \"%G\" \"$grubfile\")\""
            else
                output4="$output4\n\"$grubfile\" is owned by \"$(stat -c \"%U\""
"$grubfile\")\" and belongs to group \"$(stat -c \"%G\" \"$grubfile\")\""
            fi
        fi
    done
    if [[ -n "$output" && -n "$output2" && -z "$output3" && -z "$output4" ]]; then
        echo -e "\nPASSED:"
        [ -n "$output" ] && echo -e "$output"
        [ -n "$output2" ] && echo -e "$output2"
    else
        echo -e "\nFAILED:"
        [ -n "$output3" ] && echo -e "$output3"
        [ -n "$output4" ] && echo -e "$output4"
    fi
}
```

## **Remediation:**

Run the following commands to set ownership and permissions on your grub configuration file(s):

```
# [ -f /boot/grub2/grub.cfg ] && chown root:root /boot/grub2/grub.cfg  
# [ -f /boot/grub2/grub.cfg ] && chmod og-rwx /boot/grub2/grub.cfg  
  
# [ -f /boot/grub2/grubenv ] && chown root:root /boot/grub2/grubenv  
# [ -f /boot/grub2/grubenv ] && chmod og-rwx /boot/grub2/grubenv  
  
# [ -f /boot/grub2/user.cfg ] && chown root:root /boot/grub2/user.cfg  
# [ -f /boot/grub2/user.cfg ] && chmod og-rwx /boot/grub2/user.cfg
```

**OR** If the system uses UEFI, edit /etc/fstab and add the fmask=0077, uid=0, and gid=0 options:

*Example:*

```
<device> /boot/efi vfat defaults,umask=0027,fmask=0077,uid=0,gid=0 0 0
```

*Note: This may require a re-boot to enable the change*

## **Additional Information:**

This recommendation is designed around the grub bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.4.3 Ensure authentication is required when booting into rescue mode (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following commands and verify that `systemd-sulogin-shell rescue` is used to start the rescue mode:

```
# grep -r /systemd-sulogin-shell /usr/lib/systemd/system/rescue.service  
/etc/systemd/system/rescue.service.d  
  
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

This line must not be different in any output and must appear at least once.

#### **Remediation:**

The `systemd` drop-in files must be created if it is necessary to change the default settings: Create the file `/etc/systemd/system/rescue.service.d/00-require-auth.conf` which contains only the configuration to be overridden:

```
[Service]  
ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue
```

#### **Additional Information:**

`systemd-unit(5)`

**CIS Controls:**

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

## ***1.5 Additional Process Hardening***

### *1.5.1 Ensure core dump storage is disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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:**

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems.

#### **Audit:**

Run the following command to verify Storage is set to none in /etc/systemd/coredump.conf:

```
# grep -i '^storage\s*=\s*none' /etc/systemd/coredump.conf
Storage=none
```

#### **Remediation:**

Edit /etc/systemd/coredump.conf and edit or add the following line:

```
Storage=none
```

#### **References:**

1. <https://www.freedesktop.org/software/systemd/man/coredump.conf.html>

## *1.5.2 Ensure core dump backtraces are disabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **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:**

A core dump includes a memory image taken at the time the operating system terminates an application. The memory image could contain sensitive data and is generally useful only for developers trying to debug problems, increasing the risk to the system.

### **Audit:**

Run the following command to verify `ProcessSizeMax` is set to 0 in `/etc/systemd/coredump.conf`:

```
# grep -i '^ProcessSizeMax\s*=\s*0' /etc/systemd/coredump.conf
ProcessSizeMax=0
```

### **Remediation:**

Edit or add the following line in `/etc/systemd/coredump.conf`:

```
ProcessSizeMax=0
```

### **Default Value:**

`ProcessSizeMax=2G`

### **References:**

1. <https://www.freedesktop.org/software/systemd/man/coredump.conf.html>

**Additional Information:**

**NIST SP 800-53 Rev. 5:**

- CM-6b.

### **1.5.3 Ensure address space layout randomization (ASLR) is enabled (Automated)**

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 script to verify kernel.randomize\_va\_space is set to 2:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="kernel.randomize_va_space"
    kpvalue="2"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## **Remediation:**

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

*Example:*

```
# printf "  
kernel.randomize_va_space = 2  
" >> /etc/sysctl.d/60-kernel_sysctl.conf
```

Run the following command to set the active kernel parameter:

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

## **References:**

1. CCI-000366: The organization implements the security configuration settings
2. NIST SP 800-53 :: CM-6 b
3. NIST SP 800-53A :: CM-6.1 (iv)
4. NIST SP 800-53 Revision 4 :: CM-6 b

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●

## **1.6 Mandatory Access Control**

Mandatory Access Control (MAC) provides an additional layer of access restrictions to processes on top of the base Discretionary Access Controls. By restricting how processes can access files and resources on a system the potential impact from vulnerabilities in the processes can be reduced.

**Impact:** Mandatory Access Control limits the capabilities of applications and daemons on a system, while this can prevent unauthorized access the configuration of MAC can be complex and difficult to implement correctly preventing legitimate access from occurring.

### **1.6.1 Configure SELinux**

SELinux implements Mandatory Access Control (MAC). Every process and system resource has a special security label called an SELinux context. A SELinux context, sometimes referred to as an SELinux label, is an identifier which abstracts away the system-level details and focuses on the security properties of the entity. Not only does this provide a consistent way of referencing objects in the SELinux policy, but it also removes any ambiguity that can be found in other identification methods. For example, a file can have multiple valid path names on a system that makes use of bind mounts.

The SELinux policy uses these contexts in a series of rules which define how processes can interact with each other and the various system resources. By default, the policy does not allow any interaction unless a rule explicitly grants access.

In Rocky Linux 8, system services are controlled by the systemd daemon; systemd starts and stops all services, and users and processes communicate with systemd using the systemctl utility. The systemd daemon can consult the SELinux policy and check the label of the calling process and the label of the unit file that the caller tries to manage, and then ask SELinux whether or not the caller is allowed the access. This approach strengthens access control to critical system capabilities, which include starting and stopping system services.

This automatically limits the damage that the software can do to files accessible by the calling user. The user does not need to take any action to gain this benefit. For an action to occur, both the traditional DAC permissions must be satisfied as well as the SELinux MAC rules. The action will not be allowed if either one of these models does not permit the action. In this way, SELinux rules can only make a system's permissions more restrictive and secure. SELinux requires a complex policy to allow all the actions required of a system under normal operation. Two such policies have been designed for use with Rocky Linux and are included with the system: `targeted` and `mls`. These are described as follows:

- `targeted`: targeted processes run in their own domain, called a confined domain. In a confined domain, the files that a targeted process has access to are limited. If a confined process is compromised by an attacker, the attacker's access to resources and the possible damage they can do is also limited. SELinux denies access to these resources and logs the denial.
- `mls`: implements Multi-Level Security (MLS), which introduces even more kinds of labels (sensitivity and category) and rules that govern access based on these.

This section provides guidance for the configuration of the `targeted` policy.

## **Notes:**

- Remember that SELinux policy rules are checked after DAC rules. SELinux policy rules are not used if DAC rules deny access first, which means that no SELinux denial is logged if the traditional DAC rules prevent the access.
- This section only applies if SELinux is in use on the system. Additional Mandatory Access Control systems exist.
- To avoid incorrect SELinux labeling and subsequent problems, ensure that you start services using a systemctl start command.

## **References:**

1. NSA SELinux resources:
  1. <http://www.nsa.gov/research/selinux>
  2. <http://www.nsa.gov/research/selinux/list.shtml>
2. Fedora SELinux resources:
  1. FAQ: <http://docs.fedoraproject.org/selinux-faq>
  2. User Guide: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html-single/using\\_selinux/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/using_selinux/index)
  3. Managing Services Guide: <http://docs.fedoraproject.org/selinux-managing-confined-services-guide>
3. SELinux Project web page and wiki:
  1. <http://www.selinuxproject.org>

### *1.6.1.1 Ensure SELinux is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

SELinux provides Mandatory Access Control.

#### **Rationale:**

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

#### **Audit:**

Verify SELinux is installed.

Run the following command:

```
# rpm -q libselinux  
libselinux-<version>
```

#### **Remediation:**

Run the following command to install SELinux:

```
# dnf install libselinux
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### *1.6.1.2 Ensure SELinux is not disabled in bootloader configuration (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.

#### **Rationale:**

SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

#### **Impact:**

Files created while SELinux is disabled are not labeled at all. This behavior causes problems when changing to enforcing mode because files are labeled incorrectly or are not labeled at all. To prevent incorrectly labeled and unlabeled files from causing problems, file systems are automatically relabeled when changing from the disabled state to permissive or enforcing mode. This can be a long running process that should be accounted for as it may extend downtime during initial re-boot.

#### **Audit:**

Run the following command to verify that neither the `selinux=0` or `enforcing=0` parameters have been set:

```
# grep -P -- '^h*(kernelopts=|linux|kernel)' $(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \)) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \; | grep -E -- '(selinux=0|enforcing=0)'
```

Nothing should be returned

## **Remediation:**

Run the following command to remove all instances of `selinux=0` and `enforcing=0` from all `CMDLINE_LINUX` parameters:

```
grubby --update-kernel ALL --remove-args 'selinux=0 enforcing=0'
```

## **Additional Information:**

This recommendation is designed around the grub 2 bootloader, if LILO or another bootloader is in use in your environment enact equivalent settings.

## **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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.6.1.3 Ensure SELinux policy is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only.

#### **Rationale:**

Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

#### **Audit:**

Run the following commands and ensure output matches either "targeted" or "mls":

```
# grep -E '^s*SELINUXTYPE=(targeted|mls)\b' /etc/selinux/config  
SELINUXTYPE=targeted  
  
# sestatus | grep Loaded  
  
Loaded policy name:           targeted
```

#### **Remediation:**

Edit the `/etc/selinux/config` file to set the SELINUXTYPE parameter:

```
SELINUXTYPE=targeted
```

#### **Additional Information:**

If your organization requires stricter policies, ensure that they are set in the `/etc/selinux/config` file.

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

#### *1.6.1.4 Ensure the SELinux mode is not disabled (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- Enforcing - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- Permissive - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- Disabled - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

**Note:** you can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd\_t domain permissive:

```
# semanage permissive -a httpd_t
```

##### **Rationale:**

Running SELinux in disabled mode is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

## **Audit:**

Run the following commands and ensure output matches:

Run the following command to verify SELinux's current mode:

```
# getenforce  
  
Enforcing  
-OR-  
Permissive
```

Run the following command to verify SELinux's configured mode:

```
# grep -Ei '^SELINUX=(enforcing|permissive)' /etc/selinux/config  
  
SELINUX=enforcing  
-OR-  
SELINUX=permissive
```

## **Remediation:**

Run one of the following commands to set SELinux's running mode:

To set SELinux mode to Enforcing:

```
# setenforce 1
```

*OR*

To set SELinux mode to Permissive:

```
# setenforce 0
```

Edit the `/etc/selinux/config` file to set the SELINUX parameter:

For Enforcing mode:

```
SELINUX=enforcing
```

*OR*

For Permissive mode:

```
SELINUX=permissive
```

## **References:**

1. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/sect-security-enhanced\\_linux-introduction-selinux\\_modes](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-introduction-selinux_modes)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.6.1.5 Ensure the SELinux mode is enforcing (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

SELinux can run in one of three modes: disabled, permissive, or enforcing:

- Enforcing - Is the default, and recommended, mode of operation; in enforcing mode SELinux operates normally, enforcing the loaded security policy on the entire system.
- Permissive - The system acts as if SELinux is enforcing the loaded security policy, including labeling objects and emitting access denial entries in the logs, but it does not actually deny any operations. While not recommended for production systems, permissive mode can be helpful for SELinux policy development.
- Disabled - Is strongly discouraged; not only does the system avoid enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future

*Note: you can set individual domains to permissive mode while the system runs in enforcing mode. For example, to make the httpd\_t domain permissive:*

```
# semanage permissive -a httpd_t
```

#### **Rationale:**

Running SELinux in disabled mode the system not only avoids enforcing the SELinux policy, it also avoids labeling any persistent objects such as files, making it difficult to enable SELinux in the future.

Running SELinux in Permissive mode, though helpful for developing SELinux policy, only logs access denial entries, but does not deny any operations.

## **Audit:**

Run the following commands and ensure output matches:

Run the following command to verify SELinux's current mode:

```
# getenforce  
Enforcing
```

Run the following command to verify SELinux's configured mode:

```
# grep -i SELINUX=enforcing /etc/selinux/config  
SELINUX=enforcing
```

## **Remediation:**

Run the following command to set SELinux's running mode:

```
# setenforce 1
```

Edit the `/etc/selinux/config` file to set the SELINUX parameter:

For Enforcing mode:

```
SELINUX=enforcing
```

## **References:**

1. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/security-enhanced\\_linux-introduction-selinux\\_modes](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/security-enhanced_linux-introduction-selinux_modes)
2. CCI-002165: The information system enforces organization-defined discretionary access control policies over defined subjects and objects.
3. NIST SP 800-53 Revision 4 :: AC-3 (4)
4. CCI-002696: The information system verifies correct operation of organization-defined security functions.
5. NIST SP 800-53 Revision 4 :: SI-6 a

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *1.6.1.6 Ensure no unconfined services exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Unconfined processes run in unconfined domains

#### **Rationale:**

For unconfined processes, SELinux policy rules are applied, but policy rules exist that allow processes running in unconfined domains almost all access. Processes running in unconfined domains fall back to using DAC rules exclusively. If an unconfined process is compromised, SELinux does not prevent an attacker from gaining access to system resources and data, but of course, DAC rules are still used. SELinux is a security enhancement on top of DAC rules – it does not replace them

#### **Audit:**

Run the following command and verify no output is produced:

```
# ps -ez | grep unconfined_service_t
```

#### **Remediation:**

Investigate any unconfined processes found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

#### **Additional Information:**

Occasionally certain daemons such as backup or centralized management software may require running unconfined. Any such software should be carefully analyzed and documented before such an exception is made.

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

### *1.6.1.7 Ensure SETroubleshoot is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server

#### **Description:**

The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.

#### **Rationale:**

The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.

#### **Audit:**

Verify `setroubleshoot` is not installed.

Run the following command:

```
# rpm -q setroubleshoot  
package setroubleshoot is not installed
```

#### **Remediation:**

Run the following command to uninstall `setroubleshoot`:

```
# dnf remove setroubleshoot
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> 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.	●	●	●

### *1.6.1.8 Ensure the MCS Translation Service (mcstrans) is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`

#### **Rationale:**

Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.

#### **Audit:**

Verify `mcstrans` is not installed.

Run the following command:

```
# rpm -q mcstrans
package mcstrans is not installed
```

#### **Remediation:**

Run the following command to uninstall `mcstrans`:

```
# dnf remove mcstrans
```

**CIS Controls:**

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

## **1.7 Command Line Warning Banners**

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

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

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

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

### *1.7.1 Ensure message of the day is configured properly (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

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

#### **Rationale:**

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

#### **Audit:**

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

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

Run the following command and verify no results are returned:

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

**Remediation:**

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

OR

If the motd is not used, this file can be removed.

Run the following command to remove the motd file:

```
# rm /etc/motd
```

## *1.7.2 Ensure local login warning banner is configured properly (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

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

### **Rationale:**

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

### **Audit:**

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

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

Run the following command and verify no results are returned:

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

**Remediation:**

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

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

### *1.7.3 Ensure remote login warning banner is configured properly (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

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

#### **Rationale:**

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

#### **Audit:**

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

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

Run the following command and verify no results are returned:

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

**Remediation:**

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

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

## *1.7.4 Ensure permissions on /etc/motd are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

### **Remediation:**

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

```
# chown root:root /etc/motd
# chmod u-x,go-wx /etc/motd
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

## *1.7.5 Ensure permissions on /etc/issue are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

### **Remediation:**

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

```
# chown root:root /etc/issue
# chmod u-x,go-wx /etc/issue
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b></p> <p>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.</p>			
v7	<p><b>14.6 Protect Information through Access Control Lists</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>			

## *1.7.6 Ensure permissions on /etc/issue.net are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

### **Remediation:**

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

```
# chown root:root /etc/issue.net
# chmod u-x,go-wx /etc/issue.net
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

## **1.8 GNOME Display Manager**

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

The system will need to be re-booted, or brought down to run level 3 and back to run level 5 for changes to the GDM configuration to take effect.

**Note:** If GDM is not installed on the system, this section can be skipped

### *1.8.1 Ensure GNOME Display Manager is removed (Manual)*

#### **Profile Applicability:**

- Level 2 - Server

#### **Description:**

The GNOME Display Manager (GDM) is a program that manages graphical display servers and handles graphical user logins.

#### **Rationale:**

If a Graphical User Interface (GUI) is not required, it should be removed to reduce the attack surface of the system.

#### **Impact:**

Removing the GNOME Display manager will remove the GUI from the system.

#### **Audit:**

Run the following command and verify the output:

```
# rpm -q gdm  
package gdm is not installed
```

#### **Remediation:**

Run the following command to remove the `gdm` package

```
# dnf remove gdm
```

#### **References:**

1. <https://wiki.gnome.org/Projects/GDM>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

## *1.8.2 Ensure GDM login banner is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

### **Rationale:**

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

**Note:** If a graphical login is not required, it should be removed to reduce the attack surface of the system.

### **Audit:**

Verify that /etc/dconf/profile/gdm exists and includes the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Verify that a file exists in /etc/dconf/db/gdm.d/ and includes the following: (*This is typically /etc/dconf/db/gdm.d/01-banner-message*)

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

## **Remediation:**

Edit or create the file `/etc/dconf/profile/gdm` and add the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Edit or create the file `/etc/dconf/db/gdm.d/` and add the following: (*This is typically /etc/dconf/db/gdm.d/01-banner-message*)

```
[org/gnome/login-screen]
banner-message-enable=true
banner-message-text='<banner message>'
```

*Example Banner Text:* 'Authorized users only. All activity may be monitored and reported.'

Run the following command to update the system databases:

```
# dconf update
```

## **Additional Information:**

Additional options and sections may appear in the `/etc/dconf/db/gdm.d/01-banner-message` file.

If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user and apply an equivalent banner.

## **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.1 Establish and Maintain a Secure Configuration Process</b></p> <p>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.</p>	●	●	●
v7	<p><b>5.1 Establish Secure Configurations</b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

### *1.8.3 Ensure last logged in user display is disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

GDM is the GNOME Display Manager which handles graphical login for GNOME based systems.

#### **Rationale:**

Displaying the last logged in user eliminates half of the Userid/Password equation that an unauthorized person would need to log on.

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place.

#### *Notes:*

- *If a graphical login is not required, it should be removed to reduce the attack surface of the system.*
- *If a different GUI login service is in use and required on the system, consult your documentation to disable displaying the last logged on user*

#### **Audit:**

Verify that /etc/dconf/profile/gdm exists and includes the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Verify that a file exists in /etc/dconf/db/gdm.d/ and includes the following: (*This is typically /etc/dconf/db/gdm.d/00-login-screen*)

```
[org/gnome/login-screen]
disable-user-list=true
```

## **Remediation:**

Edit or create the file `/etc/dconf/profile/gdm` and add the following:

```
user-db:user
system-db:gdm
file-db:/usr/share/gdm/greeter-dconf-defaults
```

Edit or create the file `/etc/dconf/db/gdm.d/` and add the following: (*This is typically /etc/dconf/db/gdm.d/00-login-screen*)

```
[org/gnome/login-screen]
# Do not show the user list
disable-user-list=true
```

Run the following command to update the system databases:

```
# dconf update
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## **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.	●	●	●

## *1.8.4 Ensure XDMCP is not enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

X Display Manager Control Protocol (XDMCP) is designed to provide authenticated access to display management services for remote displays

### **Rationale:**

XDMCP is inherently insecure.

- XDMCP is not a ciphered protocol. This may allow an attacker to capture keystrokes entered by a user
- XDMCP is vulnerable to man-in-the-middle attacks. This may allow an attacker to steal the credentials of legitimate users by impersonating the XDMCP server.

### **Audit:**

Run the following command and verify the output:

```
# grep -Eis '^s*Enable\s*=\\s*true' /etc/gdm/custom.conf
```

Nothing should be returned

### **Remediation:**

Edit the file /etc/gdm/custom.conf and remove the line

```
Enable=true
```

### **Default Value:**

false (This is denoted by no Enabled= entry in the file /etc/gdm/custom.conf in the [xdmcp] section)

### **References:**

1. <https://help.gnome.org/admin/gdm/2.32/configuration.html.en>

**CIS Controls:**

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

## *1.8.5 Ensure automatic mounting of removable media is disabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

### **Description:**

By default GNOME automatically mounts removable media when inserted as a convenience to the user.

### **Rationale:**

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

### **Impact:**

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

### **Audit:**

Run the following command to verify automatic mounting is disabled:

```
# gsettings get org.gnome.desktop.media-handling automount  
false
```

Verify result is "false".

## **Remediation:**

Ensure that automatic mounting of media is disabled for all GNOME users:

```
# cat << EOF >> /etc/dconf/db/local.d/00-media-automount
[org/gnome/desktop/media-handling]
automount=false
automount-open=false
EOF
```

Apply the changes with:

```
# dconf update
```

## **References:**

1. <https://access.redhat.com/solutions/20107>

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>10.3 Disable Autorun and Autoplay for Removable Media</u> Disable autorun and autoplay auto-execute functionality for removable media.	●	●	●
v7	<u>8.5 Configure Devices Not To Auto-run Content</u> Configure devices to not auto-run content from removable media.	●	●	●

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

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

Newer patches may contain security enhancements that would not be available through the latest full update. As a result, it is recommended that the latest software patches be used to take advantage of the latest functionality. 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:**

Run the following command and verify there are no updates or patches to install:

```
# dnf check-update
```

### **Remediation:**

Use your package manager to update all packages on the system according to site policy. The following command will install all available updates:

```
# dnf update
```

### **Additional Information:**

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

```
# dnf check-update
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>7.3 Perform Automated Operating System Patch Management</b></p> <p>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v8	<p><b>7.4 Perform Automated Application Patch Management</b></p> <p>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.</p>	●	●	●
v7	<p><b>3.4 Deploy Automated Operating System Patch Management Tools</b></p> <p>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.</p>	●	●	●

## *1.10 Ensure system-wide crypto policy is not legacy (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The system-wide crypto-policies followed by the crypto core components allow consistently deprecating and disabling algorithms system-wide.

The individual policy levels (DEFAULT, LEGACY, FUTURE, and FIPS) are included in the crypto-policies(7) package.

### **Rationale:**

If the Legacy system-wide crypto policy is selected, it includes support for TLS 1.0, TLS 1.1, and SSH2 protocols or later. The algorithms DSA, 3DES, and RC4 are allowed, while RSA and Diffie-Hellman parameters are accepted if larger than 1023-bits.

These legacy protocols and algorithms can make the system vulnerable to attacks, including those listed in RFC 7457

### **Impact:**

Environments that require compatibility with older insecure protocols may require the use of the less secure LEGACY policy level.

### **Audit:**

Run the following command to verify that the system-wide crypto policy is not LEGACY

```
# grep -E -i '^\\s*LEGACY\\s*(\\s+#.*)?\\$' /etc/crypto-policies/config
```

Verify that no lines are returned

## **Remediation:**

Run the following command to change the system-wide crypto policy

```
# update-crypto-policies --set <CRYPTO POLICY>
```

## **Example:**

```
# update-crypto-policies --set DEFAULT
```

Run the following to make the updated system-wide crypto policy active

```
# update-crypto-policies
```

## **Default Value:**

DEFAULT

## **References:**

1. CRYPTO-POLICIES(7)
2. <https://access.redhat.com/articles/3642912#what-polices-are-provided-1>

## **Additional Information:**

To switch the system to FIPS mode, run the following command:

```
fips-mode-setup --enable
```

## **NIST SP 800-53 Rev. 5:**

- SC-8

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 Encrypt All Sensitive Information in Transit</b> Encrypt all sensitive information in transit.		●	●

## **2 Services**

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

## ***2.1 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 Ensure time synchronization is in use (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

**Note:** If another method for time synchronization is being used, this section may be skipped.

#### **Rationale:**

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

#### **Audit:**

Run the following commands to verify that chrony is installed:

```
# rpm -q chrony  
chrony-<version>
```

#### **Remediation:**

Run the following command to install `chrony`:

```
# dnf install chrony
```

**Additional Information:**

On systems where host based time synchronization is not available, verify that chrony is installed.

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

**NIST SP 800-53 Rev. 5:**

- AU-3
- AU-12

**CIS Controls:**

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

## *2.1.2 Ensure chrony is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

Multiple servers may be configured.

Run the following command and verify OPTIONS includes '-u chrony':

```
# grep ^OPTIONS /etc/sysconfig/chronyd  
OPTIONS="-u chrony"
```

Additional options may be present.

### **Remediation:**

Add or edit server or pool lines to /etc/chrony.conf as appropriate:

```
server <remote-server>
```

Add or edit the OPTIONS in /etc/sysconfig/chronyd to include '-u chrony':

```
OPTIONS="-u chrony"
```

**Additional Information:**

On systems where host based time synchronization is not available, verify that chrony is installed.

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

**NIST SP 800-53 Rev. 5:**

- AU-3
- AU-12

**CIS Controls:**

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

## ***2.2 Special Purpose Services***

This section describes services that are installed on systems that specifically need to run these services. If any of these services are not required, it is recommended that the package be removed, or the service be masked to reduce the potential attack surface.

**Note:** This should not be considered a comprehensive list of services not required for normal system operation. You may wish to consider additions to those listed here for your environment

## 2.2.1 Ensure xinetd is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The eXtended InterNET Daemon (`xinetd`) is an open source super daemon that replaced the original `inetd` daemon. The `xinetd` daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests.

### Rationale:

If there are no xinetd services required, it is recommended that the package be removed to reduce the attack surface area of the system.

*Note: If an xinetd service or services are required, ensure that any xinetd service not required is stopped and disabled*

### Audit:

Run the following command to verify `xinetd` is not installed:

```
# rpm -q xinetd  
package xinetd is not installed
```

### Remediation:

Run the following command to remove `xinetd`:

```
# dnf remove xinetd
```

### Additional Information:

#### NIST SP 800-53 Rev. 5:

- CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><b>2.6 <u>Address unapproved software</u></b></p> <p>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●
v7	<p><b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

## *2.2.2 Ensure xorg-x11-server-common is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server

### **Description:**

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

### **Rationale:**

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

### **Impact:**

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

### **Audit:**

Run the following command to Verify X Windows Server is not installed.

```
# rpm -q xorg-x11-server-common  
package xorg-x11-server-common is not installed
```

### **Remediation:**

Run the following command to remove the X Windows Server packages:

```
# dnf remove xorg-x11-server-common
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.3 Ensure Avahi Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 2 - Workstation

### **Description:**

Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

### **Rationale:**

Automatic discovery of network services is not normally required for system functionality. It is recommended to remove this package to reduce the potential attack surface.

### **Audit:**

Run one of the following command to verify `avahi-autoipd` and `avahi` are not installed:

```
# rpm -q avahi-autoipd avahi
package avahi-autoipd is not installed
package avahi is not installed
```

### **Remediation:**

Run the following commands to stop, mask and remove `avahi-autoipd` and `avahi`:

```
# systemctl stop avahi-daemon.socket avahi-daemon.service
# dnf remove avahi-autoipd avahi
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.4 Ensure CUPS is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server

### **Description:**

The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability.

### **Rationale:**

If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be removed to reduce the potential attack surface.

*Note: Removing CUPS will prevent printing from the system*

### **Impact:**

Disabling CUPS will prevent printing from the system, a common task for workstation systems.

### **Audit:**

Run the following command to verify cups is not installed:

```
# rpm -q cups  
package cups is not installed
```

### **Remediation:**

Run the following command to remove cups:

```
# dnf remove cups
```

### **References:**

1. More detailed documentation on CUPS is available at the project homepage at <http://www.cups.org>.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.5 Ensure DHCP Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

### **Rationale:**

Unless a system is specifically set up to act as a DHCP server, it is recommended that the rpm -q dhcp-server package be removed to reduce the potential attack surface.

### **Audit:**

Run the following command to verify `dhcp` is not installed:

```
# rpm -q dhcp-server  
package dhcp-server is not installed
```

### **Remediation:**

Run the following command to remove `dhcp`:

```
# dnf remove dhcp-server
```

### **References:**

1. `dhcpcd(8)`

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.6 Ensure DNS Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network.

### **Rationale:**

Unless a system is specifically designated to act as a DNS server, it is recommended that the package be removed to reduce the potential attack surface.

### **Audit:**

Run one of the following commands to verify `bind` is not installed:

```
# rpm -q bind  
package bind is not installed
```

### **Remediation:**

Run the following command to remove `bind`:

```
# dnf remove bind
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.7 Ensure FTP Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

### **Rationale:**

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be removed to reduce the potential attack surface.

### **Audit:**

Run the following command to verify `ftp` is not installed:

```
# rpm -q ftp  
package ftp is not installed
```

### **Remediation:**

Run the following command to remove `ftp`:

```
# dnf remove ftp
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.8 Ensure VSFTP Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

FTP (File Transfer Protocol) is a traditional and widely used standard tool for transferring files between a server and clients over a network, especially where no authentication is necessary (permits anonymous users to connect to a server).

### **Rationale:**

Unless there is a need to run the system as a FTP server, it is recommended that the package be removed to reduce the potential attack surface.

### **Audit:**

Run the following command to verify `vsftpd` is not installed:

```
# rpm -q vsftpd  
package vsftpd is not installed
```

### **Remediation:**

Run the following command to remove `vsftpd`:

```
# dnf remove vsftpd
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.9 Ensure TFTP Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

### **Rationale:**

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

### **Audit:**

Run the following command to verify `tftp-server` is not installed:

```
# rpm -q tftp-server  
package tftp-server is not installed
```

### **Remediation:**

Run the following command to remove `tftp-server`:

```
# dnf remove tftp-server
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.10 Ensure a web server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Web servers provide the ability to host web site content.

### **Rationale:**

Unless there is a need to run the system as a web server, it is recommended that the packages be removed to reduce the potential attack surface.

**Note:** Several http servers exist. They should also be audited, and removed, if not required.

### **Audit:**

Run the following command to verify `httpd` and `nginx` are not installed:

```
# rpm -q httpd nginx
package httpd is not installed
package nginx is not installed
```

### **Remediation:**

Run the following command to remove `httpd` and `nginx`:

```
# dnf remove httpd nginx
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.11 Ensure IMAP and POP3 server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

`dovecot` is an open source IMAP and POP3 server for Linux based systems.

### **Rationale:**

Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the package be removed to reduce the potential attack surface.

**Note:** Several IMAP/POP3 servers exist and can use other service names. These should also be audited and the packages removed if not required.

### **Audit:**

Run the following command to verify `dovecot` and `cyrus-imapd` are not installed:

```
# rpm -q dovecot cyrus-imapd  
package dovecot is not installed  
package cyrus-imapd is not installed
```

### **Remediation:**

Run the following command to remove `dovecot` and `cyrus-imapd`:

```
# dnf remove dovecot cyrus-imapd
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.12 Ensure Samba is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Server Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems.

### **Rationale:**

If there is no need to mount directories and file systems to Windows systems, then this package can be removed to reduce the potential attack surface.

### **Audit:**

Run the following command to verify `samba` is not installed:

```
# rpm -q samba  
package samba is not installed
```

### **Remediation:**

Run the following command to remove `samba`:

```
# dnf remove samba
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.2.13 Ensure HTTP Proxy Server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Squid is a standard proxy server used in many distributions and environments.

### **Rationale:**

Unless a system is specifically set up to act as a proxy server, it is recommended that the squid package be removed to reduce the potential attack surface.

**Note:** Several HTTP proxy servers exist. These should be checked and removed unless required.

### **Audit:**

Run the following command to verify squid is not installed:

```
# rpm -q squid  
package squid is not installed
```

### **Remediation:**

Run the following command to remove the squid package:

```
# dnf remove squid
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## 2.2.14 Ensure net-snmp is not installed (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

Net-SNMP is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

Support for SNMPv2 classic (a.k.a. "SNMPv2 historic" - RFCs 1441-1452) was dropped with the 4.0 release of the UCD-snmp package.

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

### Rationale:

The SNMP server can communicate using SNMPv1, which transmits data in the clear and does not require authentication to execute commands. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. If the the SNMP service is not required, the net-snmp package should be removed to reduce the attack surface of the system.

*Note: If SNMP is required:*

- *The server should be configured for SNMP v3 only. User Authentication and Message Encryption should be configured.*
- *If SNMP v2 is absolutely necessary, modify the community strings' values.*

### Audit:

Run the following command to verify net-snmp is not installed:

```
# rpm -q net-snmp
package net-snmp is not installed
```

## **Remediation:**

Run the following command to remove net-snmpd:

```
# dnf remove net-snmp
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-7

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 Address unapproved software</b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## *2.2.15 Ensure NIS server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `ypserv` package provides the Network Information Service (NIS). This service, formally known as Yellow Pages, is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

### **Rationale:**

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the `ypserv` package be removed, and if required a more secure services be used.

### **Audit:**

Run the following command to verify `ypserv` is not installed:

```
# rpm -q ypserv  
package ypserv is not installed
```

### **Remediation:**

Run the following command to remove `ypserv`:

```
# dnf remove ypserv
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><b>2.6 <u>Address unapproved software</u></b></p> <p>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●
v7	<p><b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

## *2.2.16 Ensure telnet-server is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `telnet-server` package contains the `telnet` daemon, which accepts connections from users from other systems via the `telnet` protocol.

### **Rationale:**

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow a user with access to sniff network traffic the ability to steal credentials. The `ssh` package provides an encrypted session and stronger security.

### **Audit:**

Run the following command to verify the `telnet-server` package is not installed:

```
rpm -q telnet-server  
package telnet-server is not installed
```

### **Remediation:**

Run the following command to remove the `telnet-server` package:

```
# dnf remove telnet-server
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v7	<p><b>2.6 <u>Address unapproved software</u></b></p> <p>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●
v7	<p><b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

## *2.2.17 Ensure mail transfer agent is configured for local-only mode (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.

### **Rationale:**

The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.

### *Notes:*

- *This recommendation is designed around the postfix mail server.*
- *Depending on your environment you may have an alternative MTA installed such as sendmail. If this is the case consult the documentation for your installed MTA to configure the recommended state.*

### **Audit:**

Run the following command to verify that the MTA is not listening on any non-loopback address ( 127.0.0.1 or ::1 )

Nothing should be returned

```
# ss -lntu | grep -E ':25\s' | grep -E -v '\s(127.0.0.1|::1):25\s'
```

## **Remediation:**

Edit `/etc/postfix/main.cf` and add the following line to the RECEIVING MAIL section. If the line already exists, change it to look like the line below:

```
inet_interfaces = loopback-only
```

Run the following command to restart postfix:

```
# systemctl restart postfix
```

## **CIS Controls:**

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

## *2.2.18 Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

If the system does not require network shares, it is recommended that the nfs-utils package be removed to reduce the attack surface of the system.

### **Impact:**

Many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-package is required as a dependency, the nfs-server should be disabled and masked to reduce the attack surface of the system.

### **Audit:**

Run the following command to verify nfs-utils is not installed:

```
# rpm -q nfs-utils
package nfs-utils is not installed
```

*OR*

If the nfs-package is required as a dependency, run the following command to verify that the nfs-server service is masked:

```
# systemctl is-enabled nfs-server
masked
```

## **Remediation:**

Run the following command to remove nfs-utils:

```
# dnf remove nfs-utils
```

*OR*

If the nfs-package is required as a dependency, run the following command to stop and mask the nfs-server service:

```
# systemctl --now mask nfs-server
```

## **Additional Information:**

Many of the libvirt packages used by Enterprise Linux virtualization are dependent on the nfs-utils package. If the nfs-package is required as a dependency, the nfs-server should be disabled and masked to reduce the attack surface of the system.

## **CIS Controls:**

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

## *2.2.19 Ensure rpcbind is not installed or the rpcbind services are masked (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The rpcbind utility maps RPC services to the ports on which they listen. RPC processes notify rpcbind when they start, registering the ports they are listening on and the RPC program numbers they expect to serve. The client system then contacts rpcbind on the server with a particular RPC program number. The rpcbind service redirects the client to the proper port number so it can communicate with the requested service

Portmapper is an RPC service, which always listens on tcp and udp 111, and is used to map other RPC services (such as nfs, nlockmgr, quotad, mountd, etc.) to their corresponding port number on the server. When a remote host makes an RPC call to that server, it first consults with portmap to determine where the RPC server is listening.

### **Rationale:**

A small request (~82 bytes via UDP) sent to the Portmapper generates a large response (7x to 28x amplification), which makes it a suitable tool for DDoS attacks. If rpcbind is not required, it is recommended that the rpcbind package be removed to reduce the attack surface of the system.

### **Impact:**

Many of the libvirt packages used by Enterprise Linux virtualization, and the nfs-utils package used for The Network File System (NFS), are dependent on the `rpcbind` package. If the `rpcbind` package is required as a dependency, the services `rpcbind.service` and `rpcbind.socket` should be stopped and masked to reduce the attack surface of the system.

## Audit:

Run the following command to verify `rpcbind` is not installed:

```
# rpm -q rpcbind  
package rpcbind is not installed
```

*OR*

If the `rpcbind` package is required as a dependency, run the following commands to verify that the `rpcbind` and `rpcbind.socket` services are masked:

```
# systemctl is-enabled rpcbind  
masked  
  
# systemctl is-enabled rpcbind.socket  
masked
```

## Remediation:

Run the following command to remove `nfs-utils`:

```
# dnf remove rpcbind
```

*OR*

If the `rpcbind` package is required as a dependency, run the following commands to stop and mask the `rpcbind` and `rpcbind.socket` services:

```
# systemctl --now mask rpcbind  
# systemctl --now mask rpcbind.socket
```

## CIS Controls:

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

## *2.2.20 Ensure rsync is not installed or the rsyncd service is masked (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

Unless required, the `rsync` package should be removed to reduce the attack surface area of the system.

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

**Note:** If a required dependency exists for the `rsync` package, but the `rsyncd` service is not required, the service should be masked.

### **Impact:**

There are packages that are dependent on the `rsync` package. If the `rsync` package is removed, these packages will be removed as well.

Before removing the `rsync` package, review any dependent packages to determine if they are required on the system. If a dependent package is required, mask the `rsyncd` service and leave the `rsync` package installed.

## Audit:

Run the following command to verify that `rsync` is not installed:

```
# rpm -q rsync  
package rsync is not installed
```

*OR*

Run the following command to verify the `rsyncd` service is masked:

```
# systemctl is-enabled rsyncd  
masked
```

## Remediation:

Run the following command to remove the `rsync` package:

```
# dnf remove rsync
```

*OR*

Run the following command to mask the `rsyncd` service:

```
# systemctl --now mask rsyncd
```

## CIS Controls:

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

## **2.3 Service Clients**

A number of insecure services exist. While disabling the servers prevents a local attack against these services, it is advised to remove their clients unless they are required.

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

### *2.3.1 Ensure NIS Client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (`ypbind`) was used to bind a machine to an NIS server and receive the distributed configuration files.

#### **Rationale:**

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

#### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### **Audit:**

Run the following command to verify that the `ypbind` package is not installed:

```
# rpm -q ypbnd  
package ypbnd is not installed
```

#### **Remediation:**

Run the following command to remove the `ypbind` package:

```
# dnf remove ypbnd
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

### *2.3.2 Ensure rsh client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `rsh` package contains the client commands for the `rsh` services.

#### **Rationale:**

These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the `rsh` package removes the clients for `rsh`, `rcp` and `rlogin`.

#### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### **Audit:**

Run the following command to verify that the `rsh` package is not installed:

```
# rpm -q rsh  
package rsh is not installed
```

#### **Remediation:**

Run the following command to remove the `rsh` package:

```
# dnf remove rsh
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

### *2.3.3 Ensure talk client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `talk` software makes it possible for users to send and receive messages across systems through a terminal session. The `talk` client, which allows initialization of talk sessions, is installed by default.

#### **Rationale:**

The software presents a security risk as it uses unencrypted protocols for communication.

#### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

#### **Audit:**

Run the following command to verify that the `talk` package is not installed:

```
# rpm -q talk  
package talk is not installed
```

#### **Remediation:**

Run the following command to remove the `talk` package:

```
# dnf remove talk
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

## *2.3.4 Ensure telnet client is not installed (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `telnet` package contains the `telnet` client, which allows users to start connections to other systems via the telnet protocol.

### **Rationale:**

The `telnet` protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The `ssh` package provides an encrypted session and stronger security and is included in most Linux distributions.

### **Impact:**

Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

### **Audit:**

Run the following command to verify that the `telnet` package is not installed:

```
# rpm -q telnet
package telnet is not installed
```

### **Remediation:**

Run the following command to remove the `telnet` package:

```
# dnf remove telnet
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

### *2.3.5 Ensure LDAP client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.

#### **Rationale:**

If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.

#### **Impact:**

Removing the LDAP client will prevent or inhibit using LDAP for authentication in your environment.

#### **Audit:**

Run the following command to verify that the `openldap-clients` package is not installed:

```
# rpm -q openldap-clients  
package openldap-clients is not installed
```

#### **Remediation:**

Run the following command to remove the `openldap-clients` package:

```
# dnf remove openldap-clients
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>2.6 <u>Address unapproved software</u></b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

### *2.3.6 Ensure TFTP client is not installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Trivial File Transfer Protocol (TFTP) is a simple protocol for exchanging files between two TCP/IP machines. TFTP servers allow connections from a TFTP Client for sending and receiving files.

#### **Rationale:**

TFTP does not have built-in encryption, access control or authentication. This makes it very easy for an attacker to exploit TFTP to gain access to files

#### **Audit:**

Run the following command to verify `tftp` is not installed:

```
# rpm -q tftp  
package tftp is not installed
```

#### **Remediation:**

Run the following command to remove `tftp`:

```
# dnf remove tftp
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

## *2.4 Ensure nonessential services are removed or masked (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

A network port is identified by its number, the associated IP address, and the type of the communication protocol such as TCP or UDP.

A listening port is a network port on which an application or process listens on, acting as a communication endpoint.

Each listening port can be open or closed (filtered) using a firewall. In general terms, an open port is a network port that accepts incoming packets from remote locations.

### **Rationale:**

Services listening on the system pose a potential risk as an attack vector. These services should be reviewed, and if not required, the service should be stopped, and the package containing the service should be removed. If required packages have a dependency, the service should be stopped and masked to reduce the attack surface of the system.

### **Audit:**

Run the following command:

```
# lsof -i -P -n | grep -v "(ESTABLISHED)"
```

Review the output to ensure that all services listed are required on the system. If a listed service is not required, remove the package containing the service. If the package containing the service is required, stop and mask the service

## **Remediation:**

Run the following command to remove the package containing the service:

```
# dnf remove <package_name>
```

*OR If required packages have a dependency:*

Run the following command to stop and mask the service:

```
# systemctl --now mask <service_name>
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-7

## **CIS Controls:**

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

## **3 Network Configuration**

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

**Note:**

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`

Function to check IPv6 status:

```

#!/usr/bin/env bash

check_ipv6()
{
    output=""
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"

    if [ -s "$grubfile" ]; then
        ! grep -P -- "^\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
        ipv6.disable=1 && output="IPv6 Disabled in \"$grubfile\""
    fi

    if grep -Pqs -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc && \
        grep -Pqs --
        "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc && \
        sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
        "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
        "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $"; then
            [ -n "$output" ] && output="$output, and in sysctl config" ||
            output="ipv6 disabled in sysctl config"
    fi

    [ -n "$output" ] && echo -e "\n$output\n" || echo -e "\nIPv6 is enabled on
the system\n"
}
check_ipv6

```

### ***3.1 Disable unused network protocols and devices***

To reduce the attack surface of a system, unused network protocols and devices should be disabled.

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.

### *3.1.1 Verify if IPv6 is enabled on the system (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices.

#### **Rationale:**

It is recommended that either IPv6 settings are configured OR IPv6 be disabled to reduce the attack surface of the system.

#### **Impact:**

IETF RFC 4038 recommends that applications are built with an assumption of dual stack.

If IPv6 is disabled through sysctl config, `SSH_X11forwarding` may no longer function as expected. We recommend that SSH X11forwarding be disabled, but if required, the following will allow for `SSH_X11forwarding` with IPv6 disabled through sysctl config:

Add the following line the `/etc/ssh/sshd_config` file:

```
AddressFamily inet
```

Run the following command to re-start the openSSH server:

```
# systemctl restart sshd
```

## Audit:

Run the following script to verify IPv6 status on the system:

```
#!/usr/bin/env bash

check_ipv6()
{
    output=""
    grubfile=$(find /boot -type f \( -name 'grubenv' -o -name 'grub.conf' -o -name 'grub.cfg' \) -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"

    if [ -s "$grubfile" ]; then
        ! grep -P -- "^\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq -- ipv6.disable=1 && output="IPv6 Disabled in \"$grubfile\""
        fi

    if grep -Pqs -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc && \
        grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $" $searchloc && \
        sysctl net.ipv6.conf.all.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)? $" && \
        sysctl net.ipv6.conf.default.disable_ipv6 | grep -Pqs --
"^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)? $"; then
        [ -n "$output" ] && output="$output, and in sysctl config" ||
        output="ipv6 disabled in sysctl config"
        fi

    [ -n "$output" ] && echo -e "\n$output\n" || echo -e "\nIPv6 is enabled on
the system\n"
}
check_ipv6
```

## **Remediation:**

If IPv6 is to be disabled, use **one** of the two following methods to disable IPv6 on the system:

To disable IPv6 through the GRUB2 config, run the following command to add `ipv6.disable=1` to the `GRUB_CMDLINE_LINUX` parameters:

```
grubby --update-kernel ALL --args 'ipv6.disable=1'
```

**OR** To disable IPv6 through sysctl settings, set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

*Example:*

```
# printf "
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
" >> /etc/sysctl.d/60-disable_ipv6.conf
```

Run the following command to set the active kernel parameters:

```
# {
    sysctl -w net.ipv6.conf.all.disable_ipv6=1
    sysctl -w net.ipv6.conf.default.disable_ipv6=1
    sysctl -w net.ipv6.route.flush=1
}
```

## **Additional Information:**

IPv4 is based on 32-bit addressing, limiting it to a total of 4.3 billion addresses. IPv6 is based on 128-bit addressing and can support 340 undecillion, which is 340 trillion<sup>3</sup> addresses. Having more addresses has grown in importance with the expansion of smart devices and connectivity. IPv6 provides more than enough globally unique IP addresses for every networked device currently on the planet, helping ensure providers can keep pace with the expected proliferation of IP-based devices.

## **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

### *3.1.2 Ensure SCTP is disabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **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
# lsmod | grep sctp
<No output>
```

#### **Remediation:**

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

*Example:*

```
printf "
install sctp /bin/true
" >> /etc/modprobe.d/sctp.conf
```

**CIS Controls:**

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

### *3.1.3 Ensure DCCP is disabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery.

#### **Rationale:**

If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

#### **Audit:**

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

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

#### **Remediation:**

Edit or create a file in the `/etc/modprobe.d/` directory ending in `.conf`

*Example:*

```
printf "
install dccp /bin/true
" >> /etc/modprobe.d/dccp.conf
```

**CIS Controls:**

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

### *3.1.4 Ensure wireless interfaces are disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server

#### **Description:**

Wireless networking is used when wired networks are unavailable.

#### **Rationale:**

If wireless is not to be used, wireless devices should be disabled to reduce the potential attack surface.

#### **Impact:**

Many if not all laptop workstations and some desktop workstations will connect via wireless requiring these interfaces be enabled.

## Audit:

Run the following script to verify no wireless interfaces are active on the system:

```
#!/usr/bin/env bash

{
    if command -v nmcli >/dev/null 2>&1 ; then
        if nmcli radio all | grep -Eq '\s*\S+\s+disabled\s+\S+\s+disabled\b';
then
            echo "Wireless is not enabled"
        else
            nmcli radio all
        fi
    elif [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
        t=0
        mname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f "$driverdir"/device/driver/module)";done | sort -u)
        for dm in $mname; do
            if grep -Eq "^\s*install\s+$dm\s+/bin/(true|false)" /etc/modprobe.d/*.*.conf; then
                /bin/true
            else
                echo "$dm is not disabled"
                t=1
            fi
        done
        [ "$t" -eq 0 ] && echo "Wireless is not enabled"
    else
        echo "Wireless is not enabled"
    fi
}
```

## Remediation:

Run the following script to disable any wireless interfaces:

```
#!/usr/bin/env bash

{
    if command -v nmcli >/dev/null 2>&1 ; then
        nmcli radio all off
    else
        if [ -n "$(find /sys/class/net/*/ -type d -name wireless)" ]; then
            mname=$(for driverdir in $(find /sys/class/net/*/ -type d -name wireless | xargs -0 dirname); do basename "$(readlink -f "$driverdir"/device/driver/module)";done | sort -u)
            for dm in $mname; do
                echo "install $dm /bin/true" >>
/etc/modprobe.d/disable_wireless.conf
            done
        fi
    fi
}
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>15.4 <u>Disable Wireless Access on Devices if Not Required</u></b> Disable wireless access on devices that do not have a business purpose for wireless access.			●
v7	<b>15.5 <u>Limit Wireless Access on Client Devices</u></b> Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.			●

## **3.2 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.

**Note:**

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`

### 3.2.1 Ensure IP forwarding is disabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `net.ipv4.ip_forward` and `net.ipv6.conf.all.forwarding` flags are used to tell the system whether it can forward packets or not.

#### Rationale:

Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

#### Audit:

Run the following script to verify `net.ipv4.ip_forward` is to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.ip_forward"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the running
configuration and in \"$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to \"$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

**IF IPv6 is enabled on the system:**

**Note:** Function to verify IPv6 status on the system is available in the "Network Configuration" section overview

Run the following script to verify net.ipv6.conf.all.forwarding is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv6.conf.all.forwarding"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"\$krp\" != \"\$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## **Remediation:**

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

*Example:*

```
# printf "  
net.ipv4.ip_forward = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv4.ip_forward=0  
    sysctl -w net.ipv4.route.flush=1  
}
```

**IF IPv6 is enabled on the system:**

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

*Example:*

```
# printf "  
net.ipv6.conf.all.forwarding = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

```
# {  
    sysctl -w net.ipv6.conf.all.forwarding=0  
    sysctl -w net.ipv6.route.flush=1  
}
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### 3.2.2 Ensure packet redirect sending is disabled (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### 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 script to verify `net.ipv4.conf.all.send_redirects` is to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.send_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}')
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the running
configuration and in \"$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\"$kpname\" is set to \"$krp\" in
the running configuration\n\""
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify `net.ipv4.conf.default.send_redirects` is to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.default.send_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### **3.3 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.

**Note:**

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the ".conf" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`

### *3.3.1 Ensure source routed packets are not accepted (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 script to verify `net.ipv4.conf.all.accept_source_route` is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.accept_source_route"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify `net.ipv4.conf.default.accept_source_route` is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.default.accept_source_route"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"\$krp\" != \"\$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z \"$pafile\" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

**IF IPv6 is enabled on the system:**

**Note:** Function to verify IPv6 status on the system is available in the "Network Configuration" section overview

Run the following script to verify net.ipv6.conf.all.accept\_source\_route is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pofile="" fafile=""
    kpname="net.ipv6.conf.all.accept_source_route"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pofile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pofile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pofile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\'$kpname\' is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\'$kpname\' is set incorrectly in
\"\$fafile\""
        [ -z "$pofile" ] && echo -e "\'$kpname = \$kpvalue\' is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify `net.ipv4.conf.default.accept_source_route` is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pofile="" fafile=""
    kpname="net.ipv4.conf.default.accept_source_route"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pofile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pofile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pofile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pofile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## **Remediation:**

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

*Example:*

```
# printf "  
net.ipv4.conf.all.accept_source_route = 0  
net.ipv4.conf.default.accept_source_route = 0  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**IF IPv6 is enabled on the system:**

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

*Example:*

```
# printf "  
net.ipv6.conf.all.accept_source_route = 0  
net.ipv6.conf.default.accept_source_route = 0  
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### *3.3.2 Ensure ICMP redirects are not accepted (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 script to verify `net.ipv4.conf.all.accept_redirects` is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.accept_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv4.conf.default.accept\_redirects is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.default.accept_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\'$kpname\' is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\'$kpname\' is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\'$kpname = \$kpvalue\' is not set in a
kernel parameter configuration file\n"
    fi
}
```

**IF IPv6 is enabled on the system:**

**Note:** Function to verify IPv6 status on the system is available in the "Network Configuration" section overview

Run the following script to verify net.ipv6.conf.all.accept\_redirects is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv6.conf.all.accept_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\'$kpname\' is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv6.conf.default.accept\_redirects is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv6.conf.default.accept_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\'$kpname\' is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\'$kpname\' is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\'$kpname = \$kpvalue\' is not set in a
kernel parameter configuration file\n"
    fi
}
```

## **Remediation:**

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

*Example:*

```
# printf "
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**IF IPv6 is enabled on the system:**

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

*Example:*

```
# printf "
net.ipv6.conf.all.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### *3.3.3 Ensure secure ICMP redirects are not accepted (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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` and `net.ipv4.conf.default.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.

## Audit:

Run the following script to verify `net.ipv4.conf.all.secure_redirects` is to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.secure_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}')
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv4.conf.default.secure\_redirects is to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fofile=""
    kpname="net.ipv4.conf.default.secure_redirects"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fofile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fofile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n \"$fofile\" ] && echo -e "\n\"\$kpname\" is set incorrectly in
\"\$fofile\""
        [ -z \"$pafile\" ] && echo -e "\n\"\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.default.secure_redirects = 0
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### 3.3.4 Ensure suspicious packets are logged (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### 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 script to verify `net.ipv4.conf.all.log_martians` is set to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.log_martians"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F= '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the running
configuration and in \"$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to \"$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv4.conf.default.log\_martians is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.default.log_martians"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

### *3.3.5 Ensure broadcast ICMP requests are ignored (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 script to verify `net.ipv4.icmp_echo_ignore_broadcasts` is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.icmp_echo_ignore_broadcasts"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"\$krp\" != \"\$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.icmp_echo_ignore_broadcasts = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### 3.3.6 Ensure bogus ICMP responses are ignored (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### 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 script to verify `net.ipv4.icmp_ignore_bogus_error_responses` is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.icmp_ignore_bogus_error_responses"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?\$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\"$kpname\" is set to \"$kpvalue\" in the running
configuration and in \"$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\"$kpname\" is set to \"$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## **Remediation:**

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

*Example:*

```
# printf "  
net.ipv4.icmp_ignore_bogus_error_responses = 1  
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

### **CIS Controls:**

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

### *3.3.7 Ensure Reverse Path Filtering is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

## Audit:

Run the following script to verify `net.ipv4.conf.all.rp_filter` is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.all.rp_filter"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv4.conf.default.rp\_filter is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.conf.default.rp_filter"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\$kpname\" is set to \"$kpvalue\" in the running
configuration and in \"$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\$kpname\" is set to \"$krp\" in
the running configuration\n"
        [ -n \"$fafile\" ] && echo -e "\n\$kpname\" is set incorrectly in
\"$fafile\""
        [ -z \"$pafile\" ] && echo -e "\n\$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.rp_filter = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following commands to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### *3.3.8 Ensure TCP SYN Cookies is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 script to verify `net.ipv4.tcp_syncookies` is to 1:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv4.tcp_syncookies"
    kpvalue="1"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'"
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:"
        [ "$krp" != "$kpvalue" ] && echo -e "\n\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

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

*Example:*

```
# printf "
net.ipv4.tcp_syncookies = 1
" >> /etc/sysctl.d/60-netipv4_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### *3.3.9 Ensure IPv6 router advertisements are not accepted (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

## Audit:

**IF IPv6 is enabled on the system:**

**Note:** Function to verify IPv6 status on the system is available in the "Network Configuration" section overview

Run the following script to verify `net.ipv6.conf.all.accept_ra` is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv6.conf.all.accept_ra"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)"
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$\"$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL: "
        [ "$krp" != "$kpvalue" ] && echo -e "\\"$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"$kpname = $kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

Run the following script to verify net.ipv6.conf.default.accept\_ra is set to 0:

```
#!/usr/bin/env bash

{
    krp="" pafile="" fafile=""
    kpname="net.ipv6.conf.default.accept_ra"
    kpvalue="0"
    searchloc="/run/sysctl.d/*.conf /etc/sysctl.d/*.conf
/usr/local/lib/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /lib/sysctl.d/*.conf
/etc/sysctl.conf"
    krp=$(sysctl "$kpname" | awk -F= '{print $2}' | xargs)
    pafile=$(grep -Psl -- "^\h*$kpname\h*=\h*$kpvalue\b\h*(#.*)?$$"
$searchloc)"
    fafile=$(grep -s -- "^\s*$kpname" $searchloc | grep -Pv --
"\h*=\h*$kpvalue\b\h*" | awk -F: '{print $1}'")
    if [ "$krp" = "$kpvalue" ] && [ -n "$pafile" ] && [ -z "$fafile" ]; then
        echo -e "\nPASS:\n\$kpname\" is set to \"\$kpvalue\" in the running
configuration and in \"\$pafile\""
    else
        echo -e "\nFAIL:
[ \"$krp\" != \"$kpvalue\" ] && echo -e \"\$kpname\" is set to \"\$krp\" in
the running configuration\n"
        [ -n "$fafile" ] && echo -e "\n\"\$kpname\" is set incorrectly in
\"\$fafile\""
        [ -z "$pafile" ] && echo -e "\n\"\$kpname = \$kpvalue\" is not set in a
kernel parameter configuration file\n"
    fi
}
```

## Remediation:

**IF IPv6 is enabled on the system:**

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

*Example:*

```
# printf "
net.ipv6.conf.all.accept_ra = 0
net.ipv6.conf.default.accept_ra = 0
" >> /etc/sysctl.d/60-netipv6_sysctl.conf
```

Run the following command to set the active kernel parameters:

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

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

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

### **3.4 Firewall Configuration**

A firewall is a set of rules. When a data packet moves into or out of a protected network space, its contents (in particular, information about its origin, target, and the protocol it plans to use) are tested against the firewall rules to see if it should be allowed through.

To provide a Host Based Firewall, the Linux kernel includes support for:

- Netfilter - A set of hooks inside the Linux kernel that allows kernel modules to register callback functions with the network stack. A registered callback function is then called back for every packet that traverses the respective hook within the network stack. Includes the ip\_tables, ip6\_tables, arp\_tables, and ebtables kernel modules. These modules are some of the significant parts of the Netfilter hook system.
- nftables - A subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames. nftables is supposed to replace certain parts of Netfilter, while keeping and reusing most of it. nftables utilizes the building blocks of the Netfilter infrastructure, such as the existing hooks into the networking stack, connection tracking system, userspace queueing component, and logging subsystem. **Is available in Linux kernels 3.13 and newer.**

In order to configure firewall rules for Netfilter or nftables, a firewall utility needs to be installed. Guidance has been included for the following firewall utilities:

- FirewallD - Provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend. Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program. firewalld supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.
- nftables - Includes the nft utility for configuration of the nftables subsystem of the Linux kernel
- iptables - Includes the iptables, ip6tables, arptables and ebtables utilities for configuration Netfilter and the ip\_tables, ip6\_tables, arp\_tables, and ebtables kernel modules.

**Note:**

- *Only one method should be used to configure a firewall on the system. Use of more than one method could produce unexpected results.*
- *This section is intended only to ensure the resulting firewall rules are in place, not how they are configured.*

### **3.4.1 Configure firewalld**

***If nftables or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.***

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options. It also provides an interface for services or applications to add iptables, ip6tables and ebttables rules directly. This interface can also be used by advanced users.

In the v0.6.0 release, firewalld gained support for using nftables as a firewall back-end.

**Note:** Configuration of a live system's firewall directly over a remote connection will often result in being locked out.

### *3.4.1.1 Ensure firewalld is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

firewalld is a firewall management tool for Linux operating systems. It provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the iptables backend or provides firewall features by acting as a front-end for the Linux kernel's netfilter framework via the nftables utility.

firewalld replaces iptables as the default firewall management tool. Use the firewalld utility to configure a firewall for less complex firewalls. The utility is easy to use and covers the typical use cases scenario. FirewallD supports both IPv4 and IPv6 networks and can administer separate firewall zones with varying degrees of trust as defined in zone profiles.

*Note: Starting in v0.6.0, FirewallD added support for acting as a front-end for the Linux kernel's netfilter framework via the nftables userspace utility, acting as an alternative to the nft command line program.*

#### **Rationale:**

A firewall utility is required to configure the Linux kernel's netfilter framework via the iptables or nftables back-end.

The Linux kernel's netfilter framework host-based firewall can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

*Note: Only one firewall utility should be installed and configured. FirewallD is dependent on the iptables package.*

#### **Impact:**

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

## Audit:

Run the following command to verify that `firewalld` and `iptables` are installed:

```
# rpm -q firewalld iptables  
firewalld-<version>  
iptables-<version>
```

## Remediation:

Run the following command to install `FirewallD` and `iptables`:

```
# dnf install firewalld iptables
```

## Additional Information:

### NIST SP 800-53 Rev. 5:

- CA-9

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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 iptables-services not installed with firewalld (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `iptables-services` package contains the `iptables.service` and `ip6tables.service`. These services allow for management of the Host Based Firewall provided by the `iptables` package.

#### **Rationale:**

`iptables.service` and `ip6tables.service` are still supported and can be installed with the `iptables-services` package. Running both firewalld and the services included in the `iptables-services` package may lead to conflict.

#### **Impact:**

Running both firewalld and `iptables/ip6tables` service may lead to conflict.

#### **Audit:**

Run the following commands to verify that the `iptables-services` package is not installed

```
# rpm -q iptables-services  
package iptables-services is not installed
```

#### **Remediation:**

Run the following commands to stop the services included in the `iptables-services` package and remove the `iptables-services` package

```
# systemctl stop iptables  
# systemctl stop ip6tables  
# dnf remove iptables-services
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CA-9
- CM-7

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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 nftables either not installed or masked with firewalld (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

#### **Rationale:**

Running both firewalld and nftables may lead to conflict.

#### **Note:**

- Support for using nftables as the back-end for firewalld was added in release v0.6.0
- firewalld may be configured as the front-end to nftables. If this case, nftables should be stopped and masked instead of removed.

#### **Audit:**

Run the following command to verify that nftables is not installed:

```
# rpm -q nftables
package nftables is not installed
```

*OR*

Run the following commands to verify that nftables is inactive:

```
# systemctl is-active nftables
inactive
```

Run the following command to verify nftables.service is masked:

```
# systemctl is-enabled nftables
masked
```

## **Remediation:**

Run the following command to remove nftables:

```
# dnf remove nftables
```

*OR*

Run the following command to stop and mask nftables"

```
systemctl --now mask nftables
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.1.4 Ensure firewalld service enabled and running (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`firewalld.service` enables the enforcement of firewall rules configured through `firewalld`

#### **Rationale:**

Ensure that the `firewalld.service` is enabled and running to enforce firewall rules configured through `firewalld`

#### **Impact:**

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

#### **Audit:**

Run the following command to verify that `firewalld` is enabled:

```
# systemctl is-enabled firewalld  
enabled
```

Run the following command to verify that `firewalld` is running

```
# firewall-cmd --state  
running
```

#### **Remediation:**

Run the following command to unmask `firewalld`

```
# systemctl unmask firewalld
```

Run the following command to enable and start `firewalld`

```
# systemctl --now enable firewalld
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.1.5 Ensure firewalld default zone is set (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

A firewall zone defines the trust level for a connection, interface or source address binding. This is a one to many relation, which means that a connection, interface or source can only be part of one zone, but a zone can be used for many network connections, interfaces and sources.

- The default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone.
- If no zone assigned to a connection, interface or source, only the default zone is used.
- The default zone is not always listed as being used for an interface or source as it will be used for it either way. This depends on the manager of the interfaces.

Connections handled by NetworkManager are listed as NetworkManager requests to add the zone binding for the interface used by the connection. Also interfaces under control of the network service are listed also because the service requests it.

#### **Note:**

- *A firewalld zone configuration file contains the information for a zone.*
  - *These are the zone description, services, ports, protocols, icmp-blocks, masquerade, forward-ports and rich language rules in an XML file format.*
  - *The file name has to be zone\_name.xml where length of zone\_name is currently limited to 17 chars.*
- *NetworkManager binds interfaces to zones automatically*

#### **Rationale:**

Because the default zone is the zone that is used for everything that is not explicitly bound/assigned to another zone, it is important for the default zone to set

#### **Audit:**

Run the following command and verify that the default zone adheres to company policy:

```
# firewall-cmd --get-default-zone
```

## **Remediation:**

Run the following command to set the default zone:

```
# firewall-cmd --set-default-zone=<NAME_OF_ZONE>
```

*Example:*

```
# firewall-cmd --set-default-zone=public
```

## **References:**

1. <https://firewalld.org/documentation>
2. <https://firewalld.org/documentation/man-pages/firewalld.zone>

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.1.6 Ensure network interfaces are assigned to appropriate zone (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

firewall zones define the trust level of network connections or interfaces.

#### **Rationale:**

A network interface not assigned to the appropriate zone can allow unexpected or undesired network traffic to be accepted on the interface.

#### **Impact:**

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

#### **Audit:**

Run the following and verify that the interface(s) follow site policy for zone assignment

```
# find /sys/class/net/* -maxdepth 1 | awk -F"/" '{print $NF}' | while read -r netint; do [ "$netint" != "lo" ] && firewall-cmd --get-active-zones | grep -B1 $netint; done
```

*Example output:*

```
<custom zone>
  eth0
```

#### **Remediation:**

Run the following command to assign an interface to the appropriate zone.

```
# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>
```

*Example:*

```
# firewall-cmd --zone=customzone --change-interface=eth0
```

**Default Value:**

default zone defined in the firewalld configuration

**References:**

1. <https://firewalld.org/documentation/zone/connections-interfaces-and-sources.html>

**Additional Information:**

The firewall in the Linux kernel is not able to handle network connections with the name shown by NetworkManager, it can only handle the network interfaces used by the connection. Because of this NetworkManager tells firewalld to assign the network interface that is used for this connection to the zone defined in the configuration of that connection. This assignment happens before the interface is used. The configuration of the connection can either be the NetworkManager configuration or also an `ifcfg`.

*Example: If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration. If a connection has more than one interface, all of them will be supplied to firewalld. Also changes in the names of interfaces will be handled by NetworkManager and supplied to firewalld.*

If the zone is not set in the configuration file, the interfaces will be assigned to the default zone defined in the firewalld configuration

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.1.7 Ensure firewalld drops unnecessary services and ports (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Services and ports can be accepted or explicitly rejected or dropped by a zone.

For every zone, you can set a default behavior that handles incoming traffic that is not further specified. Such behavior is defined by setting the target of the zone. There are three options - default, ACCEPT, REJECT, and DROP.

- ACCEPT - you accept all incoming packets except those disabled by a specific rule.
- REJECT - you disable all incoming packets except those that you have allowed in specific rules and the source machine is informed about the rejection.
- DROP - you disable all incoming packets except those that you have allowed in specific rules and no information sent to the source machine.

#### **Rationale:**

To reduce the attack surface of a system, all services and ports should be blocked unless required

## **Audit:**

Run the following command and review output to ensure that listed services and ports follow site policy.

```
# firewall-cmd --get-active-zones | awk '!/:/ {print $1}' | while read ZN; do  
firewall-cmd --list-all --zone=$ZN; done
```

## **Remediation:**

Run the following command to remove an unnecessary service:

```
# firewall-cmd --remove-service=<service>
```

*Example:*

```
# firewall-cmd --remove-service=cockpit
```

Run the following command to remove an unnecessary port:

```
# firewall-cmd --remove-port=<port-number>/<port-type>
```

*Example:*

```
# firewall-cmd --remove-port=25/tcp
```

Run the following command to make new settings persistent:

```
# firewall-cmd --runtime-to-permanent
```

## **References:**

1. firewalld.service(5)
2. [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/8/html/securing\\_networks/using-and-configuring火walls\\_securing-networks](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/securing_networks/using-and-configuring火walls_securing-networks)

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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 nftables**

**If firewalld or iptables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.**

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables. The biggest change with the successor nftables is its simplicity. With iptables, we have to configure every single rule and use the syntax which can be compared with normal commands. With nftables, the simpler syntax, much like BPF (Berkely Packet Filter) means shorter lines and less repetition. Support for nftables should also be compiled into the kernel, together with the related nftables modules. It is available in Linux kernels >= 3.13. **Please ensure that your kernel supports nftables before choosing this option.**

This section broadly assumes starting with an empty nftables firewall ruleset (established by flushing the rules with nft flush ruleset). Remediation steps included only affect the live system, you will also need to configure your default firewall configuration to apply on boot. **Configuration of a live systems firewall directly over a remote connection will often result in being locked out.** It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

**Note:** Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

*The following will implement the firewall rules of this section and open ICMP, IGMP, and port 22(ssh) from anywhere. Opening the ports for ICMP, IGMP, and port 22(ssh) needs to be updated in accordance with local site policy. Allow port 22(ssh) needs to be updated to only allow systems requiring ssh connectivity to connect, as per site policy.*

Save the script below as /etc/nftables/nftables.rules

```

#!/sbin/nft -f

# This nftables.rules config should be saved as /etc/nftables/nftables.rules

# flush nftables ruleset
flush ruleset

# Load nftables ruleset

# nftables config with inet table named filter

table inet filter {
    # Base chain for input hook named input (Filters inbound network packets)
    chain input {
        type filter hook input priority 0; policy drop;

        # Ensure loopback traffic is configured
        iif "lo" accept
        ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
        ip6 saddr ::1 counter packets 0 bytes 0 drop

        # Ensure established connections are configured
        ip protocol tcp ct state established accept
        ip protocol udp ct state established accept
        ip protocol icmp ct state established accept

        # Accept port 22(SSH) traffic from anywhere
        tcp dport ssh accept

        # Accept ICMP and IGMP from anywhere
        icmpv6 type { destination-unreachable, packet-too-big, time-exceeded,
parameter-problem, mld-listener-query, mld-listener-report, mld-listener-done, nd-
router-solicit, nd-router-advert, nd-neighbor-solicit, nd-neighbor-advert, ind-
neighbor-solicit, ind-neighbor-advert, mld2-listener-report } accept
        icmp type { destination-unreachable, router-advertisement, router-
solicitation, time-exceeded, parameter-problem } accept
        ip protocol igmp accept
    }

    # Base chain for hook forward named forward (Filters forwarded network
packets)
    chain forward {
        type filter hook forward priority 0; policy drop;
    }

    # Base chain for hook output named output (Filters outbound network packets)
    chain output {
        type filter hook output priority 0; policy drop;
        # Ensure outbound and established connections are configured
        ip protocol tcp ct state established,related,new accept
        ip protocol udp ct state established,related,new accept
        ip protocol icmp ct state established,related,new accept
    }
}

```

Run the following command to load the file into nftables

```
# nft -f /etc/nftables/nftables.rules
```

*All changes in the nftables subsections are temporary*

To make these changes permanent:

Run the following command to create the nftables.rules file

```
nft list ruleset > /etc/nftables/nftables.rules
```

Add the following line to /etc/sysconfig/nftables.conf

```
include "/etc/nftables/nftables.rules"
```

### **3.4.2.1 Ensure nftables is installed (Automated)**

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

nftables provides a new in-kernel packet classification framework that is based on a network-specific Virtual Machine (VM) and a new nft userspace command line tool. nftables reuses the existing Netfilter subsystems such as the existing hook infrastructure, the connection tracking system, NAT, userspace queuing and logging subsystem.

#### **Note:**

- *nftables is available in Linux kernel 3.13 and newer.*
- *Only one firewall utility should be installed and configured.*

#### **Rationale:**

nftables is a subsystem of the Linux kernel that can protect against threats originating from within a corporate network to include malicious mobile code and poorly configured software on a host.

#### **Impact:**

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

#### **Audit:**

Run the following command to verify that nftables is installed:

```
# rpm -q nftables  
nftables-<version>
```

#### **Remediation:**

Run the following command to install nftables

```
# dnf install nftables
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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 firewalld is either not installed or masked with nftables (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

#### **Rationale:**

Running both `nftables.service` and `firewalld.service` may lead to conflict and unexpected results.

#### **Audit:**

Run the following command to verify that `firewalld` is not installed:

```
# rpm -q firewalld  
package firewalld is not installed
```

*OR*

Run the following command to verify that FirewallD is not running

```
command -v firewall-cmd >/dev/null && firewall-cmd --state | grep 'running'  
not running
```

Run the following command to verify that FirewallD is masked

```
# systemctl is-enabled firewalld  
masked
```

## **Remediation:**

Run the following command to remove firewalld

```
# dnf remove firewalld
```

*OR*

Run the following command to stop and mask firewalld

```
# systemctl --now mask firewalld
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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 iptables-services not installed with nftables (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `iptables-services` package contains the `iptables.service` and `ip6tables.service`. These services allow for management of the Host Based Firewall provided by the `iptables` package.

#### **Rationale:**

`iptables.service` and `ip6tables.service` are still supported and can be installed with the `iptables-services` package. Running both nftables and the services included in the `iptables-services` package may lead to conflict.

#### **Audit:**

Run the following commands to verify that the `iptables-services` package is not installed

```
# rpm -q iptables-services  
package iptables-services is not installed
```

#### **Remediation:**

Run the following commands to stop the services included in the `iptables-services` package and remove the `iptables-services` package

```
# systemctl stop iptables  
# systemctl stop ip6tables  
  
# dnf remove iptables-services
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9
- CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</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.</p>			
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</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.</p>			

### *3.4.2.4 Ensure iptables are flushed with nftables (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

nftables is a replacement for iptables, ip6tables, ebtables and arptables

#### **Rationale:**

It is possible to mix iptables and nftables. However, this increases complexity and also the chance to introduce errors. For simplicity flush out all iptables rules, and ensure it is not loaded

#### **Audit:**

Run the following commands to ensure not iptables rules exist

For iptables:

```
# iptables -L  
No rules should be returned
```

For ip6tables:

```
# ip6tables -L  
No rules should be returned
```

#### **Remediation:**

Run the following commands to flush iptables:

For iptables:

```
# iptables -F
```

For ip6tables:

```
# ip6tables -F
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.5 Ensure an nftables table exists (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Tables hold chains. Each table only has one address family and only applies to packets of this family. Tables can have one of five families.

#### **Rationale:**

nftables doesn't have any default tables. Without a table being build, nftables will not filter network traffic.

#### **Impact:**

Adding rules to a running nftables can cause loss of connectivity to the system

#### **Audit:**

Run the following command to verify that a nftables table exists:

```
# nft list tables
```

Return should include a list of nftables:

*Example:*

```
table inet filter
```

#### **Remediation:**

Run the following command to create a table in nftables

```
# nft create table inet <table name>
```

*Example:*

```
# nft create table inet filter
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.6 Ensure nftables base chains exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Chains are containers for rules. They exist in two kinds, base chains and regular chains. A base chain is an entry point for packets from the networking stack, a regular chain may be used as jump target and is used for better rule organization.

#### **Rationale:**

If a base chain doesn't exist with a hook for input, forward, and delete, packets that would flow through those chains will not be touched by nftables.

#### **Impact:**

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

#### **Audit:**

Run the following commands and verify that base chains exist for INPUT, FORWARD, and OUTPUT.

```
# nft list ruleset | grep 'hook input'  
type filter hook input priority 0;  
  
# nft list ruleset | grep 'hook forward'  
type filter hook forward priority 0;  
  
# nft list ruleset | grep 'hook output'  
type filter hook output priority 0;
```

## **Remediation:**

Run the following command to create the base chains:

```
# nft create chain inet <table name> <base chain name> { type filter hook <(input|forward|output)> priority 0 \; }
```

*Example:*

```
# nft create chain inet filter input { type filter hook input priority 0 \; }
# nft create chain inet filter forward { type filter hook forward priority 0
\; }
# nft create chain inet filter output { type filter hook output priority 0 \;
}
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.7 Ensure nftables loopback traffic is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network

#### **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 traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

## Audit:

Run the following commands to verify that the loopback interface is configured:

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'iif "lo" accept'  
iif "lo" accept  
  
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip saddr'  
ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
```

**IF IPv6 is enabled, run the following command to verify that the IPv6 loopback interface is configured:**

```
# nft list ruleset | awk '/hook input/,/}/' | grep 'ip6 saddr'  
ip6 saddr ::1 counter packets 0 bytes 0 drop
```

*OR*

*Verify that IPv6 is disabled:*

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/env bash  
  
ipv6_chk()  
{  
    passing=""  
    grubfile=$(find /boot -type f \(\ -name 'grubenv' -o -name 'grub.conf' -o  
-name 'grub.cfg' \) \  
    -exec grep -P -- '^\\h*(kernelopts=|linux|kernel)' {} \;)"  
    ! grep -P -- "^\\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --  
    ipv6.disable=1 && passing="true"  
    grep -Pq -- "^\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$" \  
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
    /run/sysctl.d/*.conf && \  
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$" \  
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf  
    /run/sysctl.d/*.conf && \  
    sysctl net.ipv6.conf.all.disable_ipv6 | \  
    grep -Pq -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$" &&  
    sysctl net.ipv6.conf.default.disable_ipv6 | \  
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$" &&  
    passing="true"  
    if [ "$passing" = true ] ; then  
        echo -e "\nIPv6 is disabled on the system\n"  
    else  
        echo -e "\nIPv6 is enabled on the system\n"  
    fi  
}  
ipv6_chk
```

## **Remediation:**

Run the following commands to implement the loopback rules:

```
# nft add rule inet filter input iif lo accept  
# nft create rule inet filter input ip saddr 127.0.0.0/8 counter drop
```

*IF IPv6 is enabled:*

Run the following command to implement the IPv6 loopback rules:

```
# nft add rule inet filter input ip6 saddr ::1 counter drop
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

### **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.8 Ensure nftables outbound and established connections are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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 commands and verify all rules for established incoming connections match site policy: site policy:

```
# nft list ruleset | awk '/hook input/,/}/' | grep -E 'ip protocol  
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established accept  
ip protocol udp ct state established accept  
ip protocol icmp ct state established accept
```

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

```
# nft list ruleset | awk '/hook output/,/}/' | grep -E 'ip protocol  
(tcp|udp|icmp) ct state'
```

Output should be similar to:

```
ip protocol tcp ct state established,related,new accept  
ip protocol udp ct state established,related,new accept  
ip protocol icmp ct state established,related,new accept
```

## **Remediation:**

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

```
# nft add rule inet filter input ip protocol tcp ct state established accept
# nft add rule inet filter input ip protocol udp ct state established accept
# nft add rule inet filter input ip protocol icmp ct state established accept
# nft add rule inet filter output ip protocol tcp ct state
new,related,established accept
# nft add rule inet filter output ip protocol udp ct state
new,related,established accept
# nft add rule inet filter output ip protocol icmp ct state
new,related,established accept
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.9 Ensure nftables default deny firewall policy (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Base chain policy is the default verdict that will be applied to packets reaching the end of the chain.

#### **Rationale:**

There are two policies: accept (Default) and drop. If the policy is set to accept, the firewall will accept any packet that is not configured to be denied and the packet will continue traversing the network stack.

It is easier to white list acceptable usage than to black list unacceptable usage.

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

#### **Impact:**

If configuring nftables over ssh, creating a base chain with a policy of drop will cause loss of connectivity.

Ensure that a rule allowing ssh has been added to the base chain prior to setting the base chain's policy to drop

#### **Audit:**

Run the following commands and verify that base chains contain a policy of DROP.

```
# nft list ruleset | grep 'hook input'  
  
type filter hook input priority 0; policy drop;  
  
# nft list ruleset | grep 'hook forward'  
  
type filter hook forward priority 0; policy drop;  
  
# nft list ruleset | grep 'hook output'  
  
type filter hook output priority 0; policy drop;
```

## **Remediation:**

Run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

```
# nft chain <table family> <table name> <chain name> { policy drop \; }
```

*Example:*

```
# nft chain inet filter input { policy drop \; }
# nft chain inet filter forward { policy drop \; }
# nft chain inet filter output { policy drop \; }
```

## **Default Value:**

accept

## **References:**

1. Manual Page nft

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.2.10 Ensure nftables service is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The nftables service allows for the loading of nftables rulesets during boot, or starting on the nftables service

#### **Rationale:**

The nftables service restores the nftables rules from the rules files referenced in the /etc/sysconfig/nftables.conf file during boot or the starting of the nftables service

#### **Audit:**

Run the following command and verify that the nftables service is enabled:

```
# systemctl is-enabled nftables  
enabled
```

#### **Remediation:**

Run the following command to enable the nftables service:

```
# systemctl enable nftables
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</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.</p>			
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</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.</p>			

### *3.4.2.11 Ensure nftables rules are permanent (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames.

The nftables service reads the `/etc/sysconfig/nftables.conf` file for a nftables file or files to include in the nftables ruleset.

A nftables ruleset containing the input, forward, and output base chains allow network traffic to be filtered.

#### **Rationale:**

Changes made to nftables ruleset only affect the live system, you will also need to configure the nftables ruleset to apply on boot

## Audit:

Run the following commands to verify that input, forward, and output base chains are configured to be applied to a nftables ruleset on boot:

Run the following command to verify the input base chain:

```
# awk '/hook input/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\\"","\"",\$2);print \$2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
        type filter hook input priority 0; policy drop;

        # Ensure loopback traffic is configured
        iif "lo" accept
        ip saddr 127.0.0.0/8 counter packets 0 bytes 0 drop
        ip6 saddr ::1 counter packets 0 bytes 0 drop

        # Ensure established connections are configured
        ip protocol tcp ct state established accept
        ip protocol udp ct state established accept
        ip protocol icmp ct state established accept

        # Accept port 22(SSH) traffic from anywhere
        tcp dport ssh accept

        # Accept ICMP and IGMP from anywhere
        icmpv6 type { destination-unreachable, packet-too-big, time-
exceeded, parameter-problem, mld-listener-query, mld-listener-report, mld-
listener-done, nd-router-solicit, nd-router-advert, nd-neighbor-solicit, nd-
neighbor-advert, ind-neighbor-solicit, ind-neighbor-advert, mld2-listener-
report } accept
```

*Note: Review the input base chain to ensure that it follows local site policy*

Run the following command to verify the forward base chain:

```
# awk '/hook forward/,/}/' $(awk '$1 ~ /^s*include/ { gsub("\\"","\"",\$2);print \$2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
        # Base chain for hook forward named forward (Filters forwarded
network packets)
        chain forward {
            type filter hook forward priority 0; policy drop;
        }
```

*Note: Review the forward base chain to ensure that it follows local site policy.*

Run the following command to verify the forward base chain:

```
# awk '/hook output/,/}/' $(awk '$1 ~ /^\\s*include/ { gsub("\\\"", "", $2); print $2 }' /etc/sysconfig/nftables.conf)
```

Output should be similar to:

```
# Base chain for hook output named output (Filters outbound network
packets)
chain output {
    type filter hook output priority 0; policy drop;
    # Ensure outbound and established connections are configured
    ip protocol tcp ct state established,related,new accept
    ip protocol tcp ct state established,related,new accept
    ip protocol udp ct state established,related,new accept
    ip protocol icmp ct state established,related,new accept
}
```

*Note: Review the output base chain to ensure that it follows local site policy.*

### Remediation:

Edit the `/etc/sysconfig/nftables.conf` file and un-comment or add a line with `include <Absolute path to nftables rules file>` for each nftables file you want included in the nftables ruleset on boot:

*Example:*

```
include "/etc/nftables/nftables.rules"
```

### Additional Information:

#### NIST SP 800-53 Rev. 5:

- CA-9

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</b></p> <p>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>			
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</b></p> <p>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.</p>			

### **3.4.3 Configure iptables**

***If firewalld or nftables are being used in your environment, please follow the guidance in their respective section and pass-over the guidance in this section.***

IPtables is an application that allows a system administrator to configure the IPv4 and 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 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.

**Note:** Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

### ***3.4.3.1 Configure iptables software***

This section provides guidance for installing, enabling, removing, and disabling software packages necessary for using IPTables as the method for configuring and maintaining a Host Based Firewall on the system.

**Note:** Using more than one method to configure and maintain a Host Based Firewall can cause unexpected results. If FirewallD or NFTables are being used for configuration and maintenance, this section should be skipped and the guidance in their respective section followed.

### *3.4.3.1.1 Ensure iptables packages are installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

iptables is a utility program that allows a system administrator to configure the tables provided by the Linux kernel firewall, implemented as different Netfilter modules, and the chains and rules it stores. Different kernel modules and programs are used for different protocols; iptables applies to IPv4, ip6tables to IPv6, arptables to ARP, and ebtables to Ethernet frames.

#### **Rationale:**

A method of configuring and maintaining firewall rules is necessary to configure a Host Based Firewall.

#### **Audit:**

Run the following command to verify that `iptables` and `iptables-services` are installed:

```
rpm -q iptables iptables-services  
iptables-<version>  
iptables-services-<version>
```

#### **Remediation:**

Run the following command to install `iptables` and `iptables-services`

```
# dnf install iptables iptables-services
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.1.2 Ensure nftables is not installed with iptables (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

nftables is a subsystem of the Linux kernel providing filtering and classification of network packets/datagrams/frames and is the successor to iptables.

#### **Rationale:**

Running both `iptables` and `nftables` may lead to conflict.

#### **Audit:**

Run the following command to verify that nftables is not installed:

```
# rpm -q nftables  
package nftables is not installed
```

#### **Remediation:**

Run the following command to remove `nftables`:

```
# dnf remove nftables
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9
- CM-7

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</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.</p>			
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b>            Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>			
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</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.</p>			

### *3.4.3.1.3 Ensure firewalld is either not installed or masked with iptables (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

firewalld (Dynamic Firewall Manager) provides a dynamically managed firewall with support for network/firewall “zones” to assign a level of trust to a network and its associated connections, interfaces or sources. It has support for IPv4, IPv6, Ethernet bridges and also for IPSet firewall settings. There is a separation of the runtime and permanent configuration options.

#### **Rationale:**

Running `iptables.service` and\or `ip6tables.service` with `firewalld.service` may lead to conflict and unexpected results.

#### **Audit:**

Run the following command to verify that `firewalld` is not installed:

```
# rpm -q firewalld  
package firewalld is not installed
```

*OR*

Run the following commands to verify that `firewalld` is stopped and masked

```
# systemctl status firewalld | grep "Active: " | grep -v "active (running)"  
No output should be returned  
  
# systemctl is-enabled firewalld  
masked
```

## **Remediation:**

Run the following command to remove firewalld

```
# yum remove firewalld
```

*OR*

Run the following command to stop and mask firewalld

```
# systemctl --now mask firewalld
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### 3.4.3.2 Configure IPv4 iptables

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

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

**Note:**

- This section broadly assumes starting with an empty IPTables firewall ruleset (established by flushing the rules with `iptables -F`).
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out.
- It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. *This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.*

```
#!/bin/bash

# Flush IPTables rules
iptables -F

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

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

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

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

### 3.4.3.2.1 Ensure iptables loopback traffic is configured (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### 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.

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

#### 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:****NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.2.2 Ensure iptables outbound and established connections are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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.

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

#### **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
```

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.2.3 Ensure iptables rules exist for all open ports (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Note:**

- Changing firewall settings while connected over network can result in being locked out of the system.
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

## Audit:

Run the following command to determine open ports:

```
# ss -4tuln
```

Netid State Address:Port	Recv-Q	Send-Q	Local Address:Port	Peer
udp UNCONN *:*	0	0	*	:68
udp UNCONN *:*	0	0	*	:123
tcp LISTEN *:*	0	128	*	:22

Run the following command to determine firewall rules:

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

Chain	policy	pkts	bytes	target	prot	opt	in	out	source	destination
INPUT	DROP	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
		0	0	ACCEPT	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0
				tcp dpt:22 state NEW						

Verify all open ports listening on non-localhost addresses have at least one firewall rule.

*Note: The last line identified by the "tcp dpt:22 state NEW" identifies it as a firewall rule for new connections on tcp port 22.*

## Remediation:

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

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

## Additional Information:

### NIST SP 800-53 Rev. 5:

- CA-9

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 Implement and Manage a Firewall on Servers</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.</p>	●	●	●
v7	<p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b>            Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●
v7	<p><b>9.4 Apply Host-based Firewalls or Port Filtering</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.</p>	●	●	●

### *3.4.3.2.4 Ensure iptables default deny firewall policy (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

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

#### **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:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.2.5 Ensure iptables rules are saved (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `iptables-services` package includes the `/etc/sysconfig/iptables` file. The `iptables` rules in this file will be loaded by the `iptables.service` during boot, or when it is started or re-loaded.

#### **Rationale:**

If the `iptables` rules are not saved and a system re-boot occurs, the `iptables` rules will be lost.

#### **Audit:**

Review the file `/etc/sysconfig/iptables` and ensure it contains the complete correct rule-set.

*Example:* `/etc/sysconfig/iptables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [4:463]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s 127.0.0.0/8 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:23:37 2020
```

## **Remediation:**

Run the following commands to create or update the /etc/sysconfig/iptables file:

Run the following command to review the current running iptables configuration:

```
# iptables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT    all  --  anywhere
DROP      all  --  loopback/8
ACCEPT    tcp  --  anywhere        anywhere
ESTABLISHED
ACCEPT    udp  --  anywhere        anywhere
ESTABLISHED
ACCEPT    icmp --  anywhere        anywhere
ESTABLISHED
ACCEPT    tcp  --  anywhere        anywhere
state NEW

Chain FORWARD (policy DROP)
target     prot opt source          destination

Chain OUTPUT (policy DROP)
target     prot opt source          destination
ACCEPT    all  --  anywhere
ACCEPT    tcp  --  anywhere        anywhere
state NEW,ESTABLISHED
ACCEPT    udp  --  anywhere        anywhere
state NEW,ESTABLISHED
ACCEPT    icmp --  anywhere        anywhere
state NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file /etc/sysconfig/iptables:

```
# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.2.6 Ensure iptables is enabled and active (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`iptables.service` is a utility for configuring and maintaining `iptables`.

#### **Rationale:**

`iptables.service` will load the `iptables` rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the `iptables` rules will be cleared during a re-boot of the system.

#### **Audit:**

Run the following commands to verify `iptables` is enabled:

```
# systemctl is-enabled iptables  
enabled
```

Run the following command to verify `iptables.service` is active:

```
# systemctl is-active iptables  
active
```

#### **Remediation:**

Run the following command to enable and start `iptables`:

```
# systemctl --now enable iptables
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### 3.4.3.3 Configure IPv6 ip6tables

**If IPv6 is not enabled on the system, this section can be skipped.**

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).
- Configuration of a live systems firewall directly over a remote connection will often result in being locked out. It is advised to have a known good firewall configuration set to run on boot and to configure an entire firewall structure in a script that is then run and tested before saving to boot.

*The following script will implement the firewall rules of this section and open port 22(ssh) from anywhere. This needs to be updated to only allow systems requiring ssh connectivity to connect as per site policy.*

```
#!/bin/bash

# Flush ip6tables rules
ip6tables -F

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

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

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

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

### *3.4.3.3.1 Ensure ip6tables loopback traffic is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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.

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

## 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      ::/0

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

**OR** verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(-name 'grubenv' -o -name 'grub.conf' -o
-name 'grub.cfg'\) \
-exec grep -P1 -- '^\\h*(kernelopts=|linux|kernel)' {} \;)
    ! grep -P -- "^\\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "^\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?\$" \
/etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?\$" \
\
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?\$" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?\$" &&
    passing="true"
    if [ "\$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

## **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
```

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.3.2 Ensure ip6tables outbound and established connections are configured (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **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.

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

## Audit:

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

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

## OR verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(
        -name 'grubenv' -o
        -name 'grub.conf' -o
        -name 'grub.cfg' \
    \)
    -exec grep -Pl -- '^h*(kernelopts=|linux|kernel)' {} \;)"
    ! grep -P -- "^\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "^\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\h*.all\.disable_ipv6\h*=\h*1\h*(#.*)?$$" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\h*.default\.disable_ipv6\h*=\h*1\h*(#.*)?$$" &&
    passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

## 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
```

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.3.3 Ensure ip6tables firewall rules exist for all open ports (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Note:**

- Changing firewall settings while connected over network can result in being locked out of the system.
- The remediation command opens up the port to traffic from all sources. Consult iptables documentation and set any restrictions in compliance with site policy.

#### **Audit:**

Run the following command to determine open ports:

```
# ss -6tuln

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

Run the following command to determine firewall rules:

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

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

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

**OR** verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```
#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(
        -name 'grubenv' -o
        -name 'grub.conf' -o
        -name 'grub.cfg' \) \
        -exec grep -P1 -- '^\\h*(kernelopts=|linux|kernel)' {} \;)
    ! grep -P -- "^\\h*(kernelopts=|linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "^\s*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$" \
    /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\.all\.disable_ipv6\h*=\h*1\h*(#.*)?$" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "^\h*net\.ipv6\.conf\.default\.disable_ipv6\h*=\h*1\h*(#.*)?$" &&
    passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk
```

## **Remediation:**

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

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

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.3.4 Ensure ip6tables default deny firewall policy (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

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

#### **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)
```

#### **OR Verify IPv6 is disabled:**

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(
        -name 'grubenv' -o
        -name 'grub.conf' -o
        -name 'grub.cfg' \) \
        -exec grep -Pl -- '^h*(kernelopts=linux|kernel)' {} \;)
    ! grep -P -- "^\h*(kernelopts=linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "\s*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)? $" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)? $" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)? $" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)? $" &&
    passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk

```

## **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:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### 3.4.3.3.5 Ensure ip6tables rules are saved (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `iptables-services` package includes the `/etc/sysconfig/ip6tables` file. The `ip6tables` rules in this file will be loaded by the `ip6tables.service` during boot, or when it is started or re-loaded.

#### Rationale:

If the `ip6tables` rules are not saved and a system re-boot occurs, the `ip6tables` rules will be lost.

#### Audit:

Review the file `/etc/sysconfig/ip6tables` and ensure it contains the complete correct rule-set.

*Example:* `/etc/sysconfig/ip6tables`

```
# sample configuration for iptables service
# you can edit this manually or use system-config-firewall
# Generated by iptables-save v1.4.21 on Wed Mar 25 14:23:37 2020
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -s ::1/128 -j DROP
-A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p udp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p icmp -m state --state ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m state --state NEW -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
-A OUTPUT -p icmp -m state --state NEW,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Wed Mar 25 14:58:32 2020
```

**OR** Verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(
        -name 'grubenv' -o
        -name 'grub.conf' -o
        -name 'grub.cfg' \) \
        -exec grep -Pl -- '^h*(kernelopts=linux|kernel)' {} \;)
    ! grep -P -- "^\h*(kernelopts=linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "\s*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)? $" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)? $" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)? $" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)? $" &&
    passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk

```

## **Remediation:**

Run the following commands to create or update the /etc/sysconfig/ip6tables file:

Run the following command to review the current running iptables configuration:

```
# ip6tables -L
```

Output should include:

```
Chain INPUT (policy DROP)
target    prot opt source          destination
ACCEPT    all   anywhere          anywhere
DROP      all   localhost         anywhere
ACCEPT    tcp   anywhere          anywhere          state
ESTABLISHED
ACCEPT    udp   anywhere          anywhere          state
ESTABLISHED
ACCEPT    icmp  anywhere          anywhere          state
ESTABLISHED
ACCEPT    tcp   anywhere          anywhere          tcp dpt:ssh
state NEW

Chain FORWARD (policy DROP)
target    prot opt source          destination

Chain OUTPUT (policy DROP)
target    prot opt source          destination
ACCEPT    all   anywhere          anywhere
ACCEPT    tcp   anywhere          anywhere          state
NEW,ESTABLISHED
ACCEPT    udp   anywhere          anywhere          state
NEW,ESTABLISHED
ACCEPT    icmp  anywhere          anywhere          state
NEW,ESTABLISHED
```

Run the following command to save the verified running configuration to the file /etc/sysconfig/ip6tables:

```
# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[ OK ]
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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.	●	●	●

### *3.4.3.3.6 Ensure ip6tables is enabled and active (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`ip6tables.service` is a utility for configuring and maintaining `ip6tables`.

#### **Rationale:**

`ip6tables.service` will load the `iptables` rules saved in the file `/etc/sysconfig/iptables` at boot, otherwise the `ip6tables` rules will be cleared during a re-boot of the system.

#### **Audit:**

Run the following commands to verify `ip6tables` is enabled:

```
# systemctl is-enabled ip6tables  
enabled
```

Run the following command to verify `ip6tables.service` is active

```
# systemctl is-active ip6tables  
active
```

**OR** verify IPv6 is disabled:

Run the following script. Output will confirm if IPv6 is disabled on the system.

```

#!/usr/bin/env bash

ipv6_chk()
{
    passing=""
    grubfile=$(find /boot -type f \(
        -name 'grubenv' -o
        -name 'grub.conf' -o
        -name 'grub.cfg' \) \
        -exec grep -Pl -- '^h*(kernelopts=linux|kernel)' {} \;)
    ! grep -P -- "^\h*(kernelopts=linux|kernel)" "$grubfile" | grep -vq --
    ipv6.disable=1 && passing="true"
    grep -Pq -- "\s*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)?\$" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)?\$" \
        /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf && \
    sysctl net.ipv6.conf.all.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.all\.disable_ipv6=h*=h*1\h*(#.*)?\$" &&
    sysctl net.ipv6.conf.default.disable_ipv6 | \
    grep -Pq -- "\h*net\.ipv6\.conf\.default\.disable_ipv6=h*=h*1\h*(#.*)?\$" &&
    passing="true"
    if [ "$passing" = true ] ; then
        echo -e "\nIPv6 is disabled on the system\n"
    else
        echo -e "\nIPv6 is enabled on the system\n"
    fi
}
ipv6_chk

```

## **Remediation:**

Run the following command to enable and start ip6tables:

```
# systemctl --now start ip6tables
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CA-9

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</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.	●	●	●
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</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, log monitoring, and auditing, using tools included in most distributions.

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

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

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

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

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

## **4.1 Configure System Accounting (auditd)**

The Linux Auditing System operates on a set of rules that collects certain types of system activity to facilitate incident investigation, detect unauthorized access or modification of data. By default events will be logged to `/var/log/audit/audit.log`, which can be configured in `/etc/audit/auditd.conf`.

The following types of audit rules can be specified:

- Control rules: Configuration of the auditing system.
- File system rules: Allow the auditing of access to a particular file or a directory. Also known as file watches.
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- On the command line using the `auditctl` utility. These rules are not persistent across reboots.
- In `/etc/audit/audit.rules`. These rules have to be merged and loaded before they are active.

### **Notes:**

- For 64 bit systems that have `arch` as a rule parameter, you will need two rules: one for 64 bit and one for 32 bit systems calls. For 32 bit systems, only one rule is needed.
- If the auditing system is configured to be locked (`-e 2`), a system reboot will be required in order to load any changes.
- Key names are optional on the rules and will not be used as a compliance auditing. The usage of key names is highly recommended as it facilitates organization and searching, as such, all remediation steps will have key names supplied.
- It is best practice to store the rules, in number prepended files, in `/etc/audit/rules.d/`. Rules must end in a `.rules` suffix. This then requires the use of `augenrules` to merge all the rules into `/etc/audit/audit.rules` based on their alphabetical (lexical) sort order. All benchmark recommendations follow this best practice for remediation, specifically using the prefix of `50` which is center weighed if all rule sets make use of the number prepending naming convention.
- Your system may have been customized to change the default `UID_MIN`. All samples output uses `1000`, but this value will not be used in compliance auditing. To confirm the `UID_MIN` for your system, run the following command: `awk '/^s*UID_MIN/{print $2}' /etc/login.defs`

## Normalization

The Audit system normalizes some entries, so when you look at the sample output keep in mind that:

- With regards to users whose login UID is not set, the values `-1` / `unset` / `4294967295` are equivalent and normalized to `-1`.
- When comparing field types and both sides of the comparison is valid fields types, such as `euid!=uid`, then the auditing system may normalize such that the output is `uid!=euid`.
- Some parts of the rule may be rearranged whilst others are dependent on previous syntax. For example, the following two statements are the same:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid!=-1 -F  
key=user_emulation
```

and

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k  
user_emulation
```

## Capacity planning

The recommendations in this section implement auditing policies that not only produces large quantities of logged data, but may also negatively impact system performance.

Capacity planning is critical in order not to adversely impact production environments.

- Disk space. If a significantly large set of events are captured, additional on system or off system storage may need to be allocated. If the logs are not sent to a remote log server, ensure that log rotation is implemented else the disk will fill up and the system will halt. Even when logs are sent to a log server, ensure sufficient disk space to allow caching of logs in the case of temporary network outages.
- Disk IO. It is not just the amount of data collected that should be considered, but the rate at which logs are generated.
- CPU overhead. System call rules might incur considerable CPU overhead. Test the systems open/close syscalls per second with and without the rules to gauge the impact of the rules.

#### ***4.1.1 Ensure auditing is enabled***

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

#### *4.1.1.1 Ensure auditd is installed (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk

##### **Rationale:**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

##### **Audit:**

Run the following command and verify auditd is installed:

```
# rpm -q audit
```

##### **Remediation:**

Run the following command to Install auditd

```
# dnf install audit
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-3
- AU-3(1)
- AU-12
- SI-5

## CIS Controls:

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

#### *4.1.1.2 Ensure auditd service is enabled (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Turn on the `auditd` daemon to record system events.

##### **Rationale:**

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

##### **Audit:**

Run the following command to verify `auditd` is enabled:

```
# systemctl is-enabled auditd  
enabled
```

Verify result is "enabled".

##### **Remediation:**

Run the following command to enable `auditd`:

```
# systemctl --now enable auditd
```

##### **Additional Information:**

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

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.1.1.3 Ensure auditing for processes that start prior to auditd is enabled (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Configure grub2 so that processes that are capable of being audited can be audited even if they start up prior to auditd startup.

##### **Rationale:**

Audit events need to be captured on processes that start up prior to auditd, so that potential malicious activity cannot go undetected.

##### **Audit:**

Run the following command:

```
# find /boot -type f -name 'grubenv' -exec grep -P  
'kernelopts=([^\n\r]+\h+)?(audit=1)' {} \;
```

Output will include audit=1

##### **Remediation:**

Run the following command to add audit=1 to GRUB\_CMDLINE\_LINUX:

```
# grubby --update-kernel ALL --args 'audit=1'
```

##### **Additional Information:**

This recommendation is designed around the grub2 bootloader, if another bootloader is in use in your environment enact equivalent settings.

**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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### *4.1.1.4 Ensure audit\_backlog\_limit is sufficient (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The backlog limit has a default setting of 64

##### **Rationale:**

During boot if `audit=1`, then the backlog will hold 64 records. If more than 64 records are created during boot, auditd records will be lost and potential malicious activity could go undetected.

##### **Audit:**

Run the following command and verify the `audit_backlog_limit=` parameter is set to an appropriate size for your organization

```
# find /boot -type f -name 'grubenv' -exec grep -P  
'kernelopts=([^\#\n\r]+\h+)?(audit_backlog_limit=\S+\b)' {} \;
```

Validate that the line(s) returned contain a value for `audit_backlog_limit=` and the value is sufficient for your organization.

**Recommended that this value be 8192 or larger.**

##### **Remediation:**

Run the following command to add `audit_backlog_limit=<BACKLOG SIZE>` to GRUB\_CMDLINE\_LINUX:

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=<BACKLOG SIZE>'
```

*Example:*

```
# grubby --update-kernel ALL --args 'audit_backlog_limit=8192'
```

**Additional Information:**

**NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

**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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### ***4.1.2 Configure Data Retention***

When auditing, it is important to carefully configure the storage requirements for audit logs. By default, auditd will max out the log files at 5MB and retain only 4 copies of them. Older versions will be deleted. It is possible on a system that the 20 MBs of audit logs may fill up the system causing loss of audit data. While the recommendations here provide guidance, check your site policy for audit storage requirements.

#### *4.1.2.1 Ensure audit log storage size is configured (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.

##### **Rationale:**

It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.

##### **Audit:**

Run the following command and ensure output is in compliance with site policy:

```
# grep -w "\s*max_log_file\s*=" /etc/audit/auditd.conf  
max_log_file = <MB>
```

##### **Remediation:**

Set the following parameter in `/etc/audit/auditd.conf` in accordance with site policy:

```
max_log_file = <MB>
```

##### **Additional Information:**

The `max_log_file` parameter is measured in megabytes.

Other methods of log rotation may be appropriate based on site policy. One example is time-based rotation strategies which don't have native support in auditd configurations. Manual audit of custom configurations should be evaluated for effectiveness and completeness.

##### **NIST SP 800-53 Rev. 5:**

- AU-8

**CIS Controls:**

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

#### *4.1.2.2 Ensure audit logs are not automatically deleted (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The `max_log_file_action` setting determines how to handle the audit log file reaching the max file size. A value of `keep_logs` will rotate the logs but never delete old logs.

##### **Rationale:**

In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

##### **Audit:**

Run the following command and verify output matches:

```
# grep max_log_file_action /etc/audit/auditd.conf  
max_log_file_action = keep_logs
```

##### **Remediation:**

Set the following parameter in `/etc/audit/auditd.conf`:

```
max_log_file_action = keep_logs
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-8

**CIS Controls:**

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

#### *4.1.2.3 Ensure system is disabled when audit logs are full (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The `auditd` daemon can be configured to halt the system when the audit logs are full.

The `admin_space_left_action` parameter tells the system what action to take when the system has detected that it is low on disk space. Valid values are `ignore`, `syslog`, `suspend`, `single`, and `halt`.

- `ignore`, the audit daemon does nothing
- `Syslog`, the audit daemon will issue a warning to syslog
- `Suspend`, the audit daemon will stop writing records to the disk
- `single`, the audit daemon will put the computer system in single user mode
- `halt`, the audit daemon will shutdown the system

##### **Rationale:**

In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

##### **Impact:**

If the `admin_space_left_action` parameter is set to `halt` the audit daemon will shutdown the system when the disk partition containing the audit logs becomes full.

## **Audit:**

Run the following commands and verify output matches:

```
# grep space_left_action /etc/audit/auditd.conf  
space_left_action = email  
  
# grep action_mail_acct /etc/audit/auditd.conf  
action_mail_acct = root
```

Run the following command and verify the output is either `halt` or `single`:

```
# grep -E 'admin_space_left_action\s*=\s*(halt|single)'  
/etc/audit/auditd.conf  
  
admin_space_left_action = <halt|single>
```

## **Remediation:**

Set the following parameters in `/etc/audit/auditd.conf`:

```
space_left_action = email  
action_mail_acct = root
```

Set `admin_space_left_action` to either `halt` or `single` in `/etc/audit/auditd.conf`.

*Example:*

```
admin_space_left_action = halt
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-8
- AU-12
- SI-5

**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>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●

### **4.1.3 Configure auditd rules**

The Audit system operates on a set of rules that define what is to be captured in the log files.

The following types of Audit rules can be specified:

- Control rules: Allow the Audit system's behavior and some of its configuration to be modified.
- File system rules: Allow the auditing of access to a particular file or a directory. (Also known as file watches)
- System call rules: Allow logging of system calls that any specified program makes.

Audit rules can be set:

- on the command line using the auditctl utility. Note that these rules are not persistent across reboots.
- in a file ending in `.rules` in the `/etc/audit/audit.d/` directory.

#### *4.1.3.1 Ensure changes to system administration scope (`sudoers`) is collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor scope changes for system administrators. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers`, or files in `/etc/sudoers.d`, will be written to when the file(s) or related attributes have changed. The audit records will be tagged with the identifier "scope".

##### **Rationale:**

Changes in the `/etc/sudoers` and `/etc/sudoers.d` files can indicate that an unauthorized change has been made to the scope of system administrator activity.

## **Audit:**

### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&/etc/sudoers/ \
&& / +-p *wa/ \
&& (/ key= * [!-~]* *$/ ||/ -k * [!-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&/etc/sudoers/ \
&& / +-p *wa/ \
&& (/ key= * [!-~]* *$/ ||/ -k * [!-~]* *$/) '
```

Verify the output matches:

```
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor scope changes for system administrators.

Example:

```
# printf "
-w /etc/sudoers -p wa -k scope
-w /etc/sudoers.d -p wa -k scope
" >> /etc/audit/rules.d/50-scope.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>4.8 Log and Alert on Changes to Administrative Group Membership</b> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

#### *4.1.3.2 Ensure actions as another user are always logged (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

`sudo` provides users with temporary elevated privileges to perform operations, either as the superuser or another user.

##### **Rationale:**

Creating an audit log of users with temporary elevated privileges and the operation(s) they performed is essential to reporting. Administrators will want to correlate the events written to the audit trail with the records written to `sudo`'s logfile to verify if unauthorized commands have been executed.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# awk '/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&(/ -C *euid!=uid/||/ -C *uid!=euid/) \
&& / -S *execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-a *always,exit/ \
&& / -F *arch=b[2346]{2}/ \
&&(/ -F *auid!=unset/||/ -F *auid!=-1/||/ -F *auid!=4294967295/) \
&&(/ -C *euid!=uid/||/ -C *uid!=euid/) \
&& / -S *execve/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S execve -C uid!=euid -F auid==1 -F
key=user_emulation
-a always,exit -F arch=b32 -S execve -C uid!=euid -F auid==1 -F
key=user_emulation
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor elevated privileges.

### **64 Bit systems**

Example:

```
# printf "
-a always,exit -F arch=b64 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
-a always,exit -F arch=b32 -C euid!=uid -F auid!=unset -S execve -k
user_emulation
" >> /etc/audit/rules.d/50-user_emulation.rules
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

#### *4.1.3.3 Ensure events that modify the sudo log file are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor the `sudo` log file. If the system has been properly configured to disable the use of the `su` command and force all administrators to have to log in first and then use `sudo` to execute privileged commands, then all administrator commands will be logged to `/var/log/sudo.log`. Any time a command is executed, an audit event will be triggered as the `/var/log/sudo.log` file will be opened for write and the executed administration command will be written to the log.

##### **Rationale:**

Changes in `/var/log/sudo.log` indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to `/var/log/sudo.log` to verify if unauthorized commands have been executed.

## Audit:

### On disk configuration

Run the following command to check the on disk rules:

```
# {
  SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*/logfile=/';s/,? .*\// -e 's///g' -e 's|||\\||g')
[ -n "${SUDO_LOG_FILE_ESCAPED}" ] && awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \
&& /+p *wa/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output of matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

### Running configuration

Run the following command to check loaded rules:

```
# {
  SUDO_LOG_FILE_ESCAPED=$(grep -r logfile /etc/sudoers* | sed -e
's/.*/logfile=/';s/,? .*\// -e 's///g' -e 's|||\\||g')
[ -n "${SUDO_LOG_FILE_ESCAPED}" ] && auditctl -l | awk "/^ *-w/ \
&&/"${SUDO_LOG_FILE_ESCAPED}"/ \
&& /+p *wa/ \
&&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Verify output matches:

```
-w /var/log/sudo.log -p wa -k sudo_log_file
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the sudo log file.

Example:

```
# {
SUDO_LOG_FILE=$(grep -r logfile /etc/sudoers* | sed -e 's/.*logfile=//;s/,?.*//' -e 's/"//g')
[ -n "${SUDO_LOG_FILE}" ] && printf "
-w ${SUDO_LOG_FILE} -p wa -k sudo_log_file
" >> /etc/audit/rules.d/50-sudo.rules \
|| printf "ERROR: Variable 'SUDO_LOG_FILE_ESCAPED' is unset.\n"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b> Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.		●	●

#### *4.1.3.4 Ensure events that modify date and time information are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the;

- `adjtimex` - tune kernel clock
- `settimeofday` - set time using `timeval` and `timezone` structures
- `stime` - using seconds since 1/1/1970
- `clock_settime` - allows for the setting of several internal clocks and timers

system calls have been executed. Further, ensure to write an audit record to the configured audit log file upon exit, tagging the records with a unique identifier such as "time-change".

##### **Rationale:**

Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

##### **Audit:**

###### **64 Bit systems**

###### ***On disk configuration***

Run the following command to check the on disk rules:

```

# {
awk '/^ *-a *always,exit/ \
&& -F *arch=b[2346]{2}/ \
&& -S/ \
&& (/adjtimex/ \
||/settimeofday/ \
||/clock_settime/ ) \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

awk '/^ *-w/ \
&& /etc/localtime/ \
&& +-p *wa/ \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
}

```

Verify output of matches:

```

-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-
change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-
change
-w /etc/localtime -p wa -k time-change

```

### ***Running configuration***

Run the following command to check loaded rules:

```

# {
auditctl -l | awk '/^ *-a *always,exit/ \
&& -F *arch=b[2346]{2}/ \
&& -S/ \
&& (/adjtimex/ \
||/settimeofday/ \
||/clock_settime/ ) \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 

auditctl -l | awk '/^ *-w/ \
&& /etc/localtime/ \
&& +-p *wa/ \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' 
}

```

Verify the output includes:

```

-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -F
key=time-change
-w /etc/localtime -p wa -k time-change

```

## **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with b64. In addition, also audit for the stime system call rule. For example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k  
time-change
```

### **Remediation:**

#### **Create audit rules**

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor events that modify date and time information.

## **64 Bit systems**

Example:

```
# printf "  
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-  
change  
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime -k time-  
change  
-w /etc/localtime -p wa -k time-change  
" >> /etc/audit/rules.d/50-time-change.rules
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot  
required to load rules\n"; fi
```

## **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with b64. In addition, add stime to the system call audit. Example:

```
-a always,exit -F arch=b32 -S adjtimex,settimeofday,clock_settime,stime -k  
time-change
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>5.5 Implement Automated Configuration Monitoring Systems</b> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

#### *4.1.3.5 Ensure events that modify the system's network environment are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Record changes to network environment files or system calls. The below parameters monitors the following system calls, and write an audit event on system call exit:

- `sethostname` - set the systems host name
- `setdomainname` - set the systems domain name

The files being monitored are:

- `/etc/issue` and `/etc/issue.net` - messages displayed pre-login
- `/etc/hosts` - file containing host names and associated IP addresses
- `/etc/sysconfig/network` - additional information that is valid to all network interfaces
- `/etc/sysconfig/network-scripts/` - directory containing network interface scripts and configurations files

##### **Rationale:**

Monitoring `sethostname` and `setdomainname` will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The `/etc/hosts` file is monitored for changes that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring `/etc/issue` and `/etc/issue.net` is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring `/etc/sysconfig/network` is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records should have a relevant tag associated with them.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following commands to check the on disk rules:

```
# {
  awk '/^ *-a *always,exit/ \
&& -F arch=b(32|64) / \
&& -S / \
&& (/sethostname/ \
||/setdomainname/) \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules

  awk '/^ *-w/ \
&& (/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/sysconfig/network/) \
&& +-p wa/ \
&& (/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale
```

#### *Running configuration*

Run the following command to check loaded rules:

```

# {
auditctl -l | awk '/^ *-a *always,exit/ \
&& /-F arch=b(32|64)/ \
&& /-S/ \
&& (/sethostname/ \
||/setdomainname/) \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'"

auditctl -l | awk '/^ *-w/ \
&&(/etc/issue/ \
||/etc/issue.net/ \
||/etc/hosts/ \
||/etc/sysconfig/network/) \
&& /-p wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'"
}

```

Verify the output includes:

```

-a always,exit -F arch=b64 -S sethostname,setdomainname -F key=system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -F key=system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts -p wa -k system-locale

```

## 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64

### Remediation:

#### Create audit rules

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's network environment.

## 64 Bit systems

Example:

```

# printf "
-a always,exit -F arch=b64 -S sethostname,setdomainname -k system-locale
-a always,exit -F arch=b32 -S sethostname,setdomainname -k system-locale
-w /etc/issue -p wa -k system-locale
-w /etc/issue.net -p wa -k system-locale
-w /etc/hosts -p wa -k system-locale
-w /etc/sysconfig/network -p wa -k system-locale
-w /etc/sysconfig/network-scripts/ -p wa -k system-locale
" >> /etc/audit/rules.d/50-system_local.rules

```

## Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

### Additional Information:

#### Potential reboot required

If the auditing configuration is locked (-e 2), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

#### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>5.5 Implement Automated Configuration Monitoring Systems</b> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

#### *4.1.3.6 Ensure use of privileged commands are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor privileged programs, those that have the `setuid` and/or `setgid` bit set on execution, to determine if unprivileged users are running these commands.

##### **Rationale:**

Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.

##### **Impact:**

Both the audit and remediation section of this recommendation will traverse all mounted file systems that is not mounted with either `noexec` or `nosuid` mount options. If there are large file systems without these mount options, **such traversal will be significantly detrimental to the performance of the system.**

Before running either the audit or remediation section, inspect the output of the following command to determine exactly which file systems will be traversed:

```
# findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid"
```

To exclude a particular file system due to adverse performance impacts, update the audit and remediation sections by adding a sufficiently unique string to the `grep` statement. The above command can be used to test the modified exclusions.

## **Audit:**

### **On disk configuration**

Run the following command to check on disk rules:

```
# for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
        grep -qr "${PRIVILEGED}" /etc/audit/rules.d && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in on disk configuration.\n"
    done
done
```

Verify that all output is OK.

### **Running configuration**

Run the following command to check loaded rules:

```
# {
    RUNNING=$(auditctl -l)
    [ -n "${RUNNING}" ] && for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
        for PRIVILEGED in $(find "${PARTITION}" -xdev -perm /6000 -type f); do
            printf -- "${RUNNING}" | grep -q "${PRIVILEGED}" && printf "OK:
'${PRIVILEGED}' found in auditing rules.\n" || printf "Warning:
'${PRIVILEGED}' not found in running configuration.\n"
        done
    done \
    || printf "ERROR: Variable 'RUNNING' is unset.\n"
}
```

Verify that all output is OK.

### **Special mount points**

If there are any special mount points that are not visible by default from `findmnt` as per the above audit, said file systems would have to be manually audited.

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor the use of privileged commands.

Example:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  AUDIT_RULE_FILE="/etc/audit/rules.d/50-privileged.rules"
  NEW_DATA=()
  for PARTITION in $(findmnt -n -l -k -it $(awk '/nodev/ { print $2 }' /proc/filesystems | paste -sd,) | grep -Pv "noexec|nosuid" | awk '{print $1}'); do
    readarray -t DATA < <(find "${PARTITION}" -xdev -perm /6000 -type f | awk -v UID_MIN=${UID_MIN} '{print "-a always,exit -F path=\"\$1\" -F perm=x -F auid>=\"UID_MIN\" -F auid!=unset -k privileged"}')
    for ENTRY in "${DATA[@]}"; do
      NEW_DATA+=("${ENTRY}")
    done
  done
  readarray &> /dev/null -t OLD_DATA < "${AUDIT_RULE_FILE}"
  COMBINED_DATA=( "${OLD_DATA[@]}" "${NEW_DATA[@]}" )
  printf '%s\n' "${COMBINED_DATA[@]}" | sort -u > "${AUDIT_RULE_FILE}"
}
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## **Special mount points**

If there are any special mount points that are not visible by default from just scanning `/`, change the `PARTITION` variable to the appropriate partition and re-run the remediation.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

### **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### *4.1.3.7 Ensure unsuccessful file access attempts are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor for unsuccessful attempts to access files. The following parameters are associated with system calls that control files:

- creation - `creat`
- opening - `open`, `openat`
- truncation - `truncate`, `ftruncate`

An audit log record will only be written if all of the following criteria is met for the user when trying to access a file:

- a non-privileged user (`auid>=UID_MIN`)
- is not a Daemon event (`auid=4294967295/unset/-1`)
- if the system call returned EACCES (permission denied) or EPERM (some other permanent error associated with the specific system call)

##### **Rationale:**

Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid==1/ || / -F *auid!=4294967295/ ) \
  && / -F *auid>=${UID_MIN}/ \
  && / -F *exit=-EACCES/ || / -F *exit=-EPERM/ ) \
  && / -S/ \
  && /creat/ \
  && /open/ \
  && /truncate/ \
  && / key= *[!~-]* *$/ || / -k *[!~-]* *$/" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=1000 -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=1000 -F auid!=unset -k access
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid==1/ || / -F *auid!=4294967295/ ) \
  && / -F *auid>=${UID_MIN}/ \
  && / -F *exit=-EACCES/ || / -F *exit=-EPERM/ ) \
  && / -S/ \
  && /creat/ \
  && /open/ \
  && /truncate/ \
  && / key= *[!~-]* *$/ || / -k *[!~-]* *$/" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output includes:

```

-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EACCES -F auid>=1000 -F auid!=--1 -F key=access
-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat -F exit==EPERM -F auid>=1000 -F auid!=--1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit==EACCES -F auid>=1000 -F auid!=--1 -F key=access
-a always,exit -F arch=b32 -S open,truncate,ftruncate,creat,openat -F exit==EPERM -F auid>=1000 -F auid!=--1 -F key=access

```

## 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

### Remediation:

#### Create audit rules

Edit or create a file in the /etc/audit/rules.d/ directory, ending in .rules extension, with the relevant rules to monitor unsuccessful file access attempts.

## 64 Bit systems

Example:

```

# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b64 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EACCES -F auid>=${UID_MIN} -F auid!=unset -k access
-a always,exit -F arch=b32 -S creat,open,openat,truncate,ftruncate -F exit==EPERM -F auid>=${UID_MIN} -F auid!=unset -k access
" >> /etc/audit/rules.d/50-access.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}

```

### Load audit rules

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

### Additional Information:

#### Potential reboot required

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

#### System call structure

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>14.9 Enforce Detail Logging for Access or Changes to Sensitive Data</b> Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

#### *4.1.3.8 Ensure events that modify user/group information are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Record events affecting the modification of user or group information, including that of passwords and old passwords if in use.

- /etc/group - system groups
- /etc/passwd - system users
- /etc/gshadow - encrypted password for each group
- /etc/shadow - system user passwords
- /etc/security/opasswd - storage of old passwords if the relevant PAM module is in use

The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file.

##### **Rationale:**

Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

## **Audit:**

### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/etc/group/ \
||/etc/passwd/ \
||/etc/gshadow/ \
||/etc/shadow/ \
||/etc/security/opasswd/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/) '
```

Verify the output matches:

```
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify user/group information.

Example:

```
# printf "
-w /etc/group -p wa -k identity
-w /etc/passwd -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/security/opasswd -p wa -k identity
" >> /etc/audit/rules.d/50-identity.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>4.8 Log and Alert on Changes to Administrative Group Membership</b> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

#### *4.1.3.9 Ensure discretionary access control permission modification events are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The following commands and system calls effect the permissions, ownership and various attributes of files.

- chmod
- fchmod
- fchmodat
- chown
- fchown
- fchownat
- lchown
- setxattr
- lsetxattr
- fsetxattr
- removexattr
- lremovexattr
- fremovexattr

In all cases, an audit record will only be written for non-system user ids and will ignore Daemon events. All audit records will be tagged with the identifier "perm\_mod."

##### **Rationale:**

Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid==1/ || / -F *auid!=4294967295/) \
  && / -S/ \
  && / -F *auid>=${UID_MIN}/ \
  && /chmod/ || /fchmod/ || /fchmodat/ \
  || /chown/ || /fchown/ || /fchownat/ || /lchown/ \
  || /setxattr/ || /lsetxattr/ || /fsetxattr/ \
  || /removexattr/ || /lremovexattr/ || /fremovexattr/) \
  && / key= *[!~]* *$/ || / -k *[!~]* *$/" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=unset -F key=perm_mod
```

#### *Running configuration*

Run the following command to check loaded rules:

```

# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/) \
  && -S/ \
  && -F *auid>=${UID_MIN}/ \
  && (/chmod/||/fchmod/||/fchmodat/ \
    ||/chown/||/fchown/||/fchownat/||/lchown/ \
    ||/setxattr/||/lsetxattr/||/fsetxattr/ \
    ||/removexattr/||/lremovexattr/||/fremovexattr/) \
  && (/ key= *[!~]* *$/||/ -k *[!~]* *$/) \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}

```

Verify the output matches:

```

-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=-1
-F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F
auid!=-1 -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=1000 -F auid!=-1 -F key=perm_mod

```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor discretionary access control permission modification events.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=${UID_MIN} -F
auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b64 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
-a always,exit -F arch=b32 -S
setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F
auid>=${UID_MIN} -F auid!=unset -F key=perm_mod
" >> /etc/audit/rules.d/50-perm_mod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>5.5 Implement Automated Configuration Monitoring Systems</b> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

#### *4.1.3.10 Ensure successful file system mounts are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor the use of the `mount` system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the `mount` system call is used by a non-privileged user.

##### **Rationale:**

It is highly unusual for a non privileged user to `mount` file systems to the system. While tracking `mount` commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful `open`, `creat` and `truncate` system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
  && / -F *auid>=${UID_MIN}/ \
  && / -S/ \
  && /mount/ \
  && / key= *[!-~]* *$/ || / -k *[!-~]* *$/ ) " /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid!=-1/ || / -F *auid!=4294967295/ ) \
  && / -F *auid>=${UID_MIN}/ \
  && / -S/ \
  && /mount/ \
  && / key= *[!-~]* *$/ || / -k *[!-~]* *$/ ) " \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid==1 -F key=mounts
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid==1 -F key=mounts
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful file system mounts.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=unset -k mounts
-a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=unset -k mounts
" >> /etc/audit/rules.d/50-perm_mod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

### **NIST SP 800-53 Rev. 5:**

- CM-6

### **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	●		●

#### *4.1.3.11 Ensure session initiation information is collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor session initiation events. The parameters in this section track changes to the files associated with session events.

- `/var/run/utmp` - tracks all currently logged in users.
- `/var/log/wtmp` - file tracks logins, logouts, shutdown, and reboot events.
- `/var/log/btmp` - keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`.

All audit records will be tagged with the identifier "session."

##### **Rationale:**

Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

## **Audit:**

### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/) ' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/\/var\/run\/utmp/ \
||/\/var\/log\/wtmp/ \
||/\/var\/log\/btmp/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/ ||/ -k *[!-~]* *$/) '
```

Verify the output matches:

```
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor session initiation information.

Example:

```
# printf "
-w /var/run/utmp -p wa -k session
-w /var/log/wtmp -p wa -k session
-w /var/log/btmp -p wa -k session
" >> /etc/audit/rules.d/50-session.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>		●	●
v7	<p><b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b>  Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.</p>		●	●
v7	<p><b>16.13 Alert on Account Login Behavior Deviation</b>  Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.</p>			●

#### *4.1.3.12 Ensure login and logout events are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor login and logout events. The parameters below track changes to files associated with login/logout events.

- `/var/log/lastlog` - maintain records of the last time a user successfully logged in.
- `/var/run/faillock` - directory maintains records of login failures via the `pam_faillock` module.

##### **Rationale:**

Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

## **Audit:**

### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/var/log/lastlog/ \
||/var/run/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/var/log/lastlog/ \
||/var/run/faillock/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor login and logout events.

Example:

```
# printf "
-w /var/log/lastlog -p wa -k logins
-w /var/run/faillock -p wa -k logins
" >> /etc/audit/rules.d/50-login.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>		●	●
v7	<p><b>4.9 Log and Alert on Unsuccessful Administrative Account Login</b>  Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.</p>		●	●
v7	<p><b>16.11 Lock Workstation Sessions After Inactivity</b>  Automatically lock workstation sessions after a standard period of inactivity.</p>	●	●	●
v7	<p><b>16.13 Alert on Account Login Behavior Deviation</b>  Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.</p>			●

#### *4.1.3.13 Ensure file deletion events by users are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for:

- `unlink` - remove a file
- `unlinkat` - remove a file attribute
- `rename` - rename a file
- `renameat` rename a file attribute system calls and tags them with the identifier "delete".

##### **Rationale:**

Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid==1/ || / -F *auid!=4294967295/) \
  && / -F *auid>=${UID_MIN}/ \
  && / -S/ \
  && (/unlink/ || /rename/ || /unlinkat/ || /renameat/) \
  && (/ key= *[!~-]* *$/ || / -k *[!~-]* *$/) /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F auid>=1000 -
F auid!=unset -k delete
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
  && / -F *arch=b[2346]{2}/ \
  && / -F *auid!=unset/ || / -F *auid==1/ || / -F *auid!=4294967295/) \
  && / -F *auid>=${UID_MIN}/ \
  && / -S/ \
  && (/unlink/ || /rename/ || /unlinkat/ || /renameat/) \
  && (/ key= *[!~-]* *$/ || / -k *[!~-]* *$/) \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F auid>=1000 -
F auid==1 -F key=delete
-a always,exit -F arch=b32 -S unlink,rename,unlinkat,renameat -F auid>=1000 -
F auid!=1 -F key=delete
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor file deletion events by users.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
-a always,exit -F arch=b32 -S rename,unlink,unlinkat,renameat -F
auid>=${UID_MIN} -F auid!=unset -F key=delete
" >> /etc/audit/rules.d/50-delete.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### *4.1.3.14 Ensure events that modify the system's Mandatory Access Controls are collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor SELinux, an implementation of mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux/ and /usr/share/selinux/ directories.

**Note:** If a different Mandatory Access Control method is used, changes to the corresponding directories should be audited.

##### **Rationale:**

Changes to files in the /etc/selinux/ and /usr/share/selinux/ directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

## **Audit:**

### **On disk configuration**

Run the following command to check the on disk rules:

```
# awk '/^ *-w/ \
&&(/etc/selinux/ \
||/usr/share/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)' /etc/audit/rules.d/*.rules
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

### **Running configuration**

Run the following command to check loaded rules:

```
# auditctl -l | awk '/^ *-w/ \
&&(/etc/selinux/ \
||/usr/share/selinux/) \
&&/ +-p *wa/ \
&&(/ key= *[!-~]* *$/||/ -k *[!-~]* *$/)'
```

Verify the output matches:

```
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
```

## **Remediation:**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor events that modify the system's Mandatory Access Controls.

Example:

```
# printf "
-w /etc/selinux -p wa -k MAC-policy
-w /usr/share/selinux -p wa -k MAC-policy
" >> /etc/audit/rules.d/50-MAC-policy.rules
```

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>5.5 Implement Automated Configuration Monitoring Systems</b> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

*4.1.3.15 Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the chcon command.

**Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chcon/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=unset
-k perm_chng
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chcon/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F
auid==1 -F key=perm_chng
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chcon` command.

### **64 Bit systems**

Example:

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

*4.1.3.16 Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `setfacl` command

**Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/setfacl/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid!=unset -k perm_chng
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/setfacl/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/) \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F
auid==1 -F key=perm_chng
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `setfac1` command.

### **64 Bit systems**

Example:

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/setfac1 -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-priv_cmd.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

*4.1.3.17 Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the `chacl` command

**Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chacl/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=unset
-k priv_cmd
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/bin/chacl/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F
auid==1 -F key=priv_cmd
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `chacl` command.

### **64 Bit systems**

Example:

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "$UID_MIN" ] && printf "
-a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k perm_chng
" >> /etc/audit/rules.d/50-perm_chng.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

*4.1.3.18 Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)*

**Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

**Description:**

The operating system must generate audit records for successful/unsuccessful uses of the usermod command.

**Rationale:**

Without generating audit records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Audit records can be generated from various components within the information system (e.g., module or policy filter).

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following command to check the on disk rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/sbin/usermod/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" /etc/audit/rules.d/*.rules \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid!=unset -k usermod
```

#### *Running configuration*

Run the following command to check loaded rules:

```
# {
  UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
    &&(/ -F *auid!=unset/||/ -F *auid==1/||/ -F *auid!=4294967295/) \
    &&/ -F *auid>=${UID_MIN}/ \
    &&/ -F *perm=x/ \
    &&/ -F *path=/usr/sbin/usermod/ \
    &&(/ key= *[!~]* *$/||/ -k *[!~]* *$/)" \
  || printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -S all -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F
auid==1 -F key=usermod
```

### 32 Bit systems

Follow the same procedures as for 64 bit systems and ignore any entries with b64.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor successful and unsuccessful attempts to use the `usermod` command.

### **64 Bit systems**

Example:

```
# {
  UID_MIN=$(awk '/^UID_MIN/{print $2}' /etc/login.defs)
  [ -n "${UID_MIN}" ] && printf "
-a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k usermod
" >> /etc/audit/rules.d/50-usermod.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

### **32 Bit systems**

Follow the same procedures as for 64 bit systems and ignore any entries with `b64`.

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### *4.1.3.19 Ensure kernel module loading unloading and modification is collected (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Monitor the loading and unloading of kernel modules. All the loading / listing / dependency checking of modules is done by `kmod` via symbolic links.

The following system calls control loading and unloading of modules:

- `init_module` - load a module
- `finit_module` - load a module (used when the overhead of using cryptographically signed modules to determine the authenticity of a module can be avoided)
- `delete_module` - delete a module
- `create_module` - create a loadable module entry
- `query_module` - query the kernel for various bits pertaining to modules

Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of `modules`.

##### **Rationale:**

Monitoring the use of all the various ways to manipulate kernel modules could provide system administrators with evidence that an unauthorized change was made to a kernel module, possibly compromising the security of the system.

## Audit:

### 64 Bit systems

#### *On disk configuration*

Run the following commands to check the on disk rules:

```
# {
awk '/^-a always,exit/ \
&& -F arch=b[2346]{2}/ \
&& (/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&& -S/ \
&& (/init_module/ \
|/finit_module/ \
|/delete_module/ \
|/create_module/ \
|/query_module/) \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/)' /etc/audit/rules.d/*.rules

UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && awk "/^-a always,exit/ \
&& (/ -F auid!=unset/||/ -F auid!=-1/||/ -F auid!=4294967295/) \
&& -F auid>=${UID_MIN}/ \
&& -F perm=x/ \
&& -F path=/usr/bin/kmod/ \
&& (/ key= *[!~]* *$/||/ -k *[!~]* *$/)" /etc/audit/rules.d/*.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

Verify the output matches:

```
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=1000 -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F auid!=unset -
k kernel_modules
```

#### *Running configuration*

Run the following command to check loaded rules:

```

# {
auditctl -l | awk '/^ *-a *always,exit/ \
&& / -F arch=b[2346]{2}/ \
&& (/ -F auid!=unset/||| -F auid!=-1||| -F auid!=4294967295/) \
&& / -S/ \
&& (/init_module/ \
||/finit_module/ \
||/delete_module/ \
||/create_module/ \
||/query_module/) \
&& (/ key= *[!~]* *$/||| -k *[!~]* *$/)' \
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && auditctl -l | awk "/^ *-a *always,exit/ \
&& / -F auid!=unset/||| -F auid!=-1||| -F auid!=4294967295/) \
&& / -F auid>=${UID_MIN}/ \
&& / -F perm=x/ \
&& / -F path=/usr/bin/kmod/ \
&& (/ key= *[!~]* *$/||| -k *[!~]* *$/)" \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}

```

Verify the output includes:

```

-a always,exit -F arch=b64 -S
create_module,init_module,delete_module,query_module,finit_module -F
auid>=1000 -F auid!=-1 -F key=kernel_modules
-a always,exit -S all -F path=/usr/bin/kmod -F perm=x -F auid>=1000 -F
auid!=-1 -F key=kernel_modules

```

## Symlink audit

Audit if the symlinks that `kmod` accepts is indeed pointing at it:

```

# S_LINKS=$(ls -l /usr/sbin/lsmod /usr/sbin/rmmmod /usr/sbin/insmod
/usr/sbin/modinfo /usr/sbin/modprobe /usr/sbin/depmod | grep -v " ->
./bin/kmod" || true) \
&& if [[ "${S_LINKS}" != "" ]]; then printf "Issue with symlinks:
${S_LINKS}\n"; else printf "OK\n"; fi

```

Verify the output states `OK`. If there is a symlink pointing to a different location it should be investigated.

## **Remediation:**

### **Create audit rules**

Edit or create a file in the `/etc/audit/rules.d/` directory, ending in `.rules` extension, with the relevant rules to monitor kernel module modification.

### **64 Bit systems**

Example:

```
# {
UID_MIN=$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)
[ -n "${UID_MIN}" ] && printf "
-a always,exit -F arch=b64 -S
init_module,finit_module,delete_module,create_module,query_module -F
auid>=${UID_MIN} -F auid!=unset -k kernel_modules
-a always,exit -F path=/usr/bin/kmod -F perm=x -F auid>=${UID_MIN} -F
auid!=unset -k kernel_modules
" >> /etc/audit/rules.d/50-kernel_modules.rules \
|| printf "ERROR: Variable 'UID_MIN' is unset.\n"
}
```

### **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot
required to load rules\n"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (`-e 2`), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

### **System call structure**

For performance (`man 7 audit.rules`) reasons it is preferable to have all the system calls on one line. However, your configuration may have them on one line each or some other combination. This is important to understand for both the auditing and remediation sections as the examples given are optimized for performance as per the man page.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

#### *4.1.3.20 Ensure the audit configuration is immutable (Automated)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

Set system audit so that audit rules cannot be modified with `auditctl`. Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot.

**Note:** This setting will require the system to be rebooted to update the active `auditd` configuration settings.

##### **Rationale:**

In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

##### **Audit:**

Run the following command and verify output matches:

```
# grep -Ph -- '^\\h*-e\\h+2\\b' /etc/audit/rules.d/*.rules | tail -1  
-e 2
```

## **Remediation:**

Edit or create the file `/etc/audit/rules.d/99-finalize.rules` and add the line `-e 2` at the end of the file:

*Example:*

```
# printf -- "-e 2" >> /etc/audit/rules.d/99-finalize.rules
```

## **Load audit rules**

Merge and load the rules into active configuration:

```
# augenrules --load
```

Check if reboot is required.

```
# if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then printf "Reboot required to load rules\n"; fi
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AC-3
- AU-3
- AU-3(1)
- MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v8	<p><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.</p>		●	●
v7	<p><b>6.2 Activate audit logging</b>  Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>  Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.1.3.21 Ensure the running and on disk configuration is the same (Manual)*

##### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

##### **Description:**

The Audit system have both on disk and running configuration. It is possible for these configuration settings to differ.

**Note:** Due to the limitations of `augenrules` and `auditctl`, it is not absolutely guaranteed that loading the rule sets via `augenrules --load` will result in all rules being loaded or even that the user will be informed if there was a problem loading the rules.

##### **Rationale:**

Configuration differences between what is currently running and what is on disk could cause unexpected problems or may give a false impression of compliance requirements.

##### **Audit:**

###### **Merged rule sets**

Ensure that all rules in `/etc/audit/rules.d` have been merged into `/etc/audit/audit.rules`:

```
# augenrules --check  
/usr/sbin/augenrules: No change
```

Should there be any drift, run `augenrules --load` to merge and load all rules.

## **Remediation:**

If the rules are not aligned across all three () areas, run the following command to merge and load all rules:

```
# augenrules --load
```

Check if reboot is required.

```
if [[ $(auditctl -s | grep "enabled") =~ "2" ]]; then echo "Reboot required to load rules"; fi
```

## **Additional Information:**

### **Potential reboot required**

If the auditing configuration is locked (-e 2), then `augenrules` will not warn in any way that rules could not be loaded into the running configuration. A system reboot will be required to load the rules into the running configuration.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.		●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

## **4.2 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. A centralized log server provides a single point of entry for further analysis, monitoring and filtering.

### **Security principals for logging**

- Ensure transport layer security is implemented between the client and the log server.
- Ensure that logs are rotated as per the environment requirements.
- Ensure all locally generated logs have the appropriate permissions.
- Ensure all security logs are sent to a remote log server.
- Ensure the required events are logged.

### **What is covered**

This section will cover the minimum best practices for the usage of **either rsyslog or journald**. The recommendations are written such that each is wholly independent of each other and **only one is implemented**.

- If your organization makes use of an enterprise wide logging system completely outside of `rsyslog` or `journald`, then the following recommendations does not directly apply. However, the principals of the recommendations should be followed regardless of what solution is implemented. If the enterprise solution incorporates either of these tools, careful consideration should be given to the following recommendations to determine exactly what applies.
- Should your organization make use of both `rsyslog` and `journald`, take care how the recommendations may or may not apply to you.

### **What is not covered**

- Enterprise logging systems not utilizing `rsyslog` or `journald`. As logging is very situational and dependent on the local environment, not everything can be covered here.
- Transport layer security should be applied to all remote logging functionality. Both `rsyslog` and `journald` supports secure transport and should be configured as such.
- The log server. There are a multitude of reasons for a centralized log server (and keeping a short period logging on the local system), but the log server is out of scope for these recommendations.

### **4.2.1 Configure rsyslog**

The `rsyslog` software package may be used instead of the default `journald` logging mechanism.

**Note:** This section only applies if `rsyslog` is the chosen method for client side logging. Do not apply this section if `journald` is used.

#### *4.2.1.1 Ensure rsyslog is installed (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `rsyslog` software is recommended in environments where `journald` does not meet operation requirements.

##### **Rationale:**

The security enhancements of `rsyslog` such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.

##### **Audit:**

Verify `rsyslog` is installed.

Run the following command:

```
# rpm -q rsyslog
```

Verify the output matches:

```
rsyslog-<version>
```

##### **Remediation:**

Run the following command to install `rsyslog`:

```
# dnf install rsyslog
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.2.1.2 Ensure rsyslog service is enabled (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Once the `rsyslog` package is installed, ensure that the service is enabled.

##### **Rationale:**

If the `rsyslog` service is not enabled to start on boot, the system will not capture logging events.

##### **Audit:**

Run the following command to verify `rsyslog` is enabled:

```
# systemctl is-enabled rsyslog
```

Verify the output matches:

```
enabled
```

##### **Remediation:**

Run the following command to enable `rsyslog`:

```
# systemctl --now enable rsyslog
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.2.1.3 Ensure journald is configured to send logs to rsyslog (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Data from `journald` may be stored in volatile memory or persisted locally on the server. Utilities exist to accept remote export of `journald` logs, however, use of the RSyslog service provides a consistent means of log collection and export.

##### **Rationale:**

**IF** RSyslog is the preferred method for capturing logs, all logs of the system should be sent to it for further processing.

##### **Audit:**

**IF** RSyslog is the preferred method for capturing logs

Review `/etc/systemd/journald.conf` and verify that logs are forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify the output matches:

```
ForwardToSyslog=yes
```

##### **Remediation:**

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

```
ForwardToSyslog=yes
```

Restart the service:

```
# systemctl restart rsyslog
```

### **Additional Information:**

As noted in the `journald` man pages, `journald` logs may be exported to `rsyslog` either through the process mentioned here, or through a facility like `systemd-journald.service`. There are trade-offs involved in each implementation, where `ForwardToSyslog` will immediately capture all events (and forward to an external log server, if properly configured), but may not capture all boot-up activities. Mechanisms such as `systemd-journald.service`, on the other hand, will record bootup events, but may delay sending the information to `rsyslog`, leading to the potential for log manipulation prior to export. Be aware of the limitations of all tools employed to secure a system.

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

### **NIST SP 800-53 Rev. 5:**

- AC-3
- AU-2
- AU-4
- AU-12
- MP-2
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v8	<p><b>8.9 Centralize Audit Logs</b> Centralize, to the extent possible, audit log collection and retention across enterprise assets.</p>		●	●
v7	<p><b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p><b>6.5 Central Log Management</b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.</p>		●	●

#### *4.2.1.4 Ensure rsyslog default file permissions are configured (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

RSyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

##### **Rationale:**

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

##### **Impact:**

The systems global `umask` could override, but only making the file permissions stricter, what is configured in RSyslog with the `FileCreateMode` directive. RSyslog also has its own `$umask` directive that can alter the intended file creation mode. In addition, consideration should be given to how `FileCreateMode` is used.

Thus it is critical to ensure that the intended file creation mode is not overridden with less restrictive settings in `/etc/rsyslog.conf`, `/etc/rsyslog.d/*conf` files and that `FileCreateMode` is set before any file is created.

##### **Audit:**

Run the following command:

```
# grep ^\$FileCreateMode /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Verify the output matches:

```
$FileCreateMode 0640
```

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

**NOTE:** More restrictive permissions such as 0600 is implicitly sufficient.

## **Remediation:**

Edit either `/etc/rsyslog.conf` or a dedicated `.conf` file in `/etc/rsyslog.d/` and set `$FileCreateMode` to 0640 or more restrictive:

```
$FileCreateMode 0640
```

Restart the service:

```
# systemctl restart rsyslog
```

## **References:**

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

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
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.	●	●	●
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.1.5 Ensure logging is configured (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

The `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files specifies rules for logging and which files are to be used to log certain classes of messages.

##### **Rationale:**

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

##### **Audit:**

Review the contents of `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files to ensure appropriate logging is set. In addition, run the following command and verify that the log files are logging information as expected:

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

## **Remediation:**

Edit the following lines in the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files as appropriate for your environment.

**Note:** The below configuration is shown for example purposes only. Due care should be given to how the organization wish to store log data.

```
*. emerg :omusrmsg:*
auth,authpriv.* /var/log/secure
mail.* -/var/log/mail
mail.info -/var/log/mail.info
mail.warning -/var/log/mail.warn
mail.err /var/log/mail.err
cron.* /var/log/cron
*.=warning;*.=err -/var/log/warn
*.crit /var/log/warn
*.*=mail.none;news.none -/var/log/messages
local0,local1.* -/var/log/localmessages
local2,local3.* -/var/log/localmessages
local4,local5.* -/var/log/localmessages
local6,local7.* -/var/log/localmessages
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

## **References:**

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

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.1.6 Ensure rsyslog is configured to send logs to a remote log host (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

RSyslog supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

##### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

##### **Audit:**

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that logs are sent to a central host (where `loghost.example.com` is the name of your central log host):

##### **Old format**

```
# grep "^\.*[^I][^I]*@" /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include @@<FQDN or IP of remote loghost>, for example

```
*.* @@loghost.example.com
```

##### **New format**

```
# grep -E '^\\s*([#]+\\s+)?action\\(([#]+\\s+)?\\bttarget="?[^"]+\"?\\b' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

Output should include target=<FQDN or IP of remote loghost>, for example:

```
*.* action(type="omfwd" target="loghost.example.com" port="514" protocol="tcp")
```

## **Remediation:**

Edit the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and add the following line (where `loghost.example.com` is the name of your central log host). The `target` directive may either be a fully qualified domain name or an IP address.

```
*.* action(type="omfwd" target="192.168.2.100" port="514" protocol="tcp"  
        action.resumeRetryCount="100"  
        queue.type="LinkedList" queue.size="1000")
```

Run the following command to reload the `rsyslogd` configuration:

```
# systemctl restart rsyslog
```

## **References:**

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

## **Additional Information:**

In addition, see the [RSyslog documentation](#) for implementation details of TLS.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.1.7 Ensure rsyslog is not configured to receive logs from a remote client (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

RSyslog supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

##### **Rationale:**

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

##### **Audit:**

Review the `/etc/rsyslog.conf` and `/etc/rsyslog.d/*.conf` files and verify that the system is not configured to accept incoming logs.

##### **Old format**

```
# grep '$ModLoad imtcp' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
# grep '$InputTCPServerRun' /etc/rsyslog.conf /etc/rsyslog.d/*.conf
```

No output expected.

##### **New format**

```
# grep -P -- '^h*module\(load="imtcp")' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
# grep -P -- '^h*input\(type="imtcp" port="514")' /etc/rsyslog.conf
/etc/rsyslog.d/*.conf
```

No output expected.

## **Remediation:**

Should there be any active log server configuration found in the auditing section, modify those file and remove the specific lines highlighted by the audit. Ensure none of the following entries are present in any of `/etc/rsyslog.conf` or `/etc/rsyslog.d/*.conf`.

### **Old format**

```
$ModLoad imtcp  
$InputTCPServerRun
```

### **New format**

```
module(load="imtcp")  
input(type="imtcp" port="514")
```

Restart the service:

```
# systemctl restart rsyslog
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v8	<p><b>8.2 Collect Audit Logs</b></p> <p>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b></p> <p>Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b></p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

## **4.2.2 Configure journald**

Included in the systemd suite is a journaling service called `systemd-journald.service` for the collection and storage of logging data. It creates and maintains structured, indexed journals based on logging information that is received from a variety of sources such as:

- Classic RFC3164 BSD syslog via the `/dev/log` socket
- `STDOUT/STDERR` of programs via `StandardOutput=journal + StandardError=journal` in service files (both of which are default settings)
- Kernel log messages via the `/dev/kmsg` device node
- Audit records via the kernel's audit subsystem
- Structured log messages via journald's native protocol

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

#### ***4.2.2.1 Ensure journald is configured to send logs to a remote log host***

#### *4.2.2.1.1 Ensure systemd-journal-remote is installed (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

##### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

##### **Audit:**

Verify `systemd-journal-remote` is installed.

Run the following command:

```
# rpm -q systemd-journal-remote
```

Verify the output matches:

```
systemd-journal-remote-<version>
```

##### **Remediation:**

Run the following command to install `systemd-journal-remote`:

```
# dnf install systemd-journal-remote
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.2.2.1.2 Ensure systemd-journal-remote is configured (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

##### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

##### **Audit:**

Verify `systemd-journal-remote` is configured.

Run the following command:

```
# grep -P "^( *URL=|^ *ServerKeyFile=|^ *ServerCertificateFile=|^ *TrustedCertificateFile=" /etc/systemd/journal-upload.conf
```

Verify the output matches per your environments certificate locations and the URL of the log server. Example:

```
URL=192.168.50.42
ServerKeyFile=/etc/ssl/private/journal-upload.pem
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

## **Remediation:**

Edit the `/etc/systemd/journal-upload.conf` file and ensure the following lines are set per your environment:

```
URL=192.168.50.42  
ServerKeyFile=/etc/ssl/private/journal-upload.pem  
ServerCertificateFile=/etc/ssl/certs/journal-upload.pem  
TrustedCertificateFile=/etc/ssl/ca/trusted.pem
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## **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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.2.1.3 Ensure systemd-journal-remote is enabled (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald (via `systemd-journal-remote`) supports the ability to send log events it gathers to a remote log host or to receive messages from remote hosts, thus enabling centralised log management.

##### **Rationale:**

Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system.

##### **Audit:**

Verify `systemd-journal-remote` is enabled.

Run the following command:

```
# systemctl is-enabled systemd-journal-upload.service  
enabled
```

##### **Remediation:**

Run the following command to enable `systemd-journal-remote`:

```
# systemctl --now enable systemd-journal-upload.service
```

##### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- CM-7
- SI-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.2.2.1.4 Ensure journald is not configured to receive logs from a remote client (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald supports the ability to receive messages from remote hosts, thus acting as a log server. Clients should not receive data from other hosts.

##### **NOTE:**

- The same package, `systemd-journal-remote`, is used for both sending logs to remote hosts and receiving incoming logs.
- With regards to receiving logs, there are two services; `systemd-journal-remote.socket` and `systemd-journal-remote.service`.

##### **Rationale:**

If a client is configured to also receive data, thus turning it into a server, the client system is acting outside its operational boundary.

##### **Audit:**

Run the following command to verify `systemd-journal-remote.socket` is not enabled:

```
# systemctl is-enabled systemd-journal-remote.socket
```

Verify the output matches:

```
masked
```

##### **Remediation:**

Run the following command to disable `systemd-journal-remote.socket`:

```
# systemctl --now mask systemd-journal-remote.socket
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</b></p> <p>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.</p>		●	●
v8	<p><b>8.2 Collect Audit Logs</b></p> <p>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b></p> <p>Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b></p> <p>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

#### *4.2.2.2 Ensure journald service is enabled (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Ensure that the `systemd-journald` service is enabled to allow capturing of logging events.

##### **Rationale:**

If the `systemd-journald` service is not enabled to start on boot, the system will not capture logging events.

##### **Audit:**

Run the following command to verify `systemd-journald` is enabled:

```
# systemctl is-enabled systemd-journald.service
```

Verify the output matches:

```
static
```

##### **Remediation:**

By default the `systemd-journald` service does not have an `[Install]` section and thus cannot be enabled / disabled. It is meant to be referenced as `Requires` or `Wants` by other unit files. As such, if the status of `systemd-journald` is not `static`, investigate why.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>6.2 Activate audit logging</b>            Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

#### *4.2.2.3 Ensure journald is configured to compress large log files (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

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

##### **Audit:**

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

```
# grep ^\s*Compress /etc/systemd/journald.conf
```

Verify the output matches:

```
Compress=yes
```

##### **Remediation:**

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

```
Compress=yes
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

## **Additional Information:**

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

It is possible to change the default threshold of 512 bytes per object before compression is used.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.		●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	<b>6.4 Ensure adequate storage for logs</b> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

#### *4.2.2.4 Ensure journald is configured to write logfiles to persistent disk (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

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

##### **Rationale:**

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

##### **Audit:**

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

```
# grep ^\s*Storage /etc/systemd/journald.conf
```

Verify the output matches:

```
Storage=persistent
```

##### **Remediation:**

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

```
Storage=persistent
```

Restart the service:

```
# systemctl restart systemd-journal-upload
```

### **Additional Information:**

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

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.2.5 Ensure journald is not configured to send logs to rsyslog (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Data from `journald` should be kept in the confines of the service and not forwarded on to other services.

##### **Rationale:**

If `journald` is the method for capturing logs, all logs of the system should be handled by `journald` and not forwarded to other logging mechanisms.

##### **Audit:**

If `journald` is the method for capturing logs

Review `/etc/systemd/journald.conf` and verify that logs are not forwarded to `rsyslog`.

```
# grep ^\s*ForwardToSyslog /etc/systemd/journald.conf
```

Verify that there is no output.

##### **Remediation:**

Edit the `/etc/systemd/journald.conf` file and ensure that `ForwardToSyslog=yes` is removed.

Restart the service:

```
# systemctl restart systemd-journal-upload
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v8	<p><b>8.9 Centralize Audit Logs</b> Centralize, to the extent possible, audit log collection and retention across enterprise assets.</p>		●	●
v7	<p><b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.</p>	●	●	●
v7	<p><b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●
v7	<p><b>6.5 Central Log Management</b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.</p>		●	●

#### *4.2.2.6 Ensure journald log rotation is configured per site policy (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file `/etc/systemd/journald.conf` is the configuration file used to specify how logs generated by Journald should be rotated.

##### **Rationale:**

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

##### **Audit:**

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

##### **Remediation:**

Review `/etc/systemd/journald.conf` and verify logs are rotated according to site policy. The settings should be carefully understood as there are specific edge cases and prioritization of parameters.

The specific parameters for log rotation are:

```
SystemMaxUse=
SystemKeepFree=
RuntimeMaxUse=
RuntimeKeepFree=
MaxFileSec=
```

## **Additional Information:**

See `man 5 journald.conf` for detailed information regarding the parameters in use.

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.2.7 Ensure journald default file permissions configured (Manual)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Journald will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

##### **Rationale:**

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

##### **Audit:**

First see if there is an override file `/etc/tmpfiles.d/systemd.conf`. If so, this file will override all default settings as defined in `/usr/lib/tmpfiles.d/systemd.conf` and should be inspected.

If there is no override file, inspect the default `/usr/lib/tmpfiles.d/systemd.conf` against the site specific requirements.

Ensure that file permissions are 0640.

Should a site policy dictate less restrictive permissions, ensure to follow said policy.

**NOTE:** More restrictive permissions such as 0600 is implicitly sufficient.

##### **Remediation:**

If the default configuration is not appropriate for the site specific requirements, copy `/usr/lib/tmpfiles.d/systemd.conf` to `/etc/tmpfiles.d/systemd.conf` and modify as required. Requirements is either 0640 or site policy if that is less restrictive.

## **Additional Information:**

See `man 5 tmpfiles.d` for detailed information on the permission sets for the relevant log files. Further information with examples can be found at  
<https://www.freedesktop.org/software/systemd/man/tmpfiles.d.html>

## **NIST SP 800-53 Rev. 5:**

- AC-3
- AU-2
- AU-12
- MP-2
- SI-5

## **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.	●	●	●
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.	●	●	●
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

#### *4.2.3 Ensure permissions on all logfiles are configured (Automated)*

##### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

##### **Description:**

Log files contain information from many services on the local system, or in the event of a centralized log server, others systems logs as well. In general log files are found in `/var/log/`, although application can be configured to store logs elsewhere. Should your application store logs in another, ensure to run the same test on that location.

##### **Rationale:**

It is important that log files have the correct permissions to ensure that sensitive data is protected and that only the appropriate users / groups have access to them.

##### **Audit:**

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

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

No output should be returned.

If there is any output, it is recommended that you capture said output. In the even that the remediation breaks an application due to the permission change, this output make the reverting process effortless.

##### **Remediation:**

Run the following command to set permissions on all existing log files in `/var/log`. Although the command is not destructive, ensure that the output of the audit procedure is captured in the event that the remediation causes issues.

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

If there are services that logs to other locations, ensure that those log files have the appropriate permissions.

### **Additional Information:**

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

### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

### **CIS Controls:**

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

## *4.3 Ensure logrotate is configured (Manual)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The system includes the capability of rotating log files regularly to avoid filling up the system with logs or making the logs unmanageably large. The file /etc/logrotate.d/syslog is the configuration file used to rotate log files created by syslog or rsyslog.

### **Rationale:**

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

### **Audit:**

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

### **Remediation:**

Edit /etc/logrotate.conf and /etc/logrotate.d/\* to ensure logs are rotated according to site policy.

### **Additional Information:**

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

### **NIST SP 800-53 Rev. 5:**

- AU-8

**CIS Controls:**

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

## ***5 Access, Authentication and Authorization***

## **5.1 Configure time-based job schedulers**

`cron` is a time-based job scheduler used to schedule jobs, commands or shell scripts, to run periodically at fixed times, dates, or intervals.

`at` provides the ability to execute a command or shell script at a specified date and hour, or after a given interval of time.

Other methods exist for scheduling jobs, such as `systemd timers`. If another method is used, it should be secured in accordance with local site policy

*Note: `systemd timers` are `systemd unit files` whose name ends in `.timer` that control `.service` files or events. Timers can be used as an alternative to `cron` and `at`. Timers have built-in support for calendar time events, monotonic time events, and can be run asynchronously*

*If `cron` and `at` are not installed, this section can be skipped.*

### *5.1.1 Ensure cron daemon is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `cron` daemon is used to execute batch jobs on the system.

#### **Rationale:**

While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and `cron` is used to execute them.

#### **Audit:**

Run the following command to verify `cron` is enabled:

```
# systemctl is-enabled crond  
enabled
```

Verify result is "enabled".

#### **Remediation:**

Run the following command to enable `cron`:

```
# systemctl --now enable crond
```

#### **Additional Information:**

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

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## *5.1.2 Ensure permissions on /etc/crontab are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/crontab` file is used by `cron` to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file.

### **Rationale:**

This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

### **Audit:**

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

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

### **Remediation:**

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

```
# chown root:root /etc/crontab
# chmod og-rwx /etc/crontab
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### *5.1.3 Ensure permissions on /etc/cron.hourly are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

#### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

#### **Audit:**

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

```
# stat /etc/cron.hourly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

#### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/cron.hourly`:

```
# chown root:root /etc/cron.hourly
# chmod og-rwx /etc/cron.hourly
```

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

## *5.1.4 Ensure permissions on /etc/cron.daily are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.daily` directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

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

```
# stat /etc/cron.daily
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/cron.daily`:

```
# chown root:root /etc/cron.daily
# chmod og-rwx /etc/cron.daily
```

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

## *5.1.5 Ensure permissions on /etc/cron.weekly are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.weekly` directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

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

```
# stat /etc/cron.weekly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/cron.weekly`:

```
# chown root:root /etc/cron.weekly
# chmod og-rwx /etc/cron.weekly
```

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

## *5.1.6 Ensure permissions on /etc/cron.monthly are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.monthly` directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

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

```
# stat /etc/cron.monthly
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/cron.monthly`:

```
# chown root:root /etc/cron.monthly
# chmod og-rwx /etc/cron.monthly
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b></p> <p>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.</p>			
v7	<p><b>14.6 Protect Information through Access Control Lists</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>			

## *5.1.7 Ensure permissions on /etc/cron.d are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/cron.d` directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from `/etc/crontab`, but require more granular control as to when they run. The files in this directory cannot be manipulated by the `crontab` command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory.

### **Rationale:**

Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

### **Audit:**

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

```
# stat /etc/cron.d
Access: (0700/drwx-----)  Uid: (      0/    root)  Gid: (      0/    root)
```

### **Remediation:**

Run the following commands to set ownership and permissions on `/etc/cron.d`:

```
# chown root:root /etc/cron.d
# chmod og-rwx /etc/cron.d
```

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *5.1.8 Ensure cron is restricted to authorized users (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

If `cron` is installed in the system, configure `/etc/cron.allow` to allow specific users to use these services. If `/etc/cron.allow` does not exist, then `/etc/cron.deny` is checked. Any user not specifically defined in those files is allowed to use cron. By removing the file, only users in `/etc/cron.allow` are allowed to use cron.

*Note: Even though a given user is not listed in `cron.allow`, cron jobs can still be run as that user. The `cron.allow` file only controls administrative access to the `crontab` command for scheduling and modifying cron jobs.*

#### **Rationale:**

On many systems, only the system administrator is authorized to schedule `cron` jobs. Using the `cron.allow` file to control who can run `cron` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

## Audit:

Run the following script:

```
#!/usr/bin/env bash

cron_chk()
{
    if rpm -q cronie >/dev/null; then
        [ -e /etc/cron.deny ] && echo "Fail: cron.deny exists"
        if [ ! -e /etc/cron.allow ]; then
            echo "Fail: cron.allow doesn't exist"
        else
            ! stat -Lc "%a" /etc/cron.allow | grep -Eq "[0,2,4,6]00" && echo
            "Fail: cron.allow mode too permissive"
            ! stat -Lc "%u:%g" /etc/cron.allow | grep -Eq "^0:0$" && echo "Fail:
            cron.allow owner and/or group not root"
        fi
        if [ ! -e /etc/cron.deny ] && [ -e /etc/cron.allow ] && stat -Lc "%a"
        /etc/cron.allow | grep -Eq "[0,2,4,6]00" \
            && stat -Lc "%u:%g" /etc/cron.allow | grep -Eq "^0:0$"; then
            echo "Pass"
        fi
    else
        echo "Pass: cron is not installed on the system"
    fi
}
cron_chk
```

Verify the output of the script includes Pass

## **Remediation:**

Run the following script to remove `/etc/cron.deny`, create `/etc/cron.allow`, and set the file mode on `/etc/cron.allow`:

```
#!/usr/bin/env bash

cron_fix()
{
    if rpm -q cronie >/dev/null; then
        [ -e /etc/cron.deny ] && rm -f /etc/cron.deny
        [ ! -e /etc/cron.allow ] && touch /etc/cron.allow
        chown root:root /etc/cron.allow
        chmod u-x,go-rwx /etc/cron.allow
    else
        echo "cron is not installed on the system"
    fi
}
cron_fix
```

**OR** Run the following command to remove cron:

```
# dnf remove cronie
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## **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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

### *5.1.9 Ensure at is restricted to authorized users (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

If `at` is installed in the system, configure `/etc/at.allow` to allow specific users to use these services. If `/etc/at.allow` does not exist, then `/etc/at.deny` is checked. Any user not specifically defined in those files is allowed to use `at`. By removing the file, only users in `/etc/at.allow` are allowed to use `at`.

**Note:** Even though a given user is not listed in `at.allow`, `at` jobs can still be run as that user. The `at.allow` file only controls administrative access to the `at` command for scheduling and modifying `at` jobs.

#### **Rationale:**

On many systems, only the system administrator is authorized to schedule `at` jobs. Using the `at.allow` file to control who can run `at` jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

## Audit:

Run the following script:

```
#!/usr/bin/env bash

at_chk()
{
    if rpm -q at >/dev/null; then
        [ -e /etc/at.deny ] && echo "Fail: at.deny exists"
        if [ ! -e /etc/at.allow ]; then
            echo "Fail: at.allow doesn't exist"
        else
            ! stat -Lc "%a" /etc/at.allow | grep -Eq "[0,2,4,6]00" && echo
"Fail: at.allow mode too permissive"
            ! stat -Lc "%u:%g" /etc/at.allow | grep -Eq "^0:0$" && echo "Fail:
at.allow owner and/or group not root"
        fi
        if [ ! -e /etc/at.deny ] && [ -e /etc/at.allow ] && stat -Lc "%a"
/etc/at.allow | grep -Eq "[0,2,4,6]00" \
            && stat -Lc "%u:%g" /etc/at.allow | grep -Eq "^0:0$"; then
            echo "Pass"
        fi
    else
        echo "Pass: at is not installed on the system"
    fi
}
at_chk
```

Verify the output of the script includes Pass

## **Remediation:**

Run the following script to remove /etc/at.deny, create /etc/at.allow, and set the file mode for /etc/at.allow:

```
#!/usr/bin/env bash

at_fix()
{
    if rpm -q at >/dev/null; then
        [ -e /etc/at.deny ] && rm -f /etc/at.deny
        [ ! -e /etc/at.allow ] && touch /etc/at.allow
        chown root:root /etc/at.allow
        chmod u-x,go-rwx /etc/at.allow
    else
        echo "at is not installed on the system"
    fi
}
at_fix
```

**OR** Run the following command to remove at:

```
# dnf remove at
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## **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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.	●	●	●

## **5.2 Configure SSH Server**

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

**Note:**

- The recommendations in this section only apply if the SSH daemon is installed on the system, if remote access is **not** required the SSH daemon can be removed and this section skipped.
- Once all configuration changes have been made to `/etc/ssh/sshd_config`, the `sshd` configuration must be reloaded:

Command to re-load the SSH daemon configuration:

```
# systemctl reload sshd
```

Command to remove the SSH daemon:

```
# dnf remove openssh-server
```

## *5.2.1 Ensure permissions on /etc/ssh/sshd\_config are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

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

### **Remediation:**

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

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

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## *5.2.2 Ensure permissions on SSH private host key files are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

## Audit:

**Note:** Either mode 0640 with owner root and group ssh\_keys OR mode 0600 with owner root and group root is acceptable

Run the following command and verify either:

Uid is 0/root and Gid is /ssh\_keys and permissions 0640 or more restrictive:

OR

Uid is 0/root and Gid is 0/root and permissions are 0600 or more restrictive:

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

*Example output:*

```
File: '/etc/ssh/ssh_host_rsa_key'
  Size: 1679          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8628138    Links: 1
Access: (0640/-rw-r-----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.861750616 +0000
Modify: 2018-10-22 18:24:56.861750616 +0000
Change: 2018-10-22 18:24:56.873750616 +0000
Birth: -
File: '/etc/ssh/ssh_host_ecdsa_key'
  Size: 227           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631760    Links: 1
Access: (0640/-rw-r-----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.897750616 +0000
Modify: 2018-10-22 18:24:56.897750616 +0000
Change: 2018-10-22 18:24:56.905750616 +0000
Birth: -
File: '/etc/ssh/ssh_host_ed25519_key'
  Size: 387           Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 8631762    Links: 1
Access: (0640/-rw-r-----)  Uid: ( 0/      root)  Gid: ( 993/ssh_keys)
Access: 2018-10-22 18:24:56.945750616 +0000
Modify: 2018-10-22 18:24:56.945750616 +0000
Change: 2018-10-22 18:24:56.957750616 +0000
Birth: -
```

## Remediation:

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

```
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chmod u-x,g-wx,o-rwx {} \;
# find /etc/ssh -xdev -type f -name 'ssh_host_*_key' -exec chown root:ssh_keys {} \;
```

**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.	●	●	●
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

### *5.2.3 Ensure permissions on SSH public host key files are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

## Audit:

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

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

*Example output:*

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

## Remediation:

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

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

## Default Value:

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

**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.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## *5.2.4 Ensure SSH access is limited (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- AllowUsers:
  - The `AllowUsers` variable gives the system administrator the option of allowing specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of `user@host`.
- AllowGroups:
  - The `AllowGroups` variable gives the system administrator the option of allowing specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- DenyUsers:
  - The `DenyUsers` variable gives the system administrator the option of denying specific users to `ssh` into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of `user@host`.
- DenyGroups:
  - The `DenyGroups` variable gives the system administrator the option of denying specific groups of users to `ssh` into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

### **Rationale:**

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

## Audit:

Run the following commands and verify the output:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.* )?${\n}# grep -Pi '^h*(allow|deny) (users|groups) \h+\H+(\h+.* )?${\n}/etc/ssh/sshd_config
```

Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>\nallowgroups <grouplist>\ndenyusers <userlist>\ndenygroups <grouplist>
```

## Remediation:

Edit the `/etc/ssh/sshd_config` file to set one or more of the parameter as follows:

```
AllowUsers <userlist>
```

*OR*

```
AllowGroups <grouplist>
```

*OR*

```
DenyUsers <userlist>
```

*OR*

```
DenyGroups <grouplist>
```

## Default Value:

None

## References:

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>4.3 Ensure the Use of Dedicated Administrative Accounts</b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

## *5.2.5 Ensure SSH LogLevel is appropriate (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

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

### **Rationale:**

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

### **Audit:**

Run the following command and verify that output matches loglevel VERBOSE or loglevel INFO:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep loglevel
```

```
loglevel VERBOSE or loglevel INFO
```

Run the following command and verify the output matches:

```
# grep -i 'loglevel' /etc/ssh/sshd_config | grep -Evi '(VERBOSE|INFO)'
```

```
Nothing should be returned
```

## **Remediation:**

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

```
LogLevel VERBOSE
```

*OR*

```
LogLevel INFO
```

## **Default Value:**

LogLevel INFO

## **References:**

1. [https://www.ssh.com/ssh/sshd\\_config/](https://www.ssh.com/ssh/sshd_config/)

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AU-2
- AU-12
- SI-5

## **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.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.	●	●	●

## *5.2.6 Ensure SSH PAM is enabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Impact:**

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

### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i usepam  
usepam yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*UsePAM\s+no' /etc/ssh/sshd_config  
Nothing should be returned
```

### **Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

```
UsePAM yes
```

**Default Value:**

usePAM yes

**References:**

1. SSHD\_CONFIG(5)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## 5.2.7 Ensure SSH root login is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="${hostname}" -C addr="$(grep ${hostname} /etc/hosts | awk '{print $1}')" | grep permitrootlogin
permitrootlogin no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitRootLogin\s+yes' /etc/ssh/sshd_config
Nothing should be returned
```

### Remediation:

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

```
PermitRootLogin no
```

### Default Value:

`PermitRootLogin without-password`

### References:

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-6(2)
- AC-6(5)

**CIS Controls:**

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

## *5.2.8 Ensure SSH HostbasedAuthentication is disabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep hostbasedauthentication  
hostbasedauthentication no
```

Run the following command and verify the output matches:

```
# grep -Ei '^s*HostbasedAuthentication\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

### **Remediation:**

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

```
HostbasedAuthentication no
```

### **Default Value:**

HostbasedAuthentication no

### **References:**

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	●	●	●

## *5.2.9 Ensure SSH PermitEmptyPasswords is disabled (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep permitemptypasswords  
permitemptypasswords no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitEmptyPasswords\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

### **Remediation:**

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

```
PermitEmptyPasswords no
```

### **Default Value:**

`PermitEmptyPasswords no`

### **References:**

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.	●	●	●

## 5.2.10 Ensure SSH PermitUserEnvironment is disabled (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="${hostname}" -C addr="$(grep ${hostname} /etc/hosts | awk '{print $1}')" | grep permituserenvironment  
permituserenvironment no
```

Run the following command and verify the output:

```
# grep -Ei '^s*PermitUserEnvironment\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

### Remediation:

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

```
PermitUserEnvironment no
```

### Default Value:

PermitUserEnvironment no

### References:

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

### *5.2.11 Ensure SSH IgnoreRhosts is enabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ignorerhosts  
ignorerhosts yes
```

Run the following command and verify the output:

```
# grep -Ei '^s*ignorerhosts\s+no\b' /etc/ssh/sshd_config  
Nothing should be returned
```

#### **Remediation:**

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

```
IgnoreRhosts yes
```

#### **Default Value:**

`IgnoreRhosts yes`

#### **References:**

1. `SSHD_CONFIG(5)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.	●	●	●

### *5.2.12 Ensure SSH X11 forwarding is disabled (Automated)*

#### **Profile Applicability:**

- Level 1 - Workstation
- Level 2 - Server

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i x11forwarding  
x11forwarding no
```

Run the following command and verify that the output matches:

```
# grep -Ei '^x11forwarding=yes' /etc/ssh/sshd_config  
Nothing is returned
```

#### **Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

```
X11Forwarding no
```

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-7

**CIS Controls:**

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

### *5.2.13 Ensure SSH AllowTcpForwarding is disabled (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

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

#### **Rationale:**

Leaving port forwarding enabled can expose the organization to security risks and backdoors.

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

#### **Impact:**

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

## **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i allowtcpforwarding  
allowtcpforwarding no
```

Run the following command and verify the output:

```
# grep -Ei '^s*AllowTcpForwarding\s+yes' /etc/ssh/sshd_config  
Nothing should be returned
```

## **Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

```
AllowTcpForwarding no
```

## **Default Value:**

AllowTcpForwarding yes

## **References:**

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

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.1 Establish and Maintain a Secure Configuration Process</b></p> <p>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.</p>	●	●	●
v7	<p><b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>	●	●	●

## *5.2.14 Ensure system-wide crypto policy is not over-ridden (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

System-wide Crypto policy can be over-ridden or opted out of for openSSH

### **Rationale:**

Over-riding or opting out of the system-wide crypto policy could allow for the use of less secure Ciphers, MACs, KexAlgorithms and GSSAPIKexAlgorithm

### **Audit:**

Run the following command:

```
# grep -i '^s*CRYPTO_POLICY=' /etc/sysconfig/sshd
```

No output should be returned

### **Remediation:**

Run the following commands:

```
# sed -ri "s/^s*(CRYPTO_POLICY\s*=.*$)/#\ \1/" /etc/sysconfig/sshd
# systemctl reload sshd
```

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- SC-8

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 Encrypt Sensitive Data in Transit</b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 Encrypt All Sensitive Information in Transit</b> Encrypt all sensitive information in transit.		●	●

### *5.2.15 Ensure SSH warning banner is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify that output matches:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep banner  
banner /etc/issue.net
```

#### **Remediation:**

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

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

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.1 Establish and Maintain a Secure Configuration Process</b></p> <p>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.</p>	●	●	●
v7	<p><b>5.1 Establish Secure Configurations</b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

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

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep maxauthtries  
maxauthtries 4
```

Run the following command and verify that the output:

```
# grep -Ei '^s*maxauthtries\s+([5-9]|1-9[0-9]+)' /etc/ssh/sshd_config  
Nothing is returned
```

### Remediation:

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

```
MaxAuthTries 4
```

### Default Value:

MaxAuthTries 6

**References:**

1. SSHD\_CONFIG(5)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.			
v7	<b>16.13 Alert on Account Login Behavior Deviation</b> Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			

### *5.2.17 Ensure SSH MaxStartups is configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify that output `MaxStartups` is `10:30:60` or more restrictive:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i maxstartups  
maxstartups 10:30:60
```

Run the following command and verify the output:

```
# grep -Ei '^s*maxstartups\s+(((1[1-9]| [1-9] [0-9] [0-9]+):([0-9]+):([0-9]+))|(([0-9]+):(3[1-9]| [4-9] [0-9] |[1-9] [0-9] [0-9]+):([0-9]+))|(([0-9]+):([0-9]+):(6[1-9]| [7-9] [0-9] |[1-9] [0-9] [0-9]+)))' /etc/ssh/sshd_config  
Nothing should be returned
```

#### **Remediation:**

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

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

#### **Default Value:**

`MaxStartups 10:30:100`

**References:**

1. SSHD\_CONFIG(5)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## 5.2.18 Ensure SSH MaxSessions is set to 10 or less (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

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

### Rationale:

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

### Audit:

Run the following command and verify that output `MaxSessions` is 10 or less:

```
# sshd -T -C user=root -C host="${hostname}" -C addr="$(grep ${hostname} /etc/hosts | awk '{print $1}')" | grep -i maxsessions  
maxsessions 10
```

Run the following command and verify the output:

```
grep -Ei '^s*MaxSessions\s+(1[1-9] | [2-9][0-9] | [1-9][0-9][0-9]+)' /etc/ssh/sshd_config  
Nothing should be returned
```

### Remediation:

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

```
MaxSessions 10
```

### Default Value:

MaxSessions 10

## References:

1. SSHD\_CONFIG(5)

## Additional Information:

### NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## 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.	●	●	●

## *5.2.19 Ensure SSH LoginGraceTime is set to one minute or less (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep logingracetime  
logingracetime 60
```

Run the following command and verify the output:

```
# grep -Ei '^s*LoginGraceTime\s+(0|6[1-9]|7-9)[0-9]|1-9)[0-9][0-9]+|^1m' /etc/ssh/sshd_config  
Nothing should be returned
```

### **Remediation:**

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

```
LoginGraceTime 60
```

**Default Value:**

LoginGraceTime 120

**References:**

1. SSHD\_CONFIG(5)

**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.	●	●	●

## *5.2.20 Ensure SSH Idle Timeout Interval is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of ssh sessions.

- `ClientAliveInterval` sets a timeout interval in seconds after which if no data has been received from the client, sshd will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` sets the number of client alive messages which may be sent without sshd receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, sshd will disconnect the client, terminating the session. The default value is 3.
  - The client alive messages are sent through the encrypted channel
  - Setting `ClientAliveCountMax` to 0 disables connection termination

*Example: The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds*

### **Rationale:**

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

- The recommended `ClientAliveInterval` setting is no greater than 900 seconds (15 minutes)
- The recommended `ClientAliveCountMax` setting is 0
- At the 15 minute interval, if the ssh session is inactive, the session will be terminated.

## **Impact:**

In some cases this setting may cause termination of long-running scripts over SSH or remote automation tools which rely on SSH. In developing the local site policy, the requirements of such scripts should be considered and appropriate ServerAliveInterval and ClientAliveInterval settings should be calculated to insure operational continuity.

## **Audit:**

Run the following commands and verify ClientAliveInterval is between 1 and 900:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientaliveinterval  
clientaliveinterval 900
```

Run the following command and verify ClientAliveCountMax is 0:

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep clientalivecountmax  
clientalivecountmax 3
```

Run the following commands and verify the output:

```
# grep -Ei '^\\s*ClientAliveInterval\\s+(0|9[0-9][1-9]|1[0-9][0-9][0-9][0-9]+|1[6-9]m|[2-9][0-9]m|[1-9][0-9][0-9]+m)\\b' /etc/ssh/sshd_config  
Nothing should be returned  
  
# grep -Ei '^\\s*ClientAliveCountMax\\s+([1-9]|1[0-9][0-9]+)\\b' /etc/ssh/sshd_config  
Nothing should be returned
```

## **Remediation:**

Edit the /etc/ssh/sshd\_config file to set the parameters according to site policy. This should include ClientAliveInterval between 1 and 900 and ClientAliveCountMax of 0:

```
ClientAliveInterval 900  
ClientAliveCountMax 0
```

## **Default Value:**

ClientAliveInterval 0

ClientAliveCountMax 3

## References:

1. [https://man.openbsd.org/sshd\\_config](https://man.openbsd.org/sshd_config)

## Additional Information:

### NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## 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>16.11 Lock Workstation Sessions After Inactivity</b> Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

## **5.3 Configure privilege escalation**

There are various tools which allows a permitted user to execute a command as the superuser or another user, as specified by the security policy.

### **sudo**

<https://www.sudo.ws/>

The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

`sudo` supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, which is configured via the file `/etc/sudoers` and any entries in `/etc/sudoers.d`.

### **pkexec**

<https://www.freedesktop.org/software/polkit/docs/0.105/pkexec.1.html>

### *5.3.1 Ensure sudo is installed (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`sudo` allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user ID is used to determine the user name with which to query the security policy.

#### **Rationale:**

`sudo` supports a plug-in architecture for security policies and input/output logging. Third parties can develop and distribute their own policy and I/O logging plug-ins to work seamlessly with the `sudo` front end. The default security policy is `sudoers`, which is configured via the file `/etc/sudoers` and any entries in `/etc/sudoers.d`.

The security policy determines what privileges, if any, a user has to run `sudo`. The policy may require that users authenticate themselves with a password or another authentication mechanism. If authentication is required, `sudo` will exit if the user's password is not entered within a configurable time limit. This limit is policy-specific.

#### **Audit:**

Verify that `sudo` is installed.

Run the following command:

```
# dnf list sudo

Installed Packages
sudo.x86_64          <VERSION>        @anaconda
Available Packages
sudo.x86_64          <VERSION>        updates
```

#### **Remediation:**

Run the following command to install sudo

```
# dnf install sudo
```

**References:**

1. SUDO(8)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-6(2)
- AC-6(5)

**CIS Controls:**

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

### 5.3.2 Ensure sudo commands use pty (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

`sudo` can be configured to run only from a pseudo terminal (`pseudo-pty`).

#### Rationale:

Attackers can run a malicious program using `sudo` which would fork a background process that remains even when the main program has finished executing.

#### Impact:

**WARNING:** Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning. Always use `visudo` to modify `sudo` configuration files.

#### Audit:

Verify that `sudo` can only run other commands from a pseudo terminal.

Run the following command:

```
# grep -rPi '^h*Defaults\\h+([^\#\\n\\r]+,) ?use_pty(, \\h*\\h+\\h*) *\\h*(#.*)?\\$' /etc/sudoers*
/etc/sudoers:Defaults use_pty
```

#### Remediation:

Edit the file `/etc/sudoers` with `visudo` or a file in `/etc/sudoers.d/` with `visudo -f <PATH_TO_FILE>` and add the following line:

```
Defaults use_pty
```

#### References:

1. SUDO(8)
2. VISUDO(8)

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-6(2)
- AC-6(5)

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	<b>5.1 <u>Establish Secure Configurations</u></b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

### 5.3.3 Ensure sudo log file exists (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

sudo can use a custom log file

#### Rationale:

A sudo log file simplifies auditing of sudo commands

#### Impact:

**WARNING:** Editing the `sudo` configuration incorrectly can cause `sudo` to stop functioning.  
Always use `visudo` to modify `sudo` configuration files.

#### Audit:

Run the following command to verify that sudo has a custom log file configured

```
# grep -rPsi
"^\h*Defaults \h+([^\#]+, \h*)?logfile\h*=\h*(\"|\\')?\H+(\\"|\\')?[, \h*\H+\h*]*\h*
(.*.)?\$" /etc/sudoers*
Defaults logfile="/var/log/sudo.log"
```

#### Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo` or `visudo -f` and add the following line:

```
Defaults logfile=<PATH TO CUSTOM LOG FILE>"
```

#### Example

```
Defaults logfile="/var/log/sudo.log"
```

#### References:

1. SUDO(8)
2. VISUDO(8)

### **Additional Information:**

visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

### **NIST SP 800-53 Rev. 5:**

- AU-3
- AU-3(1)

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
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.			
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

### *5.3.4 Ensure users must provide password for escalation (Automated)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The operating system must be configured so that users must provide a password for privilege escalation.

#### **Rationale:**

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

#### **Impact:**

This will prevent automated processes from being able to elevate privileges. To include Ansible and AWS builds

#### **Audit:**

**Note:** If passwords are not being used for authentication, this is not applicable.

Verify the operating system requires users to supply a password for privilege escalation.

Check the configuration of the /etc/sudoers and /etc/sudoers.d/\* files with the following command:

```
# grep -r "^[^#].*NOPASSWD" /etc/sudoers*
```

If any line is found refer to the remediation procedure below.

#### **Remediation:**

Based on the outcome of the audit procedure, use `visudo -f <PATH TO FILE>` to edit the relevant sudoers file.

Remove any line with occurrences of NOPASSWD tags in the file.

**CIS Controls:**

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

### *5.3.5 Ensure re-authentication for privilege escalation is not disabled globally (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The operating system must be configured so that users must re-authenticate for privilege escalation.

#### **Rationale:**

Without re-authentication, users may access resources or perform tasks for which they do not have authorization.

When operating systems provide the capability to escalate a functional capability, it is critical the user re-authenticate.

#### **Audit:**

Verify the operating system requires users to re-authenticate for privilege escalation.

Check the configuration of the /etc/sudoers and /etc/sudoers.d/\* files with the following command:

```
# grep -r "^[^#].*\!authenticate" /etc/sudoers*
```

If any line is found with a !authenticate tag, refer to the remediation procedure below.

#### **Remediation:**

Configure the operating system to require users to reauthenticate for privilege escalation. Based on the outcome of the audit procedure, use visudo -f <PATH TO FILE> to edit the relevant sudoers file.

Remove any occurrences of !authenticate tags in the file(s).

**CIS Controls:**

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

### *5.3.6 Ensure sudo authentication timeout is configured correctly (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`sudo` caches used credentials for a default of 5 minutes. This is for ease of use when there are multiple administrative tasks to perform. The timeout can be modified to suit local security policies.

#### **Rationale:**

Setting a timeout value reduces the window of opportunity for unauthorized privileged access to another user.

#### **Audit:**

Ensure that the caching timeout is no more than 15 minutes.

Example:

```
# grep -roP "timestamp_timeout=\K[0-9]*" /etc/sudoers*
```

If there is no `timestamp_timeout` configured in `/etc/sudoers*` then the default is 5 minutes. This default can be checked with:

```
# sudo -V | grep "Authentication timestamp timeout:"
```

**NOTE:** A value of `-1` means that the timeout is disabled. Depending on the configuration of the `timestamp_type`, this could mean for all terminals / processes of that user and not just that one single terminal session.

## **Remediation:**

If the currently configured timeout is larger than 15 minutes, edit the file listed in the audit section with `visudo -f <PATH TO FILE>` and modify the entry `timestamp_timeout=` to 15 minutes or less as per your site policy. The value is in minutes. This particular entry may appear on its own, or on the same line as `env_reset`. See the following two examples:

```
Defaults    env_reset, timestamp_timeout=15
Defaults    timestamp_timeout=15
Defaults    env_reset
```

## **References:**

1. <https://www.sudo.ws/man/1.9.0/sudoers.man.html>

## **CIS Controls:**

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

### 5.3.7 Ensure access to the su command is restricted (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

The `su` command allows a user to run a command or shell as another user. The program has been superseded by `sudo`, which allows for more granular control over privileged access. Normally, the `su` command can be executed by any user. By uncommenting the `pam_wheel.so` statement in `/etc/pam.d/su`, the `su` command will only allow users in a specific group to execute `su`. This group should be empty to reinforce the use of `sudo` for privileged access.

#### Rationale:

Restricting the use of `su`, and using `sudo` in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The `sudo` utility also provides a better logging and audit mechanism, as it can log each command executed via `sudo`, whereas `su` can only record that a user executed the `su` program.

#### Audit:

Run the following command and verify the output matches the line:

```
# grep -Pi
'^\h*auth\h+(:required|requisite)\h+pam_wheel\.so\h+(:[^#\n\r]+\h+)?((?!\\2)
(use_uid\b|group=\\H+\b))\h+(:[^#\n\r]+\h+)?((?!\\1)(use_uid\b|group=\\H+\b))(\h+.*)?$' /etc/pam.d/su

auth required pam_wheel.so use_uid group=<group_name>
```

Run the following command and verify that the group specified in `<group_name>` contains no users:

```
# grep <group_name> /etc/group

<group_name>:x:<GID>:
```

There should be no users listed after the Group ID field.

## **Remediation:**

Create an empty group that will be specified for use of the `su` command. The group should be named according to site policy.

*Example:*

```
# groupadd sugroup
```

Add the following line to the `/etc/pam.d/su` file, specifying the empty group:

```
auth required pam_wheel.so use_uid group=sugroup
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## **CIS Controls:**

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

## 5.4 Configure authselect

Authselect is a utility that simplifies the configuration of user authentication. Authselect offers two ready-made profiles that can be universally used with all modern identity management systems

Authselect makes testing and troubleshooting easy because it only modifies files in these directories:

- /etc/nsswitch.conf
- /etc/pam.d/\* files
- /etc/dconf/db/distro.d/\* files

You can create and deploy a custom profile by customizing one of the default profiles, the sssd, winbind, or the nis profile. This is particularly useful if Modifying a ready-made authselect profile is not enough for your needs. When you deploy a custom profile, the profile is applied to every user logging into the given host. This would be the recommended method, so that the existing profiles can remain unmodified.

*Example of creating a custom authselect profile called custom-profile*

```
# authselect create-profile custom-profile -b sssd --symlink-meta
```

### **WARNING:**

Do not use authselect if:

- your host is part of Linux Identity Management. Joining your host to an IdM domain with the ipa-client-install command automatically configures SSSD authentication on your host.
- Your host is part of Active Directory via SSSD. Calling the realm join command to join your host to an Active Directory domain automatically configures SSSD authentication on your host.
- It is not recommended to change the authselect profiles configured by ipa-client-install or realm join. If you need to modify them, display the current settings before making any modifications, so you can revert back to them if necessary

### *5.4.1 Ensure custom authselect profile is used (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

A custom profile can be created by copying and customizing one of the default profiles. The default profiles include: sssd, winbind, or the nis. This profile can then be customized to follow site specific requirements.

You can select a profile for the authselect utility for a specific host. The profile will be applied to every user logging into the host.

#### **Rationale:**

A custom profile is required to customize many of the pam options.

When you deploy a profile, the profile is applied to every user logging into the given host

#### **Audit:**

Run the following command to list the custom profile(s)

```
# authselect list | grep '^-\s*custom'
```

Verify output includes a custom profile:

*Example:*

```
- custom/custom-profile  Enable SSSD for system authentication (also for local users only)
```

Run the following command and verify that the current custom authselect profile is in use on the system:

```
# head -1 /etc/authselect/authselect.conf | grep 'custom/'  
custom/<CUSTOM_PROFILE_NAME>
```

## **Remediation:**

Run the following command to create a custom authselect profile:

```
# authselect create-profile <custom-profile name> <options>
```

*Example:*

```
# authselect create-profile custom-profile -b sssd --symlink-meta
```

Run the following command to select a custom authselect profile:

```
# authselect select custom/<CUSTOM PROFILE NAME> {with-<OPTIONS>}
```

*Example:*

```
# authselect select custom/custom-profile with-sudo with-faillock without-nullok
```

## **References:**

1. authselect(8)

## **Additional Information:**

with the option `--base-on=BASE-ID` or `-b=BASE-ID` the new profile will be based on a profile named BASE-ID.

The base profile location is determined with these steps:

1. If BASE-ID starts with prefix `custom/` it is a custom profile.
2. Try if BASE-ID is found in vendor profiles.
3. Try if BASE-ID is found in default profiles.
4. Return an error.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities</b></p> <p>Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.</p>			
v7	<p><b>16.7 Establish Process for Revoking Access</b></p> <p>Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>			

## 5.4.2 Ensure authselect includes with-faillock (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The pam\_faillock.so module maintains a list of failed authentication attempts per user during a specified interval and locks the account in case there were more than deny consecutive failed authentications. It stores the failure records into per-user files in the tally directory

### Rationale:

Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

### Audit:

Run the following commands to verify that faillock is enabled

```
# grep pam_faillock.so /etc/pam.d/password-auth /etc/pam.d/system-auth
```

Output should be similar to:

```
/etc/authselect/password-auth:auth      required
pam_faillock.so preauth silent
/etc/authselect/password-auth:auth      required
pam_faillock.so authfail
/etc/authselect/password-auth:account   required
pam_faillock.so
/etc/authselect/system-auth:auth        required
pam_faillock.so preauth silent
/etc/authselect/system-auth:auth        required
pam_faillock.so authfail
/etc/authselect/system-auth:account    required
pam_faillock.so
```

### Remediation:

Run the following commands to include the `with-faillock` option to the current authselect profile:

```
# authselect enable-feature with-faillock
# authselect apply-changes
```

## References:

1. faillock(8) - Linux man page
2. pam\_faillock(8) - Linux man page

## Additional Information:

### NIST SP 800-53 Rev. 5:

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## 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>16.7 Establish Process for Revoking Access</b> Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	●	●	●

## **5.5 Configure PAM**

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

### *5.5.1 Ensure password creation requirements are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The pam\_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam\_pwquality.so options.

- `try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.
- `retry=3` - Allow 3 tries before sending back a failure.
- `minlen=14` - password must be 14 characters or more

\*\* Either of the following can be used to enforce complex passwords:\*\*

- `minclass=4` - provide at least four classes of characters for the new password

#### **OR**

- `dcredit=-1` - provide at least one digit
- `ucredit=-1` - provide at least one uppercase character
- `ocredit=-1` - provide at least one special character
- `lcredit=-1` - provide at least one lowercase character

The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies

#### **Rationale:**

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

**Audit:**

Verify password creation requirements conform to organization policy:

Run the following command and verify that retry conforms to organization policy.

```
# grep pam_pwquality.so /etc/pam.d/system-auth /etc/pam.d/password-auth
```

Output should be similar to:

```
/etc/pam.d/system-auth:password requisite pam_pwquality.so try_first_pass  
local_users_only enforce_for_root retry=3  
/etc/pam.d/password-auth:password requisite pam_pwquality.so try_first_pass  
local_users_only enforce_for_root retry=3
```

Run the following commands and verify password length requirements conform to organization policy.

```
# grep ^minlen /etc/security/pwquality.conf
```

Verify minlen is 14 or more

Run one of the following commands and verify that password complexity conforms to organization policy.

```
# grep ^minclass /etc/security/pwquality.conf
```

**OR**

```
# grep -E "^\s*\$credit\s*=" /etc/security/pwquality.conf
```

## **Remediation:**

Edit the file /etc/security/pwquality.conf and add or modify the following line for password length to conform to site policy

```
minlen = 14
```

Edit the file /etc/security/pwquality.conf and add or modify the following line for password complexity to conform to site policy

```
minclass = 4
```

*OR*

```
dcredit = -1  
ucredit = -1  
ocredit = -1  
lcredit = -1
```

Run the following script to update the system-auth and password-auth files

```
#!/usr/bin/env bash

for fn in system-auth password-auth; do
    file="/etc/authselect/${(head -1 /etc/authselect/authselect.conf | grep 'custom'))/$fn"
    if ! grep -Pq --
'^\h*password\h+requisite\h+pam_pwquality.so(\h+[^\#\n\r]+)?\h+.*enforce_for_root\b.*$' "$file"; then
        sed -ri 's/^s*(password\s+requisite\s+pam_pwquality.so\s+)(.*)$/\1\2 enforce_for_root/' "$file"
    fi
    if grep -Pq --
'^\h*password\h+requisite\h+pam_pwquality.so(\h+[^\#\n\r]+)?\h+retry=([4-9]| [1-9][0-9]+)\b.*$' "$file"; then
        sed -ri '/pam_pwquality/s/retry=\S+/retry=3/' "$file"
    elif ! grep -Pq --
'^\h*password\h+requisite\h+pam_pwquality.so(\h+[^\#\n\r]+)?\h+retry=\d+\b.*$' "$file"; then
        sed -ri 's/^s*(password\s+requisite\s+pam_pwquality.so\s+)(.*)$/\1\2 retry=3/' "$file"
    fi
done
authselect apply-changes
```

## **Additional Information:**

all default authselect profiles have pam\_pwquality enabled with the expectation that options will be specified in pwquality.conf

**CIS Controls:**

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

## *5.5.2 Ensure lockout for failed password attempts is configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Lock out users after  $n$  unsuccessful consecutive login attempts.

- `deny=<n>` - Number of attempts before the account is locked
- `unlock_time=<n>` - Time in seconds before the account is unlocked

**Note:** The maximum configurable value for `unlock_time` is 604800

### **Rationale:**

Locking out user IDs after  $n$  unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

## Audit:

Verify password lockouts are configured. Depending on the version you are running, follow **one** of the two methods below.

- deny **should not** be 0 (never) or greater than 5
- unlock\_time **should** be 0 (never) or 900 seconds or more.

## Versions 8.2 and later:

Run the following command to verify that Number of failed logon attempts before the account is locked is no greater than 5:

```
# grep -E '^s*deny\s*[1-5]\b' /etc/security/faillock.conf  
deny = 5
```

Run the following command to verify that the time in seconds before the account is unlocked is either 0 (never) or 900 or more.

```
# grep -E '^s*unlock_time\s*(0|9[0-9][0-9]|1-9)[0-9][0-9]+)\b' /etc/security/faillock.conf  
unlock_time = 900
```

## Versions 8.0 and 8.1:

These settings are commonly configured with the `pam_faillock.so` module found in `/etc/pam.d/system-auth` and `/etc/pam.d/password-auth`.

Run the following command are review the output to ensure that it follows local site policy.

```
# grep -E '^s*auth\s+required\s+pam_faillock.so\s+' /etc/pam.d/password-auth  
/etc/pam.d/system-auth
```

Output should look similar to:

<code>/etc/pam.d/password-auth:auth</code>	<code>required</code>	<code>pam_faillock.so preauth silent</code>
<code>deny=5 unlock_time=900</code>		
<code>/etc/pam.d/password-auth:auth</code>	<code>required</code>	<code>pam_faillock.so authfail</code>
<code>deny=5 unlock_time=900</code>		
<code>/etc/pam.d/system-auth:auth</code>	<code>required</code>	<code>pam_faillock.so preauth silent</code>
<code>deny=5 unlock_time=900</code>		
<code>/etc/pam.d/system-auth:auth</code>	<code>required</code>	<code>pam_faillock.so authfail</code>
<code>deny=5 unlock_time=900</code>		

## **Remediation:**

Set password lockouts and unlock times to conform to site policy. deny should be not greater than 5 and unlock\_time should be 0 (never), or 900 seconds or greater.

Depending on the version you are running, follow **one** of the two methods below.

### **Versions 8.2 and later:**

Edit /etc/security/pam\_faillock.conf and update or add the following lines:

```
deny = 5
unlock_time = 900
```

### **Versions 8.0 and 8.1:**

Run the following script to update the system-auth and password-auth files. This script will update/add the deny=5 and unlock\_time=900 options.

This script should be modified as needed to follow local site policy.

```
#!/usr/bin/env bash

for fn in system-auth password-auth; do
    file="/etc/authselect/${(head -1 /etc/authselect/authselect.conf | grep 'custom/'))/$fn"
    if grep -Pq --
'^\h*auth\h+required\h+pam_faillock\.so(\h+[^\#\n\r]+)?\h+deny=(0|[6-9]|1-[9][0-9]+)\b.*$' "$file"; then
        sed -ri '/pam_faillock.so/s/deny=\S+/deny=5/g' "$file"
    elif ! grep -Pq --
'^\h*auth\h+required\h+pam_faillock\.so(\h+[^\#\n\r]+)?\h+deny=\d*\b.*$'
"$file"; then
        sed -r
's/^$\s*(auth\s+required\s+pam_faillock\.so\s+)([^{\}#\n\r]+)?\s*(\{.*\})?(.*$)/\1\2\3 deny=5 \4/' $file
    fi
    if grep -P --
'^\h*(auth\h+required\h+pam_faillock\.so\h+) ([^\#\n\r]+)?\h+unlock_time=([1-[9]|1-[9][0-9]|1-[8][0-9])\b.*$' "$file"; then
        sed -ri '/pam_faillock.so/s/unlock_time=\S+/unlock_time=900/g' "$file"
    elif ! grep -Pq --
'^\h*auth\h+required\h+pam_faillock\.so(\h+[^\#\n\r]+)?\h+unlock_time=\d*\b.*$'
"$file"; then
        sed -r
's/^$\s*(auth\s+required\s+pam_faillock\.so\s+)([^{\}#\n\r]+)?\s*(\{.*\})?(.*$)/\1\2\3 unlock_time=900 \4/' "$file"
    fi
done
authselect apply-changes
```

## **Default Value:**

deny = 3

unlock\_time = 600

### **Additional Information:**

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

If a user has been locked out because they have reached the maximum consecutive failure count defined by `deny=` in the `pam_faillock.so` module, the user can be unlocked by issuing the command `faillock --user <USERNAME> --reset`. This command sets the failed count to 0, effectively unlocking the user.

Use of the "audit" keyword may log credentials in the case of user error during authentication. This risk should be evaluated in the context of the site policies of your organization.

### **CIS Controls:**

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

### 5.5.3 Ensure password reuse is limited (Automated)

#### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

#### Description:

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

- `remember=<5>` - Number of old passwords to remember

#### Rationale:

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

**Note:** These changes only apply to accounts configured on the local system.

#### Audit:

Run the following command and verify that the remembered password history is 5 or more

```
# grep -P
'^\h*password\h+(requisite|sufficient)\h+(pam_pwhistory\.so|pam_unix\.so)\h+
[^#\n\r]+\h+)\?remember=([5-9]|1-9)[0-9]+\h*(\h+.*)\?\$' /etc/pam.d/system-
auth
```

The output should be similar to:

```
password      requisite      pam_pwhistory.so try_first_pass local_users_only
enforce_for_root retry=3 remember=5
password      sufficient    pam_unix.so sha512 shadow  try_first_pass
use_authtok  remember=5
```

## **Remediation:**

Set remembered password history to conform to site policy.

Run the following script to add or modify the `pam_pwhistory.so` and `pam_unix.so` lines to include the `remember` option:

```
#!/usr/bin/env bash

{
    file="/etc/authselect/$ (head -1 /etc/authselect/authselect.conf | grep
'custom/')/system-auth"
    if ! grep -Pq --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([^\#\n\
r]+\h+)?remember=([5-9]| [1-9][0-9]+)\b.*$' "$file"; then
        if grep -Pq --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([^\#\n\
r]+\h+)?remember=\d+\b.*$' "$file"; then
            sed -ri
's/^s*(password\s+(requisite|required|sufficient)\s+pam_pwhistory\.so\s+([^\#
\n\r]+\s+)?)(remember=\S+\s*)(\s+.*)?$/\1 remember=5 \5/' $file
        elif grep -Pq --
'^\h*password\h+(requisite|required|sufficient)\h+pam_pwhistory\.so\h+([^\#\n\
r]+\h+)?.*$' "$file"; then
            sed -ri
'/^s*password\s+(requisite|required|sufficient)\s+pam_pwhistory\.so/ s/$/
remember=5/' $file
        else
            sed -ri
'/^s*password\s+(requisite|required|sufficient)\s+pam_unix\.so/i password
required      pam_pwhistory.so  remember=5 use_authok' $file
        fi
    fi
    if ! grep -Pq --
'^\h*password\h+(requisite|required|sufficient)\h+pam_unix\.so\h+([^\#\n\r]+\h+)?remember=([5-9]| [1-9][0-9]+)\b.*$' "$file"; then
        if grep -Pq --
'^\h*password\h+(requisite|required|sufficient)\h+pam_unix\.so\h+([^\#\n\r]+\h+)?remember=\d+\b.*$' "$file"; then
            sed -ri
's/^s*(password\s+(requisite|required|sufficient)\s+pam_unix\.so\s+([^\#
\n\r]+\s+)?)(remember=\S+\s*)(\s+.*)?$/\1 remember=5 \5/' $file
        else
            sed -ri
'/^s*password\s+(requisite|required|sufficient)\s+pam_unix\.so/ s/$/
remember=5/' $file
        fi
    fi
    authselect apply-changes
}
```

**Additional Information:**

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

**NIST SP 800-53 Rev. 5:**

- IA-5(1)

**CIS Controls:**

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

### *5.5.4 Ensure password hashing algorithm is SHA-512 (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

A cryptographic hash function converts an arbitrary-length input into a fixed length output. Password hashing performs a one-way transformation of a password, turning the password into another string, called the hashed password.

#### **Rationale:**

The SHA-512 algorithm provides stronger hashing than other hashing algorithms used for password hashing with Linux, providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.

**Note:** These changes only apply to accounts configured on the local system.

## Audit:

Verify password hashing algorithm is sha512:

Run the following command to verify the hashing algorithm is sha512 in /etc/libuser.conf:

```
# grep -Ei '^s*crypt_style\s*=s*sha512\b' /etc/libuser.conf  
crypt_style = sha512
```

Run the following command to verify the hashing algorithm is sha512 in /etc/login.defs:

```
# grep -Ei '^s*ENCRYPT_METHOD\s+SHA512\b' /etc/login.defs  
ENCRYPT_METHOD SHA512
```

Run the following command to verify the hashing algorithm is configured with pam\_unix.so in /etc/pam.d/system-auth and /etc/pam.d/password-auth:

```
# grep -P --  
'^h*password\b+h+(requisite|required|sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?  
\h+sha512\b.*$' /etc/pam.d/password-auth and /etc/pam.d/system-auth
```

The output should be similar to:

```
/etc/pam.d/password-auth:password sufficient pam_unix.so sha512 shadow  
try_first_pass use_authok remember=5  
/etc/pam.d/system-auth:password sufficient pam_unix.so sha512 shadow  
try_first_pass use_authok remember=5
```

## **Remediation:**

Set password hashing algorithm to sha512.

Edit `/etc/libuser.conf` and edit or add the following line:

```
crypt_style = sha512
```

Edit `/etc/login.defs` and edit or add the following line:

```
ENCRYPT_METHOD SHA512
```

Run the following script to configure `pam_unix.so` to use the sha512 hashing algorithm:

```
#!/usr/bin/env bash

for fn in system-auth password-auth; do
    file="/etc/authselect/${(head -1 /etc/authselect/authselect.conf | grep 'custom/'))/$fn"
    if ! grep -Pq --
        '^h*password\h+(requisite|required|sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+sha512\b.*$' "$file"; then
        if grep -Pq --
            '^h*password\h+(requisite|required|sufficient)\h+pam_unix\.so(\h+[^#\n\r]+)?\h+(md5|blowfish|bigcrypt|sha256)\b.*$' "$file"; then
                sed -ri 's/(md5|blowfish|bigcrypt|sha256)/sha512/' "$file"
            else
                sed -ri
            's/(\^s*password\s+(requisite|required|sufficient)\s+pam_unix.so\s+)(.*)$/\1sha512 \3/' $file
            fi
        fi
    done
authselect apply-changes
```

**Note:** This only effects local users and passwords created after updating the files to use sha512. If it is determined that the password algorithm being used is not SHA-512, once it is changed, it is recommended that all user ID's be immediately expired and forced to change their passwords on next login.

## **Additional Information:**

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

The following command may be used to expire all non-system user ID's immediately and force them to change their passwords on next login. Any system accounts that need to be expired should be carefully done separately by the system administrator to prevent any potential problems.

```
# awk -F: '($3<'"$(awk '/^UID_MIN/{print $2}' /etc/login.defs)"' && $1 != "nobody") { print $1 }' /etc/passwd | xargs -n 1 chage -d 0
```

## **NIST SP 800-53 Rev. 5:**

- IA-5(1)

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

## ***5.6 User Accounts and Environment***

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

### **5.6.1 Set Shadow Password Suite Parameters**

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

### *5.6.1.1 Ensure password expiration is 365 days or less (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

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

```
# grep PASS_MAX_DAYS /etc/login.defs  
PASS_MAX_DAYS 365
```

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

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

#### **Remediation:**

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

```
PASS_MAX_DAYS 365
```

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

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

### **Additional Information:**

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

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

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

### **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>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

### *5.6.1.2 Ensure minimum days between password changes is 7 or more (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

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

```
# grep ^\s*PASS_MIN_DAYS /etc/login.defs  
PASS_MIN_DAYS 7
```

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

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

## **Remediation:**

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

```
PASS_MIN_DAYS 7
```

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

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

## **Additional Information:**

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

## **CIS Controls:**

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

### *5.6.1.3 Ensure password expiration warning days is 7 or more (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

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

```
# grep PASS_WARN_AGE /etc/login.defs
PASS_WARN_AGE 7
```

Verify all users with a password have their number of days of warning before password expires set to 7 or more:

Run the following command and Review list of users and `PASS_WARN_AGE` to verify that all users' `PASS_WARN_AGE` conforms to site policy (No less than 7 days):

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

## **Remediation:**

Set the PASS\_WARN\_AGE parameter to 7 in /etc/login.defs :

```
PASS_WARN_AGE 7
```

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

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

## **Additional Information:**

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

## **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<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>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

### *5.6.1.4 Ensure inactive password lock is 30 days or less (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

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

```
# useradd -D | grep INACTIVE  
INACTIVE=30
```

Verify all users with a password have Password inactive no more than 30 days after password expires

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

```
# awk -F: '/^#[^#]*:[^!*]*:[^:]*:[^:]*:[^:]*:[^:]*:(\s*-1|3[1-9]|4-9)[0-9]|1-9)[0-9][0-9]+:[^:]*:[^:]*\s*/ {print $1":"$7}' /etc/shadow  
No <user>:<INACTIVE> should be returned
```

## **Remediation:**

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

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

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

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

## **Default Value:**

INACTIVE=-1

## **Additional Information:**

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

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

## **CIS Controls:**

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

### *5.6.1.5 Ensure all users last password change date is in the past (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

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

#### **Rationale:**

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

#### **Audit:**

Run the following command and verify nothing is returned

```
# awk -F: '/^[:]+:[^!*]/{print $1}' /etc/shadow | while read -r usr; \
do change=$(date -d "$(chage --list $usr | grep '^Last password change' | cut \
-d: -f2 | grep -v 'never$')"+%s); \
if [[ "$change" -gt "$(date +%s)" ]]; then \
echo "User: \"$usr\" last password change was \"$(chage --list $usr | grep \
'^Last password change' | cut -d: -f2)\""; fi; done
```

#### **Remediation:**

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

**CIS Controls:**

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

## *5.6.2 Ensure system accounts are secured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

Run the following commands and verify no results are returned:

```
awk -F: '($1!~/^(root|halt|sync|shutdown|nfsnobody)$/ && $3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)"' && $7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/^(\/usr)?\/bin\/false(\/)?$/) { print $1 }' /etc/passwd

awk -F: '($1!="root" && $1!~/^+/ && $3<"$(awk '/^s*UID_MIN/{print $2}' /etc/login.defs)") {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' |
awk '($2!="L" && $2!="LK") {print $1}'
```

## **Remediation:**

Run the commands appropriate for your distribution:

Set the shell for any accounts returned by the audit to nologin:

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

Lock any non root accounts returned by the audit:

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

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

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

The following command will automatically lock not root system accounts:

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

## **Additional Information:**

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

## **NIST SP 800-53 Rev. 5:**

- AC-2(5)
- AC-3
- AC-11
- MP-2

**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.			
v7	<b>14.6 Protect Information through Access Control Lists</b> 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.			

### *5.6.3 Ensure default user shell timeout is 900 seconds or less (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

`TMOUT` is an environmental setting that determines the timeout of a shell in seconds.

- `TMOUT=n` - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0` disables timeout.
- `readonly TMOUT` - Sets the `TMOUT` environmental variable as readonly, preventing unwanted modification during run-time.
- `export TMOUT` - exports the `TMOUT` variable

#### **System Wide Shell Configuration Files:**

- `/etc/profile` - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the `.bash_profile`, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the --login parameter.**
- `/etc/profile.d` - `/etc/profile` will execute the scripts within `/etc/profile.d/*.sh`. It is recommended to place your configuration in a shell script within `/etc/profile.d` to set your own system wide environmental variables.
- `/etc/bashrc` - System wide version of `.bashrc`. In Fedora derived distributions, `etc/bashrc` also invokes `/etc/profile.d/*.sh` if *non-login* shell, but redirects output to `/dev/null` if *non-interactive*. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bashrc.**

#### **Rationale:**

Setting a timeout value reduces the window of opportunity for unauthorized user access to another user's shell session that has been left unattended. It also ends the inactive session and releases the resources associated with that session.

## Audit:

Run the following script to verify that TMOUT is configured to: include a timeout of no more than 900 seconds, to be readonly, to be exported, and is not being changed to a longer timeout.

```
#!/usr/bin/env bash

{
    output1="" output2=""
    [ -f /etc/bashrc ] && BRC="/etc/bashrc"
    for f in "$BRC" /etc/profile /etc/profile.d/*.sh ; do
        grep -Pq '^\\s*([^\#]+\s+)?TMOUT=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9])\\b' "$f" && grep -Pq
        '^\\s*([^\#]+\s+)?readonly\\s+TMOUT(\\s+|\\s*;|\\s*\$)=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9])\\b' "$f" && grep -Pq
        '^\\s*([^\#]+\s+)?export\\s+TMOUT(\\s+|\\s*;|\\s*\$)=(900|[1-8][0-9][0-9]|1[1-9][0-9]|1[1-9])\\b' "$f" &&
        output1="$f"
    done
    grep -Pq '^\\s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\\d{3,})\\b'
    /etc/profile /etc/profile.d/*.sh "$BRC" && output2=$(grep -Ps
    '^\\s*([^\#]+\s+)?TMOUT=(9[0-9][1-9]|9[1-9][0-9]|0+[1-9]\\d{3,})\\b'
    /etc/profile /etc/profile.d/*.sh $BRC)
    if [ -n "$output1" ] && [ -z "$output2" ]; then
        echo -e "\nPASSED\nTMOUT is configured in: \"$output1\"\n"
    else
        [ -z "$output1" ] && echo -e "\nFAILED\nTMOUT is not configured\n"
        [ -n "$output2" ] && echo -e "\nFAILED\nTMOUT is incorrectly
        configured in: \"$output2\"\n"
    fi
}
```

## **Remediation:**

Review `/etc/bashrc`, `/etc/profile`, and all files ending in `*.sh` in the `/etc/profile.d/` directory and remove or edit all `TMOUT=_n_` entries to follow local site policy. `TMOUT` should not exceed 900 or be equal to 0.

Configure `TMOUT` in **one** of the following files:

- A file in the `/etc/profile.d/` directory ending in `.sh`
- `/etc/profile`
- `/etc/bashrc`

*TMOUT configuration examples:*

- As multiple lines:

```
TMOUT=900
readonly TMOUT
export TMOUT
```

- As a single line:

```
readonly TMOUT=900 ; export TMOUT
```

## **Additional Information:**

The audit and remediation in this recommendation apply to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked. Other methods of setting a timeout exist for other shells not covered here.

Ensure that the timeout conforms to your local policy.

## **CIS Controls:**

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

## *5.6.4 Ensure default group for the root account is GID 0 (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

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

### **Rationale:**

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

### **Audit:**

Run the following command and verify the result is 0 :

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

### **Remediation:**

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

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

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## *5.6.5 Ensure default user umask is 027 or more restrictive (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In Linux, the default permissions for any newly created directory is 0777 (`rwxrwxrwx`), and for any newly created file it is 0666 (`rw-rw-rw-`). The `umask` modifies the default Linux permissions by restricting (masking) these permissions. The `umask` is not simply subtracted, but is processed bitwise. Bits set in the `umask` are cleared in the resulting file mode.

`umask` can be set with either `octal` or `Symbolic` values:

- `Octal` (`Numeric`) Value - Represented by either three or four digits. ie `umask 0027` or `umask 027`. If a four digit `umask` is used, the first digit is ignored. The remaining three digits effect the resulting permissions for user, group, and world/other respectively.
- `Symbolic` Value - Represented by a comma separated list for User `u`, group `g`, and world/other `o`. The permissions listed are not masked by `umask`. ie a `umask` set by `umask u=rwx, g=rx, o=` is the `Symbolic` equivalent of the `Octal` `umask 027`. This `umask` would set a newly created directory with file mode `drwxr-x---` and a newly created file with file mode `rw-r-----`.

The default `umask` can be set to use the `pam_umask` module or in a System Wide Shell Configuration File. The user creating the directories or files has the discretion of changing the permissions via the `chmod` command, or choosing a different default `umask` by adding the `umask` command into a User Shell Configuration File, (`.bash_profile` or `.bashrc`), in their home directory.

Setting the default umask:

- pam\_umask module:
  - will set the umask according to the system default in /etc/login.defs and user settings, solving the problem of different umask settings with different shells, display managers, remote sessions etc.
  - umask=<mask> value in the /etc/login.defs file is interpreted as Octal
  - Setting USERGROUPS\_ENAB to yes in /etc/login.defs (default):
    - will enable setting of the umask group bits to be the same as owner bits. (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the <primary group name>
    - userdel will remove the user's group if it contains no more members, and useradd will create by default a group with the name of the user
- System Wide Shell Configuration File:
  - /etc/profile - used to set system wide environmental variables on users shells. The variables are sometimes the same ones that are in the .bash\_profile, however this file is used to set an initial PATH or PS1 for all shell users of the system. **is only executed for interactive login shells, or shells executed with the --login parameter.**
  - /etc/profile.d - /etc/profile will execute the scripts within /etc/profile.d/\* .sh. It is recommended to place your configuration in a shell script within /etc/profile.d to set your own system wide environmental variables.
  - /etc/bashrc - System wide version of .bashrc. In Fedora derived distributions, /etc/bashrc also invokes /etc/profile.d/\* .sh if non-login shell, but redirects output to /dev/null if non-interactive. **Is only executed for interactive shells or if BASH\_ENV is set to /etc/bashrc.**

User Shell Configuration Files:

- ~/.bash\_profile - Is executed to configure your shell before the initial command prompt. **Is only read by login shells.**
- ~/.bashrc - Is executed for interactive shells. **only read by a shell that's both interactive and non-login**

#### Rationale:

Setting a secure default value for umask ensures that users make a conscious choice about their file permissions. A permissive umask value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

## Audit:

Run the following to verify:

- A default user umask is set to enforce a newly created directories' permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive
- No less restrictive System Wide umask is set

Run the following script to verify that a default user umask is set enforcing a newly created directories's permissions to be 750 (drwxr-x---), and a newly created file's permissions be 640 (rw-r-----), or more restrictive:

```
#!/bin/bash

passing=""
grep -Eq '^\s*UMASK\s+(0[0-7][2-7]7|[0-7][2-7]7)\b' /etc/login.defs && grep -Eqi '^s*USERGROUPS_ENAB\s*"no"\b' /etc/login.defs && grep -Eq '^\s*session\s+(optional|requisite|required)\s+pam_umask\.so\b' /etc/pam.d/common-session && passing=true
grep -REiq '^\s*UMASK\s+\s*(0[0-7][2-7]7|[0-7][2-7]7|u=(r?|w?|x?)(r?|w?|x?)(r?|w?|x?),g=(r?x?|x?r?),o=)\b' /etc/profile* /etc/bashrc* && passing=true
[ "$passing" = true ] && echo "Default user umask is set"
```

Verify output is: "Default user umask is set"

Run the following to verify that no less restrictive system wide umask is set:

```
# grep -RPi '^(|^#[^#]* )\s*umask\s+([0-7][0-7][01][0-7]\b|[0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*
```

No file should be returned

## **Remediation:**

Review /etc/bashrc, /etc/profile, and all files ending in \*.sh in the /etc/profile.d/ directory and remove or edit all umask entries to follow local site policy. Any remaining entries should be: umask 027, umask u=rwx, g=rx, o= or more restrictive.

Configure umask in **one** of the following files:

- A file in the /etc/profile.d/ directory ending in .sh
- /etc/profile
- /etc/bashrc

*Example:*

```
# vi /etc/profile.d/set_umask.sh  
umask 027
```

Run the following command and remove or modify the umask of any returned files:

```
# grep -RPi '^(^|[^#]* )\s*umask\s+(([0-7][0-7][01][0-7]\b|[0-7][0-7][0-7][0-6]\b|[0-7][01][0-7]\b|[0-7][0-7][0-7]\b|[0-6]\b|(u=[rwx]{0,3},)?(g=[rwx]{0,3},)?o=[rwx]+\b|(u=[rwx]{1,3},)?g=[^rx]{1,3}(,o=[rwx]{0,3})?\b)' /etc/login.defs /etc/profile* /etc/bashrc*
```

Follow one of the following methods to set the default user umask:

Edit /etc/login.defs and edit the UMASK and USERGROUPS\_ENAB lines as follows:

```
UMASK 027  
USERGROUPS_ENAB no
```

Edit the files /etc/pam.d/password-auth and /etc/pam.d/system-auth and add or edit the following:

```
session optional pam_umask.so
```

**OR** Configure umask in one of the following files:

- A file in the /etc/profile.d/ directory ending in .sh
- /etc/profile
- /etc/bashrc

*Example: /etc/profile.d/set\_umask.sh*

```
umask 027
```

**Note:** this method only applies to bash and shell. If other shells are supported on the system, it is recommended that their configuration files also are checked.

**Default Value:**

UMASK 022

**Additional Information:**

- Other methods of setting a default user umask exist
- If other methods are in use in your environment they should be audited
- The default user umask can be overridden with a user specific umask
- The user creating the directories or files has the discretion of changing the permissions:
  - Using the chmod command
  - Setting a different default umask by adding the umask command into a User Shell Configuration File, (.bashrc), in their home directory
  - Manually changing the umask for the duration of a login session by running the umask command

**NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## ***6 System Maintenance***

Recommendations in this section are intended as maintenance and are intended to be checked on a frequent basis to ensure system stability. Many recommendations do not have quick remediations and require investigation into the cause and best fix available and may indicate an attempted breach of system security.

## ***6.1 System File Permissions***

This section provides guidance on securing aspects of system files and directories.

### *6.1.1 Audit system file permissions (Manual)*

#### **Profile Applicability:**

- Level 2 - Server
- Level 2 - Workstation

#### **Description:**

The RPM package manager has a number of useful options. One of these, the `-v` for RPM option, can be used to verify that system packages are correctly installed. The `-v` option can be used to verify a particular package or to verify all system packages. If no output is returned, the package is installed correctly. The following table describes the meaning of output from the verify option:

Code	Meaning
S	File size differs.
M	File mode differs (includes permissions and file type).
5	The MD5 checksum differs.
D	The major and minor version numbers differ on a device file.
L	A mismatch occurs in a link.
U	The file ownership differs.
G	The file group owner differs.
T	The file time (mtime) differs.

The `rpm -qf` command can be used to determine which package a particular file belongs to.

For example the following commands determines which package the `/bin/bash` file belongs to:

```
# rpm -qf /bin/bash  
bash-4.1.2-29.el6.x86_64  
  
# rpm -S /bin/bash  
bash: /bin/bash
```

To verify the settings for the package that controls the `/bin/bash` file, run the following:

```
# rpm -V bash-4.1.2-29.el6.x86_64  
.M..... /bin/bash  
  
# rpm --verify bash  
??5????? c /etc/bash.bashrc
```

Note that you can feed the output of the `rpm -qf` command to the `rpm -V` command:

```
# rpm -V `rpm -qf /etc/passwd`  
M..... c /etc/passwd  
S.5....T c /etc/printcap
```

### Rationale:

It is important to confirm that packaged system files and directories are maintained with the permissions they were intended to have from the OS vendor.

### Audit:

Run the following command to review all installed packages. Note that this may be very time consuming and may be best scheduled via the `cron` utility. It is recommended that the output of this command be redirected to a file that can be reviewed later.

```
# rpm -Va --nomtime --nosize --nomd5 --nolinkto > <filename>
```

### Remediation:

Correct any discrepancies found and rerun the audit until output is clean or risk is mitigated or accepted.

### References:

1. [http://docs.fedoraproject.org/en-US/Fedora%20Draft%20Documentation/0.1/html/RPM\\_Guide/index.html](http://docs.fedoraproject.org/en-US/Fedora%20Draft%20Documentation/0.1/html/RPM_Guide/index.html)

## **Additional Information:**

Since packages and important files may change with new updates and releases, it is recommended to verify everything, not just a finite list of files. This can be a time consuming task and results may depend on site policy therefore it is not a scorable benchmark item, but is provided for those interested in additional security measures.

Some of the recommendations of this benchmark alter the state of files audited by this recommendation. The audit command will alert for all changes to a file permissions even if the new state is more secure than the default.

## **NIST SP 800-53 Rev. 5:**

- AC-3
- CM-1
- CM-2
- CM-6
- CM-7
- IA-5
- MP-2

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## *6.1.2 Ensure sticky bit is set on all world-writable directories (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them.

### **Rationale:**

This feature prevents the ability to delete or rename files in world writable directories (such as `/tmp`) that are owned by another user.

### **Audit:**

Run the following command to verify no world writable directories exist without the sticky bit set:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \|) 2>/dev/null
```

No output should be returned.

### **Remediation:**

Run the following command to set the sticky bit on all world writable directories:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \|) 2>/dev/null | xargs -I '{}' chmod a+t '{}'
```

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b></p> <p>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.</p>	●	●	●
v8	<p><b>4.1 Establish and Maintain a Secure Configuration Process</b></p> <p>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.</p>	●	●	●
v7	<p><b>5.1 Establish Secure Configurations</b></p> <p>Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●

### *6.1.3 Ensure permissions on /etc/passwd are configured (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The `/etc/passwd` file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.

#### **Rationale:**

It is critical to ensure that the `/etc/passwd` file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

#### **Audit:**

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

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

#### **Remediation:**

Run the following command to set permissions on `/etc/passwd`:

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

#### **Default Value:**

`Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)`

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

## *6.1.4 Ensure permissions on /etc/shadow are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/shadow` file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

If attackers can gain read access to the `/etc/shadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/shadow` file (such as expiration) could also be useful to subvert the user accounts.

### **Audit:**

Run the following command and verify Uid and Gid are 0/root , and Access is 0000 :

```
# stat /etc/shadow
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/shadow`:

```
# chown root:root /etc/shadow
# chmod 0000 /etc/shadow
```

### **Default Value:**

Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.			

## *6.1.5 Ensure permissions on /etc/group are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/group` file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.

### **Rationale:**

The `/etc/group` file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.

### **Audit:**

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

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

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/group`:

```
# chown root:root /etc/group
# chmod u-x,g-wx,o-wx /etc/group
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.			

## *6.1.6 Ensure permissions on /etc/gshadow are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/gshadow` file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

If attackers can gain read access to the `/etc/gshadow` file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the `/etc/gshadow` file (such as group administrators) could also be useful to subvert the group.

### **Audit:**

Run the following command and verify `Uid is 0/root, Gid is 0/root and Access is 0000`:

```
# stat /etc/gshadow
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/gshadow`

```
# chown root:root /etc/gshadow
# chmod 0000 /etc/gshadow
```

### **Default Value:**

`Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)`

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

## *6.1.7 Ensure permissions on /etc/passwd- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The /etc/passwd- file contains backup user account information.

### **Rationale:**

It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

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

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

### **Remediation:**

Run the following commands to set owner, group, and permissions on /etc/passwd-:

```
# chown root:root /etc/passwd-
# chmod chmod u-x,go-wx /etc/passwd-
```

### **Default Value:**

Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

## *6.1.8 Ensure permissions on /etc/shadow- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/shadow-` file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

It is critical to ensure that the `/etc/shadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command and verify `Uid is 0/root, Gid is 0/root and Access is 0000` :

```
# stat /etc/shadow-
Access: (0000/-) Uid: ( 0/    root) Gid: ( 0/    root)
```

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/shadow-` :

```
# chown root:root /etc/shadow-
# chmod 0000 /etc/shadow-
```

### **Default Value:**

`Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)`

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.			

## *6.1.9 Ensure permissions on /etc/group- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/group-` file contains a backup list of all the valid groups defined in the system.

### **Rationale:**

It is critical to ensure that the `/etc/group-` file is protected from unauthorized access.

Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

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

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

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/group-:`

```
# chown root:root /etc/group-
# chmod u-x,go-wx /etc/group-
```

### **Default Value:**

`Access: (0644/-rw-r--r--) Uid: ( 0/ root) Gid: ( 0/ root)`

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.			

## *6.1.10 Ensure permissions on /etc/gshadow- are configured (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `/etc/gshadow-` file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.

### **Rationale:**

It is critical to ensure that the `/etc/gshadow-` file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.

### **Audit:**

Run the following command and verify `Uid is 0/root, Gid is 0/root or <gid>/shadow, and Access is 0000`:

```
# stat /etc/gshadow-
Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)
```

### **Remediation:**

Run the following commands to set owner, group, and permissions on `/etc/gshadow-` :

```
# chown root:root /etc/gshadow-
# chmod 0000 /etc/gshadow-
```

### **Default Value:**

`Access: (0000/-) Uid: ( 0/ root) Gid: ( 0/ root)`

**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.			
v7	<b>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.			

### *6.1.11 Ensure no world writable files exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.

#### **Rationale:**

Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.

#### **Audit:**

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -0002
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -0002
```

#### **Remediation:**

Removing write access for the "other" category (`chmod o-w <filename>`) is advisable, but always consult relevant vendor documentation to avoid breaking any application dependencies on a given file.

#### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>	●	●	●
v7	<p><b>5.1 Establish Secure Configurations</b>  Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●
v7	<p><b>13 Data Protection</b>  Data Protection</p>			

### *6.1.12 Ensure no unowned files or directories exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.

#### **Rationale:**

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

#### **Audit:**

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nouser
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nouser
```

#### **Remediation:**

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

#### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>			
v7	<p><b>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</b>  Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.</p>			

### *6.1.13 Ensure no ungrouped files or directories exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

#### **Rationale:**

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

#### **Audit:**

Run the following command and verify no files are returned:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -nogroup
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -nogroup
```

#### **Remediation:**

Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

#### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><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.</p>			
v7	<p><b>13.2 Remove Sensitive Data or Systems Not Regularly Accessed by Organization</b>  Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.</p>			

### *6.1.14 Audit SUID executables (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SUID program is to enable users to perform functions (such as changing their password) that require root privileges.

#### **Rationale:**

There are valid reasons for SUID programs, but it is important to identify and review such programs to ensure they are legitimate.

#### **Audit:**

Run the following command to list SUID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -4000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -4000
```

#### **Remediation:**

Ensure that no rogue SUID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

#### **Additional Information:**

##### **NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

### *6.1.15 Audit SGID executables (Manual)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

The owner of a file can set the file's permissions to run with the owner's or group's permissions, even if the user running the program is not the owner or a member of the group. The most common reason for a SGID program is to enable users to perform functions (such as changing their password) that require root privileges.

#### **Rationale:**

There are valid reasons for SGID programs, but it is important to identify and review such programs to ensure they are legitimate. Review the files returned by the action in the audit section and check to see if system binaries have a different md5 checksum than what from the package. This is an indication that the binary may have been replaced.

#### **Audit:**

Run the following command to list SGID files:

```
# df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type f -perm -2000
```

The command above only searches local filesystems, there may still be compromised items on network mounted partitions. Additionally the `--local` option to `df` is not universal to all versions, it can be omitted to search all filesystems on a system including network mounted filesystems or the following command can be run manually for each partition:

```
# find <partition> -xdev -type f -perm -2000
```

#### **Remediation:**

Ensure that no rogue SGID programs have been introduced into the system. Review the files returned by the action in the Audit section and confirm the integrity of these binaries.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- AC-3
- MP-2

**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.	●	●	●
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

## ***6.2 User and Group Settings***

This section provides guidance on securing aspects of the users and groups.

**Note:** The recommendations in this section check local users and groups. Any users or groups from other sources such as LDAP will not be audited. In a domain environment similar checks should be performed against domain users and groups.

### *6.2.1 Ensure password fields are not empty (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

An account with an empty password field means that anybody may log in as that user without providing a password.

#### **Rationale:**

All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.

#### **Audit:**

Run the following command and verify that no output is returned:

```
# awk -F: '($2 == "") { print $1 " does not have a password "}' /etc/shadow
```

#### **Remediation:**

If any accounts in the `/etc/shadow` file do not have a password, run the following command to lock the account until it can be determined why it does not have a password:

```
# passwd -l <username>
```

Also, check to see if the account is logged in and investigate what it is being used for to determine if it needs to be forced off.

#### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- IA-5(1)

**CIS Controls:**

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

## *6.2.2 Ensure all groups in /etc/passwd exist in /etc/group (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group.

### **Rationale:**

Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do
    grep -q -P "^.+?::[^:]*:$i:" /etc/group
    if [ $? -ne 0 ]; then
        echo "Group $i is referenced by /etc/passwd but does not exist in
/etc/group"
    fi
done
```

### **Remediation:**

Analyze the output of the Audit step above and perform the appropriate action to correct any discrepancies found.

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16 Account Monitoring and Control</b> Account Monitoring and Control			

### *6.2.3 Ensure no duplicate UIDs exist (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

Although the `useradd` program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the `/etc/passwd` file and change the UID field.

#### **Rationale:**

Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.

#### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do
    [ -z "$x" ] && break
    set - $x
    if [ $1 -gt 1 ]; then
        users=$(awk -F: '$3 == n { print $1 }' n=$2 /etc/passwd | xargs)
        echo "Duplicate UID ($2): $users"
    fi
done
```

#### **Remediation:**

Based on the results of the audit script, establish unique UIDs and review all files owned by the shared UIDs to determine which UID they are supposed to belong to.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16 Account Monitoring and Control</b> Account Monitoring and Control			

## *6.2.4 Ensure no duplicate GIDs exist (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Although the `groupadd` program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the `/etc/group` file and change the GID field.

### **Rationale:**

User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do
    echo "Duplicate GID ($x) in /etc/group"
done
```

### **Remediation:**

Based on the results of the audit script, establish unique GIDs and review all files owned by the shared GID to determine which group they are supposed to belong to.

### **Additional Information:**

You can also use the `grpck` command to check for other inconsistencies in the `/etc/group` file.

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16 Account Monitoring and Control</b> Account Monitoring and Control			

## *6.2.5 Ensure no duplicate user names exist (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Although the `useradd` program will not let you create a duplicate user name, it is possible for an administrator to manually edit the `/etc/passwd` file and change the user name.

### **Rationale:**

If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in `/etc/passwd`. For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/passwd | sort | uniq -d | while read x; do
    echo "Duplicate login name ${x} in /etc/passwd"
done
```

### **Remediation:**

Based on the results of the audit script, establish unique user names for the users. File ownerships will automatically reflect the change as long as the users have unique UIDs.

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16 Account Monitoring and Control</b> Account Monitoring and Control			

## *6.2.6 Ensure no duplicate group names exist (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Although the `groupadd` program will not let you create a duplicate group name, it is possible for an administrator to manually edit the `/etc/group` file and change the group name.

### **Rationale:**

If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in `/etc/group`. Effectively, the GID is shared, which is a security problem.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

cut -d: -f1 /etc/group | sort | uniq -d | while read -r x; do
    echo "Duplicate group name ${x} in /etc/group"
done
```

### **Remediation:**

Based on the results of the audit script, establish unique names for the user groups. File group ownerships will automatically reflect the change as long as the groups have unique GIDs.

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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>16 Account Monitoring and Control</b> Account Monitoring and Control			

## 6.2.7 Ensure root PATH Integrity (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The `root` user can execute any command on the system and could be fooled into executing programs unintentionally if the `PATH` is not set correctly.

### Rationale:

Including the current working directory (`.`) or other writable directory in `root`'s executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as `root` to execute a Trojan horse program.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

RPCV=$(sudo -Hiu root env | grep '^PATH=' | cut -d= -f2)
echo "$RPCV" | grep -q ":" && echo "root's path contains an empty directory (:)"
echo "$RPCV" | grep -q ":"$ && echo "root's path contains a trailing (:)"
for x in $(echo "$RPCV" | tr ":" " "); do
    if [ -d "$x" ]; then
        ls -ldH "$x" | awk '$9 == "." {print "PATH contains current working directory (.)"}
        $3 != "root" {print $9, "is not owned by root"}
        substr($1,6,1) != "-" {print $9, "is group writable"}
        substr($1,9,1) != "-" {print $9, "is world writable"}'
    else
        echo "$x is not a directory"
    fi
done
```

### Remediation:

Correct or justify any items discovered in the Audit step.

**Additional Information:****NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## *6.2.8 Ensure root is the only UID 0 account (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Any account with UID 0 has superuser privileges on the system.

### **Rationale:**

This access must be limited to only the default `root` account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in recommendation "Ensure access to the `su` command is restricted".

### **Audit:**

Run the following command and verify that only "root" is returned:

```
# awk -F: '($3 == 0) { print $1 }' /etc/passwd
root
```

### **Remediation:**

Remove any users other than `root` with UID 0 or assign them a new UID if appropriate.

### **Additional Information:**

#### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## *6.2.9 Ensure all users' home directories exist (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

Users can be defined in `/etc/passwd` without a home directory or with a home directory that does not actually exist.

### **Rationale:**

If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $7!~/^(\\!/usr)?\\!/bin\\!/false(\\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist."
    fi
done
```

**Note:** The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

## **Remediation:**

If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

The following script will create a home directory for users with an interactive shell whose home directory doesn't exist:

```
#!/bin/bash

awk -F: '$1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(/\usr)?/\sbin\nologin(/)?$/ && $7!~((/\usr)?/\bin\nfalse(/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        mkdir "$dir"
        chmod g-w,o-wrx "$dir"
        chown "$user" "$dir"
    fi
done
```

## **Additional Information:**

The audit script checks all users with interactive shells except halt, sync, shutdown, and nfsnobody.

## **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

**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.	●	●	●

## 6.2.10 Ensure users own their home directories (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The user home directory is space defined for the particular user to set local environment variables and to store personal files.

### Rationale:

Since the user is accountable for files stored in the user home directory, the user (or root) must be the owner of the directory.

### Audit:

Run the following script and verify no results are returned:

```
#!/usr/bin/env bash

UHOC()
{
for i in $( awk -F: '$1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\ /usr)?\ /sbin?\ /nologin(\ )?$/ && $7!~^(\ /usr)?\ /bin?\ /false(\ )?$/'
{print $1":"$6}' /etc/passwd); do
    user=$(echo "$i" | cut -d: -f1)
    dir=$(echo "$i" | cut -d: -f2)
    if [ ! -d "$dir" ]; then
        [ -z "$output2" ] && output2="The following users' home directories don't
exist: \"\$user\""
        || output2="$output2, \"\$user\""
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ] && [ "$owner" != "root" ]; then
            [ -z "$output" ] && output="The following users' don't own their home
directory: \"\$user\" home directory is owned by \"\$owner\""
            || output="$output, \"\$user\" home directory is owned by \"\$owner\""
        fi
    fi
done
}
UHOC
```

## **Remediation:**

Change the ownership of any home directories that are not owned by the defined user to the correct user.

The following script will create missing home directories, set the owner, and set the permissions for interactive users' home directories:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin/\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin/\!/false(\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" does not exist, creating
home directory"
        mkdir "$dir"
        chmod g-w,o-rwx "$dir"
        chown "$user" "$dir"
    else
        owner=$(stat -L -c "%U" "$dir")
        if [ "$owner" != "$user" ]; then
            chmod g-w,o-rwx "$dir"
            chown "$user" "$dir"
        fi
    fi
done
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## *6.2.11 Ensure users' home directories permissions are 750 or more restrictive (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

While the system administrator can establish secure permissions for users' home directories, the users can easily override these.

### **Rationale:**

Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin?\!/false(\!)?$/)
{print $1 " " $6}' /etc/passwd | while read -r user dir; do
    if [ ! -d "$dir" ]; then
        echo "User: \"$user\" home directory: \"$dir\" doesn't exist"
    else
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" |
cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo
"$dirperm" | cut -c10)" != "-" ]; then
            echo "User: \"$user\" home directory: \"$dir\" has permissions:
\"$(stat -L -c "%a" "$dir")\""
        fi
    fi
done
```

## **Remediation:**

Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

The following script can be used to remove permissions in excess of 750 from users' home directories:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/^(\/usr)?\/bin\/false(\/)?$/)
{print $6}' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        dirperm=$(stat -L -c "%A" "$dir")
        if [ "$(echo "$dirperm" | cut -c6)" != "-" ] || [ "$(echo "$dirperm" | cut -c8)" != "-" ] || [ "$(echo "$dirperm" | cut -c9)" != "-" ] || [ "$(echo "$dirperm" | cut -c10)" != "-" ]; then
            chmod g-w,o-rwx "$dir"
        fi
    fi
done
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## *6.2.12 Ensure users' dot files are not group or world writable (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.

### **Rationale:**

Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin?\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin?\!/false(\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    for file in "$dir"/.*; do
      if [ ! -h "$file" ] && [ -f "$file" ]; then
        fileperm=$(stat -L -c "%A" "$file")
        if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
          echo "User: \"$user\" file: \"$file\" has permissions:
\"$fileperm\""
        fi
      done
    fi
  done
fi
done
```

## **Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user dot file permissions and determine the action to be taken in accordance with site policy.

The following script will remove excessive permissions on dot files within interactive users' home directories.

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\|/usr)?\|sbin\|nologin(\|/)?$/ && $7!~^(\|/usr)?\|bin\|false(\|/)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        for file in "$dir"/.*; do
            if [ ! -h "$file" ] && [ -f "$file" ]; then
                fileperm=$(stat -L -c "%A" "$file")
                if [ "$(echo "$fileperm" | cut -c6)" != "-" ] || [ "$(echo
"$fileperm" | cut -c9)" != "-" ]; then
                    chmod go-w "$file"
                fi
            fi
        done
    fi
done
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

### *6.2.13 Ensure users' .netrc Files are not group or world accessible (Automated)*

#### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

#### **Description:**

While the system administrator can establish secure permissions for users' .`netrc` files, the users can easily override these.

#### **Rationale:**

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

If a `.netrc` file is required, and follows local site policy, it should have permissions of 600 or more restrictive.

## Audit:

Run the following script. This script will return:

- FAILED: for any .netrc file with permissions less restrictive than 600
- WARNING: for any .netrc files that exist in interactive users' home directories.

```
#!/bin/bash

awk -F: '$(stat -c "%A" "$file") < 600' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            if stat -L -c "%A" "$file" | cut -c4-10 | grep -Eq '[^-]+'; then
                echo "FAILED: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file or excessive
permissions"
            else
                echo "WARNING: User: \"$user\" file: \"$file\" exists with
permissions: \"$(stat -L -c "%a" "$file")\", remove file unless required"
            fi
        fi
    fi
done
```

Verify:

- Any lines beginning with FAILED: - File should be removed unless deemed necessary, in accordance with local site policy, and permissions are updated to be 600 or more restrictive
- Any lines beginning with WARNING: - File should be removed unless deemed necessary, and in accordance with local site policy

## **Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

The following script will remove .netrc files from interactive users' home directories

```
#!/bin/bash

awk -F: '$(1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~(\!/usr)?\!/bin\!/false(\!)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

## **CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
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.	●	●	●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## 6.2.14 Ensure no users have .forward files (Automated)

### Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

### Description:

The .forward file specifies an email address to forward the user's mail to.

### Rationale:

Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.

### Audit:

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~^(\!/usr)?\!/bin\!/false(\!)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.forward"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

## **Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .forward files and determine the action to be taken in accordance with site policy.

The following script will remove .forward files from interactive users' home directories

```
#!/bin/bash

awk -F: '$(1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(/\usr)?/\sbin?\nologin(/)?$/ && $7!~(/\usr)?/\bin?\false(/)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.forward"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
    fi
done
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## **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.	●	●	●

## *6.2.15 Ensure no users have .netrc files (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

The `.netrc` file contains data for logging into a remote host for file transfers via FTP.

### **Rationale:**

The `.netrc` file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over `.netrc` files from other systems which could pose a risk to those systems.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '($1!~/halt|sync|shutdown|nfsnobody)/ &&
$7!~/^(\/usr)?\/sbin\/nologin(\/)?$/ && $7!~/^(\/usr)?\/bin\/false(\/)?$/) {
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
  if [ -d "$dir" ]; then
    file="$dir/.netrc"
    if [ ! -h "$file" ] && [ -f "$file" ]; then
      echo "User: \"$user\" file: \"$file\" exists"
    fi
  fi
done
```

## **Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .netrc files and determine the action to be taken in accordance with site policy.

The following script will remove .netrc files from interactive users' home directories

```
#!/bin/bash

awk -F: '$1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(/\usr)?/\sbin\nologin(/)?$/ && $7!~((/\usr)?/\bin/false(/)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.netrc"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -f "$file"
    fi
done
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

## **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>16.4 Encrypt or Hash all Authentication Credentials</b> Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

## *6.2.16 Ensure no users have .rhosts files (Automated)*

### **Profile Applicability:**

- Level 1 - Server
- Level 1 - Workstation

### **Description:**

While no .rhosts files are shipped by default, users can easily create them.

### **Rationale:**

This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf. Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf, they may have been brought over from other systems and could contain information useful to an attacker for those other systems.

### **Audit:**

Run the following script and verify no results are returned:

```
#!/bin/bash

awk -F: '$1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~^(\!/usr)?\!/sbin\!/nologin(\!)?\$/ && $7!~^(\!/usr)?\!/bin\!/false(\!)?\$/ {'
print $1 " " $6 }' /etc/passwd | while read -r user dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        if [ ! -h "$file" ] && [ -f "$file" ]; then
            echo "User: \"$user\" file: \"$file\" exists"
        fi
    fi
done
```

## **Remediation:**

Making global modifications to users' files without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user .rhosts files and determine the action to be taken in accordance with site policy.

The following script will remove .rhosts files from interactive users' home directories

```
#!/bin/bash

awk -F: '($1!~/^(halt|sync|shutdown|nfsnobody)/ &&
$7!~(^(\!/usr)?\!/sbin\!/nologin(\!)?$/ && $7!~(\!/usr)?\!/bin\!/false(\!)?$/) {
print $6 }' /etc/passwd | while read -r dir; do
    if [ -d "$dir" ]; then
        file="$dir/.rhosts"
        [ ! -h "$file" ] && [ -f "$file" ] && rm -r "$file"
    fi
done
```

## **Additional Information:**

### **NIST SP 800-53 Rev. 5:**

- CM-1
- CM-2
- CM-6
- CM-7
- IA-5

### **CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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	<u>16.4 Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.	●	●	●

# Appendix: Recommendation Summary Table

Control		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 cramfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.2	Ensure mounting of squashfs filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.1.3	Ensure mounting of udf filesystems is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.2</b>	<b>Configure /tmp</b>		
1.1.2.1	Ensure /tmp is a separate partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.2	Ensure nodev option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.3	Ensure noexec option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2.4	Ensure nosuid option set on /tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.3</b>	<b>Configure /var</b>		
1.1.3.1	Ensure separate partition exists for /var (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.2	Ensure nodev option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.3	Ensure noexec option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3.4	Ensure nosuid option set on /var partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.4</b>	<b>Configure /var/tmp</b>		
1.1.4.1	Ensure separate partition exists for /var/tmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4.2	Ensure noexec option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4.3	Ensure nosuid option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4.4	Ensure nodev option set on /var/tmp partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.5</b>	<b>Configure /var/log</b>		
1.1.5.1	Ensure separate partition exists for /var/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.2	Ensure nodev option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.3	Ensure noexec option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.5.4	Ensure nosuid option set on /var/log partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.1.6</b>	<b>Configure /var/log/audit</b>		
1.1.6.1	Ensure separate partition exists for /var/log/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.6.2	Ensure noexec option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

1.1.6.3	Ensure nodev option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.6.4	Ensure nosuid option set on /var/log/audit partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.1.7</b>	<b>Configure /home</b>		
1.1.7.1	Ensure separate partition exists for /home (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.7.2	Ensure nodev option set on /home partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.7.3	Ensure nosuid option set on /home partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.7.4	Ensure usrquota option set on /home partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.7.5	Ensure grpquota option set on /home partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.1.8</b>	<b>Configure /dev/shm</b>		
1.1.8.1	Ensure nodev option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.8.2	Ensure noexec option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.8.3	Ensure nosuid option set on /dev/shm partition (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.9	Disable Automounting (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.1.10	Disable USB Storage (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.2</b>	<b>Configure Software Updates</b>		
1.2.1	Ensure GPG keys are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.2.2	Ensure gpgcheck is globally activated (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.2.3	Ensure package manager repositories are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.3</b>	<b>Filesystem Integrity Checking</b>		
1.3.1	Ensure AIDE is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.3.2	Ensure filesystem integrity is regularly checked (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.4</b>	<b>Secure Boot Settings</b>		
1.4.1	Ensure bootloader password is set (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.4.2	Ensure permissions on bootloader config are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.4.3	Ensure authentication is required when booting into rescue mode (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.5</b>	<b>Additional Process Hardening</b>		
1.5.1	Ensure core dump storage is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.2	Ensure core dump backtraces are disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.5.3	Ensure address space layout randomization (ASLR) is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>1.6</b>	<b>Mandatory Access Control</b>		
<b>1.6.1</b>	<b>Configure SELinux</b>		
1.6.1.1	Ensure SELinux is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

1.6.1.2	Ensure SELinux is not disabled in bootloader configuration (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.6.1.3	Ensure SELinux policy is configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.6.1.4	Ensure the SELinux mode is not disabled (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.6.1.5	Ensure the SELinux mode is enforcing (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.6.1.6	Ensure no unconfined services exist (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.6.1.7	Ensure SETroubleshoot is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.6.1.8	Ensure the MCS Translation Service (mcstrans) is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>1.7</b>	<b>Command Line Warning Banners</b>		
1.7.1	Ensure message of the day is configured properly (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.7.2	Ensure local login warning banner is configured properly (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.7.3	Ensure remote login warning banner is configured properly (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.7.4	Ensure permissions on /etc/motd are configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.7.5	Ensure permissions on /etc/issue are configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.7.6	Ensure permissions on /etc/issue.net are configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>1.8</b>	<b>GNOME Display Manager</b>		
1.8.1	Ensure GNOME Display Manager is removed (Manual)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.8.2	Ensure GDM login banner is configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.8.3	Ensure last logged in user display is disabled (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.8.4	Ensure XDMCP is not enabled (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.8.5	Ensure automatic mounting of removable media is disabled (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure updates, patches, and additional security software are installed (Manual)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure system-wide crypto policy is not legacy (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Services</b>		
<b>2.1</b>	<b>Time Synchronization</b>		
2.1.1	Ensure time synchronization is in use (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure chrony is configured (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>2.2</b>	<b>Special Purpose Services</b>		
2.2.1	Ensure xinetd is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.2	Ensure xorg-x11-server-common is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.3	Ensure Avahi Server is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.4	Ensure CUPS is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2.5	Ensure DHCP Server is not installed (Automated)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2.2.6	Ensure DNS Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.7	Ensure FTP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.8	Ensure VSFTP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.9	Ensure TFTP Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.10	Ensure a web server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.11	Ensure IMAP and POP3 server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.12	Ensure Samba is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.13	Ensure HTTP Proxy Server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.14	Ensure net-snmp is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.15	Ensure NIS server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.16	Ensure telnet-server is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.17	Ensure mail transfer agent is configured for local-only mode (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.18	Ensure nfs-utils is not installed or the nfs-server service is masked (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.19	Ensure rpcbind is not installed or the rpcbind services are masked (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2.20	Ensure rsync is not installed or the rsyncd service is masked (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>2.3</b>	<b>Service Clients</b>		
2.3.1	Ensure NIS Client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3.2	Ensure rsh client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3.3	Ensure talk client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3.4	Ensure telnet client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3.5	Ensure LDAP client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3.6	Ensure TFTP client is not installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.4	Ensure nonessential services are removed or masked (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3</b>	<b>Network Configuration</b>		
<b>3.1</b>	<b>Disable unused network protocols and devices</b>		
3.1.1	Verify if IPv6 is enabled on the system (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1.2	Ensure SCTP is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1.3	Ensure DCCP is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1.4	Ensure wireless interfaces are disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.2</b>	<b>Network Parameters (Host Only)</b>		
3.2.1	Ensure IP forwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.2.2	Ensure packet redirect sending is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.3</b>	<b>Network Parameters (Host and Router)</b>		
3.3.1	Ensure source routed packets are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.2	Ensure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.3	Ensure secure ICMP redirects are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.4	Ensure suspicious packets are logged (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.5	Ensure broadcast ICMP requests are ignored (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

3.3.6	Ensure bogus ICMP responses are ignored (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.7	Ensure Reverse Path Filtering is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.8	Ensure TCP SYN Cookies is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.3.9	Ensure IPv6 router advertisements are not accepted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.4</b>	<b>Firewall Configuration</b>		
<b>3.4.1</b>	<b>Configure firewalld</b>		
3.4.1.1	Ensure firewalld is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.2	Ensure iptables-services not installed with firewalld (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.3	Ensure nftables either not installed or masked with firewalld (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.4	Ensure firewalld service enabled and running (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.5	Ensure firewalld default zone is set (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.6	Ensure network interfaces are assigned to appropriate zone (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.1.7	Ensure firewalld drops unnecessary services and ports (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.4.2</b>	<b>Configure nftables</b>		
3.4.2.1	Ensure nftables is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.2	Ensure firewalld is either not installed or masked with nftables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.3	Ensure iptables-services not installed with nftables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.4	Ensure iptables are flushed with nftables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.5	Ensure an nftables table exists (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.6	Ensure nftables base chains exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.7	Ensure nftables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.8	Ensure nftables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.9	Ensure nftables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.10	Ensure nftables service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.2.11	Ensure nftables rules are permanent (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.4.3</b>	<b>Configure iptables</b>		
<b>3.4.3.1</b>	<b>Configure iptables software</b>		
3.4.3.1.1	Ensure iptables packages are installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.1.2	Ensure nftables is not installed with iptables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.1.3	Ensure firewalld is either not installed or masked with iptables (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.4.3.2</b>	<b>Configure IPv4 iptables</b>		
3.4.3.2.1	Ensure iptables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.2.2	Ensure iptables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

3.4.3.2.3	Ensure iptables rules exist for all open ports (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.2.4	Ensure iptables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.2.5	Ensure iptables rules are saved (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.2.6	Ensure iptables is enabled and active (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>3.4.3.3</b>	<b>Configure IPv6 ip6tables</b>		
3.4.3.3.1	Ensure ip6tables loopback traffic is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.3.2	Ensure ip6tables outbound and established connections are configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.3.3	Ensure ip6tables firewall rules exist for all open ports (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.3.4	Ensure ip6tables default deny firewall policy (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.3.5	Ensure ip6tables rules are saved (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.4.3.3.6	Ensure ip6tables is enabled and active (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>4</b>	<b>Logging and Auditing</b>		
<b>4.1</b>	<b>Configure System Accounting (auditd)</b>		
<b>4.1.1</b>	<b>Ensure auditing is enabled</b>		
4.1.1.1	Ensure auditd is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.1.2	Ensure auditd service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.1.3	Ensure auditing for processes that start prior to auditd is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.1.4	Ensure audit_backlog_limit is sufficient (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>4.1.2</b>	<b>Configure Data Retention</b>		
4.1.2.1	Ensure audit log storage size is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.2	Ensure audit logs are not automatically deleted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.2.3	Ensure system is disabled when audit logs are full (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>4.1.3</b>	<b>Configure auditd rules</b>		
4.1.3.1	Ensure changes to system administration scope (sudoers) is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.2	Ensure actions as another user are always logged (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.3	Ensure events that modify the sudo log file are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.4	Ensure events that modify date and time information are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.5	Ensure events that modify the system's network environment are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.6	Ensure use of privileged commands are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.7	Ensure unsuccessful file access attempts are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.1.3.8	Ensure events that modify user/group information are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.9	Ensure discretionary access control permission modification events are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.10	Ensure successful file system mounts are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.11	Ensure session initiation information is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.12	Ensure login and logout events are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.13	Ensure file deletion events by users are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.14	Ensure events that modify the system's Mandatory Access Controls are collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.15	Ensure successful and unsuccessful attempts to use the chcon command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.16	Ensure successful and unsuccessful attempts to use the setfacl command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.17	Ensure successful and unsuccessful attempts to use the chacl command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.18	Ensure successful and unsuccessful attempts to use the usermod command are recorded (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.19	Ensure kernel module loading unloading and modification is collected (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.20	Ensure the audit configuration is immutable (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.1.3.21	Ensure the running and on disk configuration is the same (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>4.2</b>	<b>Configure Logging</b>		
<b>4.2.1</b>	<b>Configure rsyslog</b>		
4.2.1.1	Ensure rsyslog is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.2	Ensure rsyslog service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.3	Ensure journald is configured to send logs to rsyslog (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.4	Ensure rsyslog default file permissions are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.5	Ensure logging is configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.6	Ensure rsyslog is configured to send logs to a remote log host (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.1.7	Ensure rsyslog is not configured to receive logs from a remote client (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>4.2.2</b>	<b>Configure journald</b>		
<b>4.2.2.1</b>	<b>Ensure journald is configured to send logs to a remote log host</b>		
4.2.2.1.1	Ensure systemd-journal-remote is installed (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.1.2	Ensure systemd-journal-remote is configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4.2.2.1.3	Ensure systemd-journal-remote is enabled (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.1.4	Ensure journald is not configured to receive logs from a remote client (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.2	Ensure journald service is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.3	Ensure journald is configured to compress large log files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.4	Ensure journald is configured to write logfiles to persistent disk (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.5	Ensure journald is not configured to send logs to rsyslog (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.6	Ensure journald log rotation is configured per site policy (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.2.7	Ensure journald default file permissions configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.2.3	Ensure permissions on all logfiles are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
4.3	Ensure logrotate is configured (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5</b>	<b>Access, Authentication and Authorization</b>		
<b>5.1</b>	<b>Configure time-based job schedulers</b>		
5.1.1	Ensure cron daemon is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.2	Ensure permissions on /etc/crontab are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.4	Ensure permissions on /etc/cron.daily are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.7	Ensure permissions on /etc/cron.d are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.8	Ensure cron is restricted to authorized users (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.1.9	Ensure at is restricted to authorized users (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5.2</b>	<b>Configure SSH Server</b>		
5.2.1	Ensure permissions on /etc/ssh/sshd_config are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.2	Ensure permissions on SSH private host key files are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.3	Ensure permissions on SSH public host key files are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.4	Ensure SSH access is limited (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.5	Ensure SSH LogLevel is appropriate (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

5.2.6	Ensure SSH PAM is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.7	Ensure SSH root login is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.8	Ensure SSH HostbasedAuthentication is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.9	Ensure SSH PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.10	Ensure SSH PermitUserEnvironment is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.11	Ensure SSH IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.12	Ensure SSH X11 forwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.13	Ensure SSH AllowTcpForwarding is disabled (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.14	Ensure system-wide crypto policy is not over-ridden (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.15	Ensure SSH warning banner is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.16	Ensure SSH MaxAuthTries is set to 4 or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.17	Ensure SSH MaxStartups is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.18	Ensure SSH MaxSessions is set to 10 or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.19	Ensure SSH LoginGraceTime is set to one minute or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.2.20	Ensure SSH Idle Timeout Interval is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5.3</b>	<b>Configure privilege escalation</b>		
5.3.1	Ensure sudo is installed (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.2	Ensure sudo commands use pty (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.3	Ensure sudo log file exists (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.4	Ensure users must provide password for escalation (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.5	Ensure re-authentication for privilege escalation is not disabled globally (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.6	Ensure sudo authentication timeout is configured correctly (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3.7	Ensure access to the su command is restricted (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5.4</b>	<b>Configure authselect</b>		
5.4.1	Ensure custom authselect profile is used (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.4.2	Ensure authselect includes with-faillock (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5.5</b>	<b>Configure PAM</b>		
5.5.1	Ensure password creation requirements are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.5.2	Ensure lockout for failed password attempts is configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.5.3	Ensure password reuse is limited (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.5.4	Ensure password hashing algorithm is SHA-512 (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>5.6</b>	<b>User Accounts and Environment</b>		

<b>5.6.1</b>	<b>Set Shadow Password Suite Parameters</b>		
5.6.1.1	Ensure password expiration is 365 days or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.1.2	Ensure minimum days between password changes is 7 or more (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.1.3	Ensure password expiration warning days is 7 or more (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.1.4	Ensure inactive password lock is 30 days or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.1.5	Ensure all users last password change date is in the past (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.2	Ensure system accounts are secured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.3	Ensure default user shell timeout is 900 seconds or less (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.4	Ensure default group for the root account is GID 0 (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6.5	Ensure default user umask is 027 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<b>6</b>	<b>System Maintenance</b>		
<b>6.1</b>	<b>System File Permissions</b>		
6.1.1	Audit system file permissions (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.2	Ensure sticky bit is set on all world-writable directories (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.3	Ensure permissions on /etc/passwd are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.4	Ensure permissions on /etc/shadow are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.5	Ensure permissions on /etc/group are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.6	Ensure permissions on /etc/gshadow are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.7	Ensure permissions on /etc/passwd- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.8	Ensure permissions on /etc/shadow- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.9	Ensure permissions on /etc/group- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.10	Ensure permissions on /etc/gshadow- are configured (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.11	Ensure no world writable files exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.12	Ensure no unowned files or directories exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.13	Ensure no ungrouped files or directories exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.14	Audit SUID executables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.1.15	Audit SGID executables (Manual)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

<b>6.2</b>	<b>User and Group Settings</b>		
6.2.1	Ensure password fields are not empty (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.2	Ensure all groups in /etc/passwd exist in /etc/group (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.3	Ensure no duplicate UIDs exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.4	Ensure no duplicate GIDs exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.5	Ensure no duplicate user names exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.6	Ensure no duplicate group names exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.7	Ensure root PATH Integrity (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.8	Ensure root is the only UID 0 account (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.9	Ensure all users' home directories exist (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.10	Ensure users own their home directories (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.11	Ensure users' home directories permissions are 750 or more restrictive (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.12	Ensure users' dot files are not group or world writable (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.13	Ensure users' .netrc Files are not group or world accessible (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.14	Ensure no users have .forward files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.15	Ensure no users have .netrc files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6.2.16	Ensure no users have .rhosts files (Automated)	<input type="checkbox"/>	<input checked="" type="checkbox"/>

# Appendix: Change History

Date	Version	Changes for this version
Mar 29, 2022	1.0.0	Published