

CIS IBM AIX 7.2 Benchmark

v1.0.0 - 09-30-2022

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
Table of Contents	2
Overview	9
Intended Audience.....	10
Consensus Guidance	11
Typographical Conventions.....	12
Recommendation Definitions.....	13
Title	13
Assessment Status.....	13
Automated	13
Manual.....	13
Profile	13
Description.....	13
Rationale Statement	13
Impact Statement.....	14
Audit Procedure.....	14
Remediation Procedure.....	14
Default Value.....	14
References	14
CIS Critical Security Controls® (CIS Controls®).....	14
Additional Information.....	14
Profile Definitions	15
Acknowledgements	16
Recommendations	17
1 Benchmark Organization	17
1.1 Benchmark Principles, Conventions and Assumptions	22
1.2 HOWTO use this benchmark	24
1.3 AIX - Installation methods.....	25
1.3.1 AIX RTE Installation	26
1.3.2 AIX Secure Profile Installation (Basic AIX Security - BAS).....	28
1.3.3 AIX MKSYSB Installation	32
1.4 AIX Patch Management	33
1.5 Summary.....	36
2 Inventory and Control of Assets.....	38
2.1 Collect system configuration regularly (Manual)	41
2.2 Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist) (Manual)	43
2.3 Allowlist Authorized Software and Report Violations (Automated)	46

2.4 Allowlist Authorized Libraries and Report Violations (Automated)	49
2.5 Allowlist Authorized Scripts and Report Violations (Automated)	51
2.6 Enforce Allowlist aka Trusted Execution Checks (Automated).....	53
2.7 Remove Unused Symbolic Links (Automated)	56
2.8 Ensure the Trusted Execution Policies cannot be modified (Automated).....	58
3 Data Protection	59
3.1 Encryption: File System Level (EFS) (Automated)	60
3.2 Encryption: Logical Volume (ELV) (Manual)	64
3.3 Ensure default user umask is 027 or more restrictive (Automated).....	66
3.4 Remove group write permission from default groups - exceptions must be in TSD and audit (Manual).....	68
3.5 Application Data with requirement for world writable directories (Manual)	70
3.6 Ensure there are no world writable files - exceptions must be in TSD and audit (Manual)	72
3.7 Ensure there are no 'staff' writable files - exceptions must be in TSD and audit (Manual).....	74
3.8 Ensure all files and directories are owned by a user (uid) and assigned to a group (gid) (Automated).....	76
4 Secure Configuration of Enterprise Assets and Software	78
4.1 System Boot	79
4.1.1 Boot phase: /etc/inittab	80
4.1.1.1 Disable writesrv (Automated)	81
4.1.1.2 Disable ntalk/talk (Automated)	83
4.1.1.3 dt (Automated)	85
4.1.1.4 piobe (Automated).....	86
4.1.1.5 qdaemon (Automated)	87
4.1.1.6 rc.nfs (Automated).....	88
4.1.1.7 cas_agent (Automated).....	90
4.1.2 Boot phase: /etc/rc.tcpip: daemons	92
4.1.2.1 inetd - aka Super Daemon (Automated).....	93
4.1.2.2 aixmibd (Automated)	95
4.1.2.3 dhcpcd (Automated).....	97
4.1.2.4 dhcprd (Automated)	99
4.1.2.5 dhcpsd (Automated).....	101
4.1.2.6 dpid2 (Automated).....	103
4.1.2.7 gated (Automated)	105
4.1.2.8 hostmibd (Automated).....	107
4.1.2.9 mrouted (Manual).....	109
4.1.2.10 named (Automated)	111
4.1.2.11 portmap (Manual).....	113
4.1.2.12 routed (Automated)	116
4.1.2.13 rwhod (Automated).....	118
4.1.2.14 sendmail (Automated)	120
4.1.2.15 snmpd (Automated).....	122
4.1.2.16 snmpmibd (Automated).....	124
4.1.2.17 timed (Automated).....	126
4.1.3 Boot phase: IPv6	128
4.1.3.1 autoconf6 (Automated).....	129
4.1.3.2 ndpd-host (Automated)	131
4.1.3.3 ndpd-router (Automated).....	134
4.1.4 NFS	136
4.1.4.1 NFS - de-install NFS client (Automated)	137
4.1.4.2 NFS - de-install NFS server (Automated).....	138
4.1.4.3 NFS - enable both nosuid and nodev options on NFS client mounts (Automated)	139
4.1.4.4 NFS - localhost removal (Automated)	141

4.1.4.5 NFS - restrict NFS access (Automated)	143
4.1.4.6 NFS - no_root_squash option (Automated).....	145
4.1.4.7 NFS - secure NFS (Automated)	147
4.1.5 Inetd Services	149
4.1.5.1 bootps (Automated).....	150
4.1.5.2 chargen (Automated)	152
4.1.5.3 comsat (Automated).....	154
4.1.5.4 daytime (Automated).....	156
4.1.5.5 discard (Automated).....	157
4.1.5.6 echo (Automated).....	158
4.1.5.7 exec (Automated).....	159
4.1.5.8 finger (Automated)	160
4.1.5.9 ftp (Automated)	161
4.1.5.10 imap2 (Automated).....	162
4.1.5.11 instsrv (Automated)	163
4.1.5.12 klogin (Automated).....	164
4.1.5.13 kshell (Automated)	166
4.1.5.14 login (Automated).....	167
4.1.5.15 netstat (Automated).....	168
4.1.5.16 ntalk (Automated).....	170
4.1.5.17 pcnfsd (Automated).....	171
4.1.5.18 pop3 (Automated)	172
4.1.5.19 rexd (Automated)	173
4.1.5.20 rquotad (Automated)	175
4.1.5.21 rstatd (Automated)	176
4.1.5.22 rusersd (Automated)	178
4.1.5.23 rwalld (Automated).....	179
4.1.5.24 shell (Automated)	180
4.1.5.25 sprayd (Automated).....	181
4.1.5.26 xmquery (Automated).....	182
4.1.5.27 talk (Automated).....	183
4.1.5.28 telnet (Automated).....	184
4.1.5.29 tftp (Automated)	186
4.1.5.30 time (Automated).....	187
4.1.5.31 uucp (Automated).....	188
4.2 Network Options: '/usr/sbin/no'	189
4.2.1 clean_partial_conns (Automated)	190
4.2.2 bcastping (Automated).....	191
4.2.3 directed_broadcast (Automated).....	192
4.2.4 icmpaddressmask (Automated)	193
4.2.5 ipforwarding (Automated).....	194
4.2.6 ipignoreredirects (Automated).....	195
4.2.7 ipsendredirects (Automated)	196
4.2.8 ipsrcrouteforward (Automated).....	197
4.2.9 ipsrcrouterrecv (Automated).....	198
4.2.10 ipsrcroutesend (Automated).....	199
4.2.11 ip6srcrouteforward (Automated).....	200
4.2.12 nfs_use_reserved_ports (Automated).....	201
4.2.13 nonlocsrcroute (Automated).....	202
4.2.14 sockthresh (Automated)	203
4.2.15 tcp_pmtu_discover (Automated)	204
4.2.16 tcp_tcpsecure (Automated)	205

4.2.17 udp_pmtu_discover (Automated)	206
4.2.18 ip6forwarding (Automated)	207
4.3 Implement and Manage a Firewall (bos.net.ipsec)	208
4.3.1 Ensure that IP Security is available (Automated)	209
4.3.2 Ensure loopback traffic is blocked on external interfaces (Automated)	211
4.3.3 Ensure that IPsec filters are active (Automated)	212
4.4 Remove or Disable Weak/Defunct Network Services	213
4.4.1 NIS.....	214
4.4.1.1 NIS - de-install NIS client (Automated).....	215
4.4.1.2 NIS - de-install NIS server (Automated)	216
4.4.1.3 NIS - remove NIS markers from password and group files (Automated).....	217
4.4.1.4 NIS - restrict NIS server communication (Automated).....	218
4.4.2 Remote command lockdown (Automated)	220
4.4.3 Removal of entries from /etc/hosts.equiv (Automated)	221
4.4.4 Removal of .rhosts and .netrc files (Automated)	222
4.4.5 Remote daemon lockdown (Automated)	223
4.5 Standard Services and Applications	225
4.5.1 Common Desktop Environment (CDE)	226
4.5.1.1 CDE - de-installing CDE (Automated)	227
4.5.1.2 /etc/inetd.conf - cmsd (Automated)	229
4.5.1.3 CDE - disabling dtlogin (Automated).....	230
4.5.1.4 /etc/inetd.conf - dtspc (Automated)	232
4.5.1.5 CDE - sgid/suid binary lockdown (Automated).....	233
4.5.1.6 CDE - remote GUI login disabled (Automated)	234
4.5.1.7 CDE - screensaver lock (Automated).....	236
4.5.1.8 CDE - login screen hostname masking (Automated)	238
4.5.1.9 CDE - /etc/dt/config/Xconfig permissions and ownership (Automated)	240
4.5.1.10 CDE - /etc/dt/config/Xservers permissions and ownership (Automated)	241
4.5.1.11 CDE - /etc/dt/config/*Xresources permissions and ownership (Automated).....	242
4.5.2 FTPD	243
4.5.2.1 FTPD: Disable root access to ftpd (Automated)	244
4.5.2.2 FTPD: Display acceptable usage policy during login (Automated)	245
4.5.2.3 FTPD: Prevent world access and group write to files (Automated)	247
4.5.3 OpenSSH.....	249
4.5.3.1 OpenSSH: Minimum version is 8.1 (Automated).....	250
4.5.3.2 OpenSSH: Remove /etc/shosts.equiv and /etc/rhosts.equiv (Automated)	252
4.5.3.3 OpenSSH: Remove .shosts files (Automated)	254
4.5.3.4 sshd_config: Restrict users and groups allowed access via OpenSSH (Manual)	255
4.5.3.5 sshd_config: PermitRootLogin is 'prohibit-password' or 'no' (Automated).....	258
4.5.3.6 sshd_config: Banner exists and message contains "Only authorized users allowed" (Automated)	261
4.5.3.7 sshd_config: HostbasedAuthentication is 'no' (Automated).....	263
4.5.3.8 sshd_config: IgnoreRhosts is 'yes' or 'shosts-only' (Automated)	266
4.5.3.9 sshd_config: PermitEmptyPasswords is 'no' (Automated)	269
4.5.3.10 sshd_config: LogLevel is 'INFO' or 'VERBOSE' (Automated)	271
4.5.3.11 sshd_config: sftp-server arguments include '-u 027 -f AUTH -l INFO' (Automated)	273
4.5.3.12 sshd_config: MaxAuthTries is '4' (Automated)	275
4.5.3.13 sshd_config: PermitUserEnvironment is 'no' (Automated)	276
4.5.3.14 sshd_config: Use Conditional exception(s). (Manual)	278
4.5.3.15 sshd_config, ssh_config: KexAlgorithms (Automated)	281
4.5.3.16 sshd_config, ssh_config: Ciphers (Automated)	284
4.5.3.17 sshd_config, ssh_config: MACs - Message Authentication Codes (Automated)	287

4.5.3.18 sshd_config, ssh_config: ReKeyLimit (Automated)	290
4.5.4 Sendmail Configuration.....	292
4.5.4.1 /etc/mail/sendmail.cf - Hide sendmail version information (Automated)	293
4.5.4.2 /etc/mail/sendmail.cf - PrivacyOptions (Automated)	295
4.5.4.3 /etc/mail/sendmail.cf - DaemonPortOptions (Automated)	297
4.5.4.4 /etc/mail/sendmail.cf - access control (Automated)	299
4.5.4.5 /var/spool/clientmqueue - access control (Automated).....	300
4.5.4.6 /var/spool/mqueue - access control (Automated)	301
4.5.5 SNMP Configuration	302
4.5.5.1 SNMP - disable private community string (Automated)	303
4.5.5.2 SNMP - disable system community string (Automated)	304
4.5.5.3 SNMP - disable public community string (Automated)	305
4.5.5.4 SNMP - disable Readwrite community access (Automated)	306
4.5.5.5 SNMP - restrict community access (Automated)	308
4.5.6 Uninstall snmp (Automated)	309
4.5.7 Uninstall/Disable sendmail (Automated)	310
4.6 Login Controls	312
4.6.1 /etc/security/login.cfg - logintimeout (Automated)	313
4.6.2 /etc/security/login.cfg - logindelay (Automated)	314
4.6.3 herald (logon message) (Automated)	315
4.6.4 loginretries (Automated)	316
4.6.5 Unattended terminal session timeout is 900 seconds (or less) (Manual)	318
4.7 Trusted Files and Directories	320
4.7.1 Trusted Directories	321
4.7.1.1 Home directory must exist (Manual).....	322
4.7.1.2 Home directory must be owned by account, or special account (Manual)	325
4.7.1.3 Home directory: write access restricted to 'owner' (Automated).....	328
4.7.1.4 AUDIT subsystem: /audit and /etc/security/audit (Automated)	332
4.7.1.5 SECURITY Subsystems: /etc/security (Automated)	334
4.7.1.6 /var/adm/ras (Automated)	336
4.7.1.7 /var/adm/sa (Automated).....	337
4.7.1.8 /var/spool/cron/crontabs (Automated)	338
4.7.1.9 Ensure all directories in root PATH deny write access to all (Automated).....	340
4.7.1.10 Ensure root user has a dedicated home directory (Automated)	343
4.7.1.11 /etc/security/audit (Automated)	345
4.7.2 Trusted Files	346
4.7.2.1 New configuration file for sendmail /etc/mail/submit.cf (Manual)	347
4.7.2.2 Verify Trust of suid, sgid, acl, and trusted-bit files and programs (Manual).....	348
4.7.2.3 crontab entries - owned by userid (Automated)	350
4.7.2.4 Home directory configuration files (Automated)	353
4.7.2.5 /smit.log (Automated)	355
4.7.2.6 /etc/group (Automated)	356
4.7.2.7 /etc/inetd.conf (Automated)	357
4.7.2.8 /etc/motd (Automated).....	359
4.7.2.9 /etc/passwd (Automated)	360
4.7.2.10 /etc/ssh/ssh_config (Automated)	361
4.7.2.11 /etc/ssh/sshd_config (Automated)	363
4.7.2.12 /var/adm/cron/at.allow (Automated)	366
4.7.2.13 /var/adm/cron/cron.allow (Automated)	367
4.7.2.14 /var/ct/RMstart.log (Automated)	368
4.7.2.15 /var/adm/cron/log (Automated).....	370
4.7.2.16 /var/tmp/dpid2.log (Automated)	371

4.7.2.17 /var/tmp/hostmibd.log (Automated)	372
4.7.2.18 /var/tmp/snmpd.log (Automated)	373
4.8 Trusted Execution (TE).....	374
4.8.1 TE - implementation (Automated)	375
4.9 Ensure root access is controlled (Automated).....	378
4.10 Disable core dumps (Automated).....	381
4.11 Remove current working directory from default /etc/environment PATH (Automated)	383
4.12 Lock historical users (Automated)	385
4.13 Remove current working directory from root's PATH (Automated).....	387
4.14 Configuration: /etc/motd (Automated)	389
5 Account Management.....	391
5.1 Establish and Maintain an Inventory of Accounts	393
5.1.1 Maintain Account Passwords	395
5.1.1.1 histexpire (Automated)	396
5.1.1.2 histsize (Automated)	397
5.1.1.3 minage (Automated).....	399
5.1.2 All accounts must have a hashed password (Automated).....	401
5.1.3 All usernames and UIDs must be unique (Automated)	403
5.1.4 All group names and GIDs must be unique (Automated)	405
5.1.5 Establish and Maintain an Inventory of Administrator accounts (Manual)	408
5.1.6 Establish and Maintain an Inventory of User Accounts (Manual)	410
5.2 Use Unique Passwords	412
5.2.1 Ensure new passwords are controlled by password attributes (disable NOCHECK) (Automated) ..	414
5.2.2 pwd_algorithm (Automated)	416
5.2.3 Ensure passwords are not hashed using 'crypt' (Automated)	418
5.2.4 Ensure password policy is enforced for all users (Automated).....	420
5.2.5 minlen (Automated).....	422
5.2.6 mindiff (Automated)	424
5.2.7 minalpha (Automated).....	426
5.2.8 minother (Automated)	427
5.2.9 maxrepeats (Automated).....	428
5.2.10 mindigit (Automated).....	430
5.2.11 minloweralpha (Automated)	431
5.2.12 minupperalpha (Automated).....	432
5.2.13 minspecialchar (Automated)	433
5.3 System Accounts	434
5.3.1 adm (Automated)	435
5.3.2 bin (Automated)	436
5.3.3 daemon (Automated)	437
5.3.4 guest (Automated)	438
5.3.5 lpd (Automated)	440
5.3.6 nobody (Automated).....	441
5.3.7 nuucp (Automated)	442
5.3.8 sys (Automated)	443
5.3.9 uucp (Automated)	444
5.3.10 Ensure System Accounts cannot access system using ftp. (Automated).....	445
5.4 User Attributes for Active Processes	447
5.5 Disable Dormant Accounts.....	448
5.6 maxage (Automated)	449
5.7 maxexpired (Automated).....	451
6 Access Control Management.....	452

6.1 Legacy RBAC mechanisms	453
6.1.1 Create baseline of executables that elevate to a different GUID (Not scored) (Manual)	454
6.1.2 Create baseline of executables that require a specific group for elevation to a different EUID (not scored) (Manual)	456
6.1.3 Create baseline of executables that elevate directly to a new EUID (not scored) (Manual)	460
6.2 RBAC managed privilege escalation	465
6.2.1 Privilege escalation: enhanced RBAC (Manual)	466
6.3 SUDO managed privilege escalation	468
6.3.1 Privilege escalation: sudo (Manual)	469
6.3.2 Ensure sudo logging is active (Manual)	471
6.3.3 Ensure sudo commands use pty (Manual)	473
6.4 Adding authorized users in at.allow (Manual)	474
6.5 Services - at access is root only (Automated)	476
6.6 Adding authorised users in cron.allow (Automated)	478
6.7 Services - crontab access is root only (Automated)	480
7 Continuous Vulnerability Management	482
7.1 Use FLRT regularly (Manual)	483
7.2 Use FLRTVC regularly (Automated)	485
8 Audit Log Management	486
8.1 Syslog	487
8.1.1 Configuring syslog - local logging (Manual)	488
8.1.2 Configuring syslog - remote logging (Automated)	490
8.1.3 Configuring syslog - remote messages (Automated)	492
8.2 AIX Auditing (Manual)	494
Appendix: Summary Table	498
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	513
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	515
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	520
Appendix: CIS Controls v7 Unmapped Recommendations	525
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	530
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	535
Appendix: CIS Controls v8 IG 3 Mapped Recommendations	542
Appendix: CIS Controls v8 Unmapped Recommendations	549
Appendix: Change History	552

Overview

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

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

This document, Security Configuration Benchmark for AIX 7.2, provides prescriptive guidance for establishing a secure configuration posture for AIX version 7.2 running on the Power Systems platform. This guide was tested against AIX 7.2 installed from IBM base installation media.

The account aka user executing this benchmark requires **root** (direct login, su, sudo or RBAC) access to system privileges are required by many of the operations presented here. Non-root access may not be able to access certain areas of the system during and/or after remediation. Further, we advise that *prior to execution* the commands and scripts included in this benchmark as well as the PATH of the (root) user are verified.

To obtain the latest version of this guide, please visit

<https://learn.cisecurity.org/benchmarks>. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel, who plan to develop, deploy, assess, or secure solutions that incorporate AIX 7.2 on the Power Systems platform.

Some skill with AIX system administration tools is expected. Most recommendations *Audit* and *Remediation* steps have been written using AIX system administration tools.

Skilled use of AIX `smit` is **recommended**. Besides providing `${HOME}/smit.log` as a record of steps taken the file `${HOME}/smit.scripts` and/or F6 panel can help with implementing complex remediation and/or audit scripts that can be executed directly. Skilled use of `vi` (or other editor already installed) is needed in order to implement some of the configuration changes (when we have not yet found a `SMIT` based command dialog or consider it more prudent to create a script using hints from SMIT and/or it is not part of AIX system administration tools. In general we always try to use an AIX command rather than a text based editor (e.g., `vi`) - as a best practice policy. One example is using the AIX command `chsec` to modify files in the directory `/etc/security` rather than using a text editor.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></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.
Note	Additional information or caveats

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Level-1 Benchmark recommendations are intended to:

- be practical and prudent,
- provide a clear security benefit
- do not inhibit the utility of the technology beyond acceptable means

- **Level 2**

Level-2 Benchmark recommendations 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

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 AIX 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 AIX benchmarks.

Author

Michael Felt

Contributor

Graham Eames

Xiaohan Qin

Bhargavi Reddy

Editor

Eric Pinnell

Justin Brown

Recommendations

1 Benchmark Organization

This benchmark provides security configuration guidance for the AIX Operating System. The scope of the guide is applicable to AIX 7.2 and above. The recommendations in this guide have been explicitly tested on AIX 7.2 TL2 and TL5.

Key Difference with AIX 7.1 (v1.1.0 and v2.0.0) benchmarks

The *key* difference is that organization of the recommendations is much more "*top-down*" - where **TOP** is the CIS Controls, rather than the historical "*bottom-up*" - where **BOTTOM** is AIXPERT process of hardening and the recommendations following a rather arbitrary grouping..

Further, the new document layout is a first step to developing a unified AIX security benchmark - that is, the recommendations are applicable not only for AIX 7.2, but also for AIX 7.1 and AIX 7.3. In support of this, a new (final) AIX 7.1 benchmark (v2.1.0) is being released in parallel with this document - with it's table of contents aka recommendation organizations more aligned with CIS controls.

The table of contents - at the chapter level follows the CIS Controls V8 table of contents as closely as possible. The sections following this opening section Benchmark Organization are ordered following the CIS Controls v8.

Within these chapters some recommendations are organized around an AIX operating system technology or service. When there are fewer than three recommendations for such an OS technology or service the recommendations are located under the base CIS Control topic.

Yet another difference: we have added recommendations. We hope, especially in the area of data protection and system hardening, to encourage IBM to follow our lead in changing many of AIX's system defaults re: file and directory permissions. We feel that the defaults (permitting group *write*) are no longer in-line with common practice for `system` and/or `cyber` security` practices.

CIS Controls - v7 and v8 Overview

CIS Controls reflect the combined knowledge of experts from every part of the IT ecosystem (companies, governments, individuals) in many roles (threat responders, threat analysts, technicians, IT operators and defenders, users, policy makers, auditors, etc.. Working, better collaborating, together we, collectively develop CIS controls.

Ideally all recommendations *should* have a CIS Control (version 7 and/or version 8) reference. This is to allow users who are still committed to CIS Controls v7 to use the document while also helping those customers prepare for migration to CIS controls v8. As stated above, the organization of the benchmark follows the published **CIS Controls version 8 v1.0.0** document organization. (Some recommendations have neither CIS v7 nor CIS v8 controls tied to the recommendation. For a list of these recommendations see the respective appendix.)

CIS Controls (v8) Design Principles

- Offense Informs Defense
 - Controls are selected, dropped, and prioritized based on data, and on specific knowledge of Attacker behavior and how to stop it
- Focus
 - Avoid adding “good things to do”
 - Don’t be tempted to solve every security problem, stick to the spirit of “Critical” Security Controls
- Feasible
 - All Sub-Controls (Safeguards) must be specific and practical to implement
- Measurable
 - All Controls, especially for Implementation Group 1 must be measurable
 - Simplify or remove ambiguous language to avoid inconsistent interpretation
 - There is a place for self-attestation
 - Some Safeguards may have a threshold
- Align
 - Create and demonstrate “peaceful co-existence” with other governance, regulatory, process management schemes, framework, and structures
 - Cooperate with and point to existing, independent standards and security recommendations where they exist, e.g., National Institute of Standards and Technology® (NIST®), Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), ATT&CK, Open Web Application Security Project® (OWASP®)

CIS Defense Model (CDM) version 2

Enterprises that have, or want to, adopt *CIS Critical Security Controls* (full name of CIS Controls) repeatedly asked for guidance - what to do first? To provide guidance on how to use CIS Controls the CIS experts (including community experts) classified the controls into three Implementation Groups (IGs). These groups are based on their difficulty and cost to implement.

A second question - "How effective are the CIS Controls?". The CDM (CIS Defense Model) was created (and now at version 2) to help answer that question - especially with regard to the 5 (five) most prevalent attack types. Download <https://workbench.cisecurity.org/files/3524/download/4422> for the latest version of CDM.

Within CDM the focus is on two concepts: *security function* and *security value*. *Security function* is best defined as the ability of a CIS Safeguard to defend against ATT&CK (MITRE ATT&CK framework) (sub-)techniques - independent of a specific attack type. *Security function* provides a foundation to allow analysis as *security value*. *Security value* is defined as the benefit a CIS safeguard provides as defense against one or more attack types.

Implementation Groups

Starting with CIS Controls Version 7.1 *Implementation Groups* (IGs) are used to prioritize implementation of recommendations. Each IG identifies a subset of CIS Controls. Each IG builds on the previous one: IG2 includes IG1, and IG3 includes all CIS Safeguards in IG1 and IG2.

- IG1 - Implementation Group 1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

- IG2 - Implementation Group 2 (Includes IG1)

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

- IG3 - Implementation Group 3 (Includes IG1 & IG2)

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

Additional Information

The latest **CDM** (see above) reaffirmed and strengthened that **IG1** provides a viable defense against the top five attacks (note: this is not AIX specific, but enterprise wide including (back-end) servers including AIX.)

For CDM v2.0, the top five attack types are: Malware, Ransomware, Web Application Hacking, Insider Privilege and Misuse, and Target Intrusions.

Running the benchmark

As stated above, the benchmark `document` is organized into sections based on major *CIS Controls Sections*. Within these sections there are recommendations and sub-sections with recommendations. There is no attempt to organize the recommendations as a sequence that will harden an AIX server in a single pass. In other words, do not expect an `audit run` based on the document order to succeed in a single pass.

Security Management is an on-going process

Having completed all the recommendations in the benchmark does not mean you 'are done'. A very important - next step - that is not part of a platform benchmark (i.e., recommendation) is using the security systems you have configured - especially with regard to reviewing logs. By reviewing logs you will be able to make adjustments to settings to continually improve your overall security. CIS appreciates any information you can share - as a proposed change, ticket or discussion - so that we can improve the next release of this benchmark.

1.1 Benchmark Principles, Conventions and Assumptions

This benchmark provides security configuration guidance for use during the configuration of the AIX 7.2 Operating System. The recommendations are organized into chapters based on `CIS Controls v8`. The chapters are organized into sub-sections, as needed, by AIX BOS OS technology and/or standard services.

Guiding principles

CIS Controls v8 developed a number of `design principles` for their development. Where applicable these design principles were copied or borrowed to decide what is retained or added to the AIX Benchmark recommendations.

- Recommendations are selected, dropped, and prioritized based on data, and on specific knowledge of Attacker behavior and how to stop it
- Avoid adding “good things to do”
- Don’t be tempted to solve every security problem, stick to the spirit of “Critical” Security Controls
- All Sub-Controls (Safeguards) must be specific and practical to implement
- All Controls, especially for Implementation Group 1 must be measurable
- Simplify or remove ambiguous language to avoid inconsistent interpretation

Section Naming and Recommendation Ordering

Most of the Chapters are named after a specific CIS Control, e.g., **Data Protection**. Some have a more generic title to combine multiple CIS Controls, e.g., the CIS Controls `01: Inventory and Control of Enterprise Assets` and `02: Inventory and Control of Software Assets` are combined in the section: **Inventory and Control of Assets**.

Implementation of Recommendations is not linear

Since recommendations are organized by Controls there is no expectation that implementation of the controls will be a process of starting at page 1 and working through to the end. Secure systems is not a linear by-product of a handbook or benchmark.

Scenarios

This benchmark envisions two scenarios: an existing system that needs to be certified or compared against a corporate standard and hardening and deploying a fresh installation.

Benchmark scope and prerequisites

- This benchmark is written for securing fully virtualized virtual machines (VM). On IBM POWER Systems VM's are also called Logical Partitions (LPAR) or as, simply, partitions.
- Fully virtualized PowerVM LPARs usually don't have any associated hardware devices. Recommendations for securing hard devices are removed as irrelevant. Even if you can use the benchmark to proof security on non-virtualized LPARs or on hardware (baremetal) systems remember that this benchmark does not include recommendations for securing devices and hardware.
- This benchmark is not approved for AIX on other types of hardware or virtualization technologies, such as KVM. Virtualization using PowerVM and Frame Management using an HMC is assumed.

Assumptions

In other words - AIX administrators do not have physical access to the POWER frame or managed system. Any physical access is exceptional and is managed by physical room controls and/or is exclusive to service providers (e.g., IAAS) or data center (server room) controls.

1.2 HOWTO use this benchmark

Again, the benchmark envisions two scenarios:

1. an existing system that needs to be certified or compared against a corporate standard and
2. hardening and deploying a fresh installation.

Fresh Installation - better for first-time users

While the benchmark is suitable for both scenario we recommend that both first-time users and experienced users (though using *THIS* benchmark for the first time) work from a fresh install of AIX and work through the recommendations is the better *Initial Approach* to developing an implementation plan for hardening an AIX image.

Therefore, the recommended approach of using this guide is to install a vanilla AIX image, via NIM or the AIX product DVD's, followed by the recommendations detailed in this guide and any other corporate standardization i.e. software installation, filesystem and user creation.

Once this initial implementation is complete you will have a base image that can be further deployed via a cloning process based on a `mksysb` backup of the system. For example, the `mksysb` image could be deployed via NIM for any subsequent operating system deployments. Additionally, this system image could be prepared for deployment using PowerVC. Either process (using NIM or PowerVC) would provide a standard build mechanism, ensuring compliance to company standards as well as the best practice recommendations detailed in this benchmark.

Additionally, you should have, in parallel, developed a process for verifying and hardening existing systems - whether they be public or private cloud based, or managed 'traditionally'.

By beginning with a new install you will have safe, secure, trusted environment for developing any additional (audit/update) scripts that you can use on existing systems.

1.3 AIX - Installation methods

The benchmark development is based on a fresh AIX installation from base media.

Below shows three methods to install AIX.

- AIX RTE (standard): used to install a generic, not-secured, system with AIX. The steps are identical whether using a NIM server, from DVD media or VIOS virtual optical mounted ISO images.
- AIX RTE (BAS) aka Basic AIX Security: the same process is followed except the **BAS** security profile is chosen. This will modify the base install so that it complies with the pre-defined security profile. **NOTE:** This profile is the base for the [AIX Security Profile Evaluation Assurance](#).
- AIX MKISYSB Installation: the key difference is that the base install is not performed from installation media but from a prepared image (often called a gold image). A security profile **cannot** be selected. Instead, these images can be *pre-hardened* according to enterprise policies. Using pre-hardened *mksysb* images greatly enhances the deployment process. After the image is installed the new system verifies it has all device drivers it needs - adding anything missing based on the new environment.

All three install methods have methods for installing extra software bundles.

1.3.1 AIX RTE Installation

Outlines the process of a fresh install where the filesets are installed individually.

AIX Installation - RTE mode

- This example is to assist you with setting up an AIX system for the "First Time Scenario". This can also be used to build a new so-called "gold image".
- Within the AIX Base Operating System Installation Menus it is recommended that the following options are selected:

```
Security Models

Type the number of your choice and press Enter.

1. Trusted AIX..... no
2. Other Security Options (Trusted AIX and Standard)
   Security options vary based on choices.
   LAS, SbD, BAS/CCEVAL, TCB

Standard Security Options

Type the number of your choice and press Enter.

1. Secure by Default..... no
2. BAS and EAL4+ Configuration Install..... no
3. Trusted Computing Base Install..... no

Install Options

1. Graphics Software..... no
2. System Management Client Software..... no
3. Create JFS2 File Systems..... yes
4. Enable System Backups to install any system..... no *
   (Installs all devices)
```

- no need to install all devices in a virtual machine aka LPAR; for bare metal deployments, choose yes.

```
Install More Software

1. Firefox (Firefox CD)..... no
2. Kerberos_5 (Expansion Pack)..... no **
3. Server (Volume 2)..... no
```

** Install Kerberos - can be now, or postponed - only when you need it

Installation Summary

```
Overwrite Installation Summary

Disks:  hdisk0
Cultural Convention:  en_US
Language:  en_US
Keyboard:  en_US
JFS2 File Systems Created:  yes
Graphics Software:  no
System Management Client Software:  no
Enable System Backups to install any system:  no
Selected Edition:  express

Optional Software being installed:

>>> 1  Continue with Install
```

- JFS2 filesystems (default)
- Enable System Backups to install any system = no *

* This is to ensure that all device drivers are installed into the operating system image for deploying to different server hardware configurations. When deploying to virtual environments additional device drivers are not needed. For deployments intended for so-called bare-metal installing all devices is recommended.

Also - do **not** consider selecting the following option)

- Secure By Default = no*

* This option performs a minimal software installation, and removes all clear password access such as `telnet` and `rlogin`. Secure by Default (SbD) also applies the AIX Security Expert high-security settings. Once installed the expansion pack cd is prompted for as SSH and SSL are installed for secure remote system accessibility. If the SbD installation option is selected through NIM, the system administrator should ensure that the relevant NIM `lpp_source` has the `openssh` and `openssl` images in place.

1.3.2 AIX Secure Profile Installation (Basic AIX Security - BAS)

AIX Installation - Using security profiles

In the classic RTE installation the answer is `no` to all three choices of a `security profile`. The first and last choices are not covered by the benchmark (*Secure by Default, Trusted AIX*). The first was a great idea, but the implementation complicates AIX (security and) update management to such a degree that the *author* does not recommend it. The latter, *Trusted AIX*, also known as LS (labeled security) installs a system that is not well served by this benchmark. This leaves one security profile *useable* for base installation: BAS (which might also later be labeled EAL4+ - that is the security assurance label that is being certified). See below for differences between *generic* (i.e., no profile) and **BAS** installation as the starting point.

Review

- Security profile is a AIX product that specifies security requirements for general-purpose operating systems in networked environments. This profile establishes the requirements necessary to achieve the security objectives of the Target of evaluation (TOE) security function and its environment. Security profile contains a base package and several extended packages. Products that are related to Security profile base package support are Identification and Authentication, Discretionary Access Control (DAC), Auditing, Cryptographic Services, Management of Security Mechanisms, and Trusted Channel communications. Security profile includes additional, optional packages for Labeled Security, Integrity Verification, Advanced Audit, General Purpose Cryptography, Advanced Management, Extended Identification and Authentication, Trusted Boot, and Virtualization.
- System administrators can install a system with the Base AIX Security (BAS) and Evaluation Assurance Level 4+ (EAL4+) option or Labeled AIX Security (LAS) and Evaluation Assurance Level 4+ (EAL4+) during a base operating system (BOS) installation. A system with these options has restrictions on the software that is installed during BOS installation, plus network access is restricted.
- Above is taken from AIX Security.pdf

BAS (Basic AIX Security) Installation

During the base installation the menu's choose the following path:

```
Security Models

Type the number of your choice and press Enter.

1. Trusted AIX..... no
2. Other Security Options (Trusted AIX and Standard)
   Security options vary based on choices.
   LAS, SbD, BAS/CCEVAL, TCB
```

- Choose option 2

```
Standard Security Options

Type the number of your choice and press Enter.

1. Secure by Default..... no
2. BAS and EAL4+ Configuration Install..... yes
3. Trusted Computing Base Install..... no
>>> 0 Continue to more software options.

88 Help ?
99 Previous Menu

>>> Choice [0]:
```

- Above shows after having selecting BAS as the `Security Profile` to install. Press `Enter` to proceed.
- Installation of graphics software (client) is optional. In the example here, it is being installed.
- At the summary screen note the line starting with `Security:` and compare that with above.

```
Disks: hdisk0
Cultural Convention: C
Language: C
Keyboard: C
JFS2 File Systems Created: yes
Graphics Software: yes
System Management Client Software: no
Enable System Backups to install any system: no
Selected Edition: express
Security: BAS and EAL4+ Technology
```

```
>>> 1 Continue with Install
```

AIX BAS preparation

- When the BAS/EAL4+ option is selected, the contents of the `/usr/sys/inst.data/sys_bundles/CC_EVAL.BOS.autoi` installation bundle are installed.
- You can optionally select to install the graphics software bundle and the documentation services software bundle with the BAS/EAL4+ option selected. If you select the Graphics Software option with the BAS/ EAL4+ option, the contents of the `/usr/sys/inst.data/sys_bundles/CC_EVAL.Graphics.bnd` software bundle are installed. If you select the Documentation Services Software option with the BAS/ EAL4+ option, the contents of the `/usr/sys/inst.data/sys_bundles/ CC_EVAL.DocServices.bnd` software bundle are installed.
- The following changes are made to the default configuration:

- RBAC is automatically enabled when this option is selected
- Remove /dev/echo from the /etc/pse.conf file.
- Instantiate streams devices.
- Allow only root to access removable media.
- Remove non-CC entries from the inetd.conf file.
- Change various file permissions.
- Register symbolic links in the sysck.cfg file.
- Register devices in the sysck.cfg file.
- Set default user and port attributes.
- Configure the doc_search application for browser use.
- Remove httpdlite from the inittab file.
- Remove writesrv from the inittab file.
- Remove mkatmpvc from the inittab file.
- Remove atmsvcd from the inittab file.
- Disable snmpd in the /etc/rc.tcpip file.
- Disable hostmib in the /etc/rc.tcpip file.
- Disable snmpmib in the /etc/rc.tcpip file.
- Disable aixmib in the /etc/rc.tcpip file.
- Disable muxatmd in the /etc/rc.tcpip file.
- NFS port (2049) is a privileged port.
- Add missing events to the /etc/security/audit/events file.
- Ensure that the loopback interface is running.
- Create synonyms for /dev/console.
- Enforce default X-server connection permissions.
- Change the /var/docsearch directory so that all files are world-readable.
- Add Object Data Manager (ODM) stanzas to set the console permissions.
- Set permissions on BSD-style ptys to 000.
- Disable .netrc files.
- Add patch directory processing.

1.3.3 AIX MKSYSB Installation

Rather than perform an installation from Installation media an image can be prepared and saved in a backup file format (bff). When the backup is the `rootvg` volume group these are known as `system images`. They are created using the command `mksysb` (make system backup). These images are, by design, meant to be used for quick deployment and cloning - as the installation provides a process for adding any missing device drivers - when the target system is not an exact clone or copy of the system the image was created on.

We expect (assume) that an experienced AIX administrator is well aware of the steps involved in creating and applying (i.e., installing) an system image made using `mksysb` and/or a third-party product designed for system image backup and recovery.

1.4 AIX Patch Management

The recommendations that follow are not a one-time test or validation. Maintaining System Integrity is a continuous process. The sections [CIS Controls V7, Section 3: Continuous Vulnerability Management](#) and [CIS Controls V8, Section 7: Continuous Vulnerability Management](#) highlight how important regular (they say automated) patching and updating are for maintaining system integrity.

No Security without regular updates/patching

At the time of writing this benchmark there is a white paper [AIX Service Strategy and Best Practices](#) that addresses this issue. In this paper you can find short descriptions of core concepts surrounding AIX Service Strategy. If any of these concepts below are not familiar - we recommend a review of the white paper.

- AIX Level Naming
 - Releases Shipped approximately every 4 years
 - Technology Levels Technology Levels contain software enhancements, new hardware exploitation, and defect fixes.

New Technology Levels generally ship annually for the latest AIX release and every other year for older releases.

- Service Packs Service Packs contain fixes for defects impacting customers, fixes for critical defects found in internal testing, and can contain enablement for new hardware.

New Service Packs are released approximately twice a year for each TL that is still active for Service Pack Support.

- Build Sequence Identifier
- Planned Maintenance and Service Pack Updates When updating using Service Packs pay attention to the release date. The Fix Level Recommendation Tool (FLRT) should be used to plan the update. IBM will generally mark an AIX Service Pack recommended 90 days after it is released.

Security Vulnerability and HIPER APARs should also be evaluated before updating to a recommended level. FLRT has links to “AIX/VIOS Security Tables” and “AIX HIPER Tables” which provide a very useful view of what HIPER or Security problems each release is exposed to, and where to get fixes.

Additional Hints and Recommendations in the *White Paper*.

There are many topics that can be reviewed directly in the white paper. Utilize this information while formal your corporate policy regarding AIX Software for both regular and security management.

- AIX Life Cycle
- AIX Level Naming
- Releases
- Technology Level
- Service Pack
- APAR
- iFixes (Interim Fixes)
- Security Fixes
- Service Pack Updates
- Technology Level Upgrades
- Release Migrations

When you write your security policy regarding AIX Patch Management we recommend you integrate at least the concepts: *Technology Level* (TL), *Service Pack* (SP), Interim Fix_ (ifix), and Security Fix.

AIX Resources

Some of the resources available to assist with AIX Patch Management are:

- **Fix Central** [http:// www.ibm.com/support/fixcentral/](http://www.ibm.com/support/fixcentral/)
- **My Notifications**
<https://www.ibm.com/systems/support/myview/subscription/css.wss/>
- **Fix Level Recommendation Tool (FLRT)**
<http://www.ibm.com/support/customer/care/flrt>
- **AIX Technology Level Lifecycles**
<http://www.ibm.com/support/docview.wss?uid=isg3T1012517%20>

Applying AIX updates/upgrades

The most common patch action is `smitty update_all` pointing at a resource containing only a service pack to apply a service pack (SP) update. The other common action is again `smitty update_all` pointing at a resource containing a technology level, but now both a technology level (TL) and it's (latest) service pack are installed. The key difference between the two is that a SP update, by definition, does not modify and features or default settings. A TL may introduce new features and also change system internal (default) values. These both differ from a `release migration` in that a release migration is performed as a special kind of AIX installation.

A final type of patch management, rather than `smit update_all` is working with the program `emgr` for installing and managing both interim and security fixes. These kinds of patches are needed when a patch cannot wait for the permanent fix applied in a service pack. The added recommendation is to update/upgrade to the service pack containing the permanent fix once it becomes available.

1.5 Summary

- This document is organized following CIS Controls Version 8. The recommendations include references to CIS Controls v8 and whenever possible includes a reference to CIS controls v7.
- The recommendations are based on hardening an insecure (base RTE, no security profile) fresh installation from a NIM server.
- The recommended maintenance strategy is:
 - Review security advisories at least monthly (see below).
 - Before making major system changes (whether security hardening, or an OS update) clone rootvg so that unexpected (adverse) effects can be reverted by rebooting the cloned rootvg.
 - Stay current and refresh the TL of each system at least once a year - For maximum system stability do not wait more 90 days before applying a new update. Remember to clone rootvg before updating!
 - Migrate to a newer TL before (when) the installed TL is no longer supported by IBM.
 - Review the Service Packs for any security or critical fixes - apply these regularly throughout the life cycle of a TL/SP.
 - Interim fixes or individual fixes are applied whenever there is a security requirement to do so. When time and priorities permit delay - wait and apply full TL/SP's.
 - Backup, frequently/regularly, rootvg using `mksysb`. System images of both *before* and *after* applying security updates should be available. There are other methods and products, other than `mksysb` (such as `alt_disk_install`), that are not covered in this document.
 - Repeat system verification after an update. (e.g., file mode changes might be reverted by the update).

Review Bulletins

There should be frequent (at least monthly) review of the security advisory bulletins to remain apprised of all known security issues. These can currently be viewed at the following URL: <https://www14.software.ibm.com/webapp/set2/flrt/doc?page=security>

- The security fixes published in the vulnerability advisories are posted here for download: <https://aix.software.ibm.com/aix/efixes/security>
- The Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) provides security and HIPER (High Impact PERvasive) reports based on the inventory of your system. FLRTVC Script is a ksh script which uses FLRT security and HIPER data (CSV file) to compare the installed filesets and interim fixes against known vulnerabilities and HIPER issues.
<https://www14.software.ibm.com/webapp/set2/flrt/sas?page=flrtvc>
- When any new AIX operating system images are deployed, review the latest available TL and SP releases and update where required. The information regarding the latest fixes can be gleaned from the IBM Fix Central website: <https://www.ibm.com/support/fixcentral/>
- Further details on the IBM recommended maintenance strategies can be found in the "IBM AIX Operating System Service Strategy Details and Best Practices" guide: <https://www14.software.ibm.com/webapp/set2/sas/f/best/home.html>

2 Inventory and Control of Assets

This section combines two controls:

- [CIS Control 01: Inventory and Control of Enterprise Assets](#) *Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.*
- [CIS Control 02: Inventory and Control of Software Assets](#) *Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*

Why Are These Control Critical?

- Enterprise Assets
 - Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Enterprises should know what data is critical to them, and proper asset management will help identify those enterprise assets that hold or manage this critical data, so that appropriate security controls can be applied.
 - External attackers are continuously scanning the internet address space of target enterprises, premise-based or in the cloud, identifying possibly unprotected assets attached to an enterprise's network. Attackers can take advantage of new assets that are installed, yet not securely configured and patched. Internally, unidentified assets can also have weak security configurations that can make them vulnerable to web- or email-based malware; and, adversaries can leverage weak security configurations for traversing the network, once they are inside.
 - Additional assets that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should be identified and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations.
 - Large, complex, dynamic enterprises understandably struggle with the challenge of managing intricate, fast-changing environments. However, attackers have shown the ability, patience, and willingness to "inventory and control" our enterprise assets at very large scale in order to support their opportunities.
 - Another challenge is that portable end-user devices will periodically join a network and then disappear, making the inventory of currently available assets very dynamic. Likewise, cloud environments and virtual machines

can be difficult to track in asset inventories when they are shut down or paused.

- Another benefit of complete enterprise asset management is supporting incident response, both when investigating the origination of network traffic from an asset on the network and when identifying all potentially vulnerable, or impacted, assets of similar type or location during an incident.
- Software Assets
 - A complete software inventory is a critical foundation for preventing attacks. Attackers continuously scan target enterprises looking for vulnerable versions of software that can be remotely exploited. For example, if a user opens a malicious website or attachment with a vulnerable browser, an attacker can often install backdoor programs and bots that give the attacker long-term control of the system. Attackers can also use this access to move laterally through the network. One of the key defenses against these attacks is updating and patching software. However, without a complete inventory of software assets, an enterprise cannot determine if they have vulnerable software, or if there are potential licensing violations.
 - Even if a patch is not yet available, a complete software inventory list allows an enterprise to guard against known attacks until the patch is released. Some sophisticated attackers use “zero-day exploits,” which take advantage of previously unknown vulnerabilities that have yet to have a patch released from the software vendor. Depending on the severity of the exploit, an enterprise can implement temporary mitigation measures to guard against attacks until the patch is released.
 - Management of software assets is also important to identify unnecessary security risks. An enterprise should review its software inventory to identify any enterprise assets running software that is not needed for business purposes. For example, an enterprise asset may come installed with default software that creates a potential security risk and provides no benefit to the enterprise. It is critical to inventory, understand, assess, and manage all software connected to an enterprise’s infrastructure.

How do these controls apply to AIX and/or POWER

Some aspects of an *enterprise asset* rarely change. Some notable aspects for AIX include things that can be counted, e.g., the number of volume groups, the number of volumes in a volume group, the number of network interfaces defined and available, and number of local users. Additional relatively static *inventory* items are hostname, domain name, volume group names, volume group policies, logical volume policies.

Likewise, for software, keeping a system secure is practically impossible if there is no record of what belongs on a system. Without a record - how is anyone to know something is bogus? Without a record - how is anyone able to be alert about applying a (security) patch to the application.

The recommendations here are just a start. Do not feel limited because something is not here. Better, submit a proposal for a new recommendation when you feel you have identified something that is missing from either *enterprise* aka hardware or infrastructure related assets (whether hard or virtual) or a software *inventory* tracking issue.

2.1 Collect system configuration regularly (Manual)

Profile Applicability:

- Level 1

Description:

Maintain a listing of the system configuration showing assets configured into the system.

Rationale:

The syslog facility `local1` is chosen as this is also the facility that the Dynamic Resource Manager (DRM) reports to. The command `logger` simplifies appending command `stdout` to the `syslogd`.

Impact:

All changes to the system configuration should be logged so that the expected configuration is documented. Regular verification of the current configuration makes it possible to identify and correct undocumented system configuration changes.

Audit:

- Verify there is a regular, automated, process to extract the system configuration and append it to a syslog.
- Verify there is a setting in `/etc/syslog.conf` to collect `local1.info` messages to a local log file.







Remediation:

- This example shows how to setup a daily cronjob. The actual frequency you use might differ. The **keyword** in the recommendation is: *regular*.
- This example also shows two `syslog` reporting lines: one to a system file, the second to a centralized `syslog` service.
- The syslog **facility** *local1* is used to keep these reports out of the standard syslog facilities. There is not meant to establish a requirement to use facility *local1*.

```
# mkdir -p /var/log/syslog
# touch /var/log/syslog/inventory.log
# print "local1.info /var/log/syslog/inventory.log rotate 1m files 24
compress" >> /etc/syslog.conf
# print "local1.info @rsyslog.domain" >> /etc/syslog.conf
# refresh -s syslogd || startsrc -s syslogd

# print "0 0 * * * /usr/sbin/lscnf -v | /usr/bin/logger -p local1.info -t
Inventory" >> /var/spool/crontabs/root
# /usr/sbin/lscnf -v | /usr/bin/logger -p local1.info -t Inventory
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>1.1 Establish and Maintain Detailed Enterprise Asset Inventory</u> Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.			
v7	<u>1.4 Maintain Detailed Asset Inventory</u> Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.			

2.2 Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist) (Manual)

Profile Applicability:

- Level 1

Description:

This recommendation is find and report (audit) software on the system that has not been included in the TE (trusted execution) TSD (trusted signature database).

Rationale:

These entries establish a so-called **AllowList**. Software not included on this **AllowList** should be generating a `syslog` and/or `audit` record whenever it is executed.

Trusted Execution (TE) is an AIX security component that can be used to monitor *unauthorized* software in real time.

Unauthorized seems a clear definition, but how TE determines *unauthorized* may not be as clear. Simply put, the goal is that all software is on the **AllowList**. If not, the software is *unauthorized*. AIX uses the term TROJAN (see below) to determine that an application is *unauthorized*. Software that does not require any special kernel privileges to run is also **authorized**.

What is a Trojan?

For this benchmark we add the AIX concept of **TROJAN** as a definition of *unauthorised*. AIX defines Trojan any executable not in the TSD with one or more of the following characteristics:

- uses either SUID or SGID
- is linked to a command in the TSD (**AllowList**)
- is in the `privcmds` (aka RBAC definition, ie, may have kernel privileges).
- is linked to a command in the `privcmds` database.

Summary: On AIX the construct **AllowList** is implemented by the TSD. The clear advantage of an **AllowList** monitored by a system security component is that the system can enforce and/or report violations of **AllowList** in real-time.

This recommendation focuses on reporting violations of the **AllowList**. A later recommendation (update or new version of benchmark) will have a Level 2 recommendation including *enforcing violations*.

Audit:

The following command will locate the software AIX considers *untrusted* aka **TROJAN**.

Note: the output goes to `stderr` so `stderr` is first joined to `stdout` and thereafter `stdout` get redirected to `/dev/null`. The argument `-i` instructs the scan to ignore NFS mounts.

```
trustchk -i -n tree / 2>&1 >/dev/null | grep untrusted
```

Remediation:

This will be a manual process. The remediation is to find and remove the offending file (currently the reported file might be the artifact of another error - most common is a symbolic link that points at a non-existent object).















The starting point is running the same command from the **AUDIT** section:

```
trustchk -i -n tree / 2>&1 >/dev/null | grep untrusted
```

Line by line, verify the root cause and act (one of):

- remove the offending object
- remove SUID/SGID settings
- remove `privcmds` setting
- add to **TSD** aka **AllowList**

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.5 Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v8	<u>2.6 Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v8	<u>2.7 Allowlist Authorized Scripts</u> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			
v7	<u>2.1 Maintain Inventory of Authorized Software</u> Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.			
v7	<u>2.3 Utilize Software Inventory Tools</u> Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.			
v7	<u>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			
v7	<u>2.7 Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			

2.3 Allowlist Authorized Software and Report Violations (Automated)

Profile Applicability:

- Level 1

Description:

At Level 1, utilize Trusted Execution (TE) to log execution of applications not yet whitelisted. This can be used to update the whitelist (TSD - `/etc/security/tsd/tsd.dat`) so that, at Profile Level 2, non-listed applications are actually prevented from executing.

Rationale:

Impact:

As long as the TE policies `STOP_UNTRUSTED=OFF` and `STOP_ON_CHKFAIL=OFF` the system will only log missing entries.

Audit:

- Run the command `trustchk -p`
The output needs to include the lines

```
TE=ON
CHKEEXEC=ON
```

- Verify syslog is configured to collect `kern.info` data, e.g.
`kern.info /var/log/syslog/kern.log 1 month files 24 compress`
- This will provide entries similar to:

```
Jan 26 15:54:32 x077 kern:info unix: Trusted Execution: pid=14221506, euid=0,
ruid=0: File not in TSD: /usr/bin/bzip2
Jan 26 15:54:32 x077 kern:info unix: Trusted Execution: pid=14221506, euid=0,
ruid=0: Allowing to execute non trusted file: /usr/bin/bzip2
```

- audit should be configured to report on TE events.

The following events need to be included in the default: class

```
TE_Untrusted
TE_FileWrite
TE_Policies
TEAdd_Stnz
TEDel_Stnz
TESwitch_algo
TEQuery_Stnz
TE_VerifyAttr
```

Remediation:




```
# trustchk -p TE=ON CHKEEXEC=ON STOP_ON_CHKFAIL=OFF

# mkdir -p /var/log/syslog
# touch /var/log/syslog/kernel.log
# print "kern.info /var/log/syslog/kernel.log rotate 1m files 24 compress" >>
/etc/syslog.conf
# print "kern.info @rsyslog.domain" >> /etc/syslog.conf
# refresh -s syslogd || startsrc -s syslogd
```

Default Value:

```
TE=OFF
```


CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.5 Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v7	<u>2.7 Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			

2.4 Allowlist Authorized Libraries and Report Violations (Automated)

Profile Applicability:

- Level 1

Description:

At Level 1, utilize Trusted Execution (TE) to log execution of applications not yet whitelisted. This can be used to update the whitelist (TSD - `/etc/security/tsd/tsd.dat`) so that, at Profile Level 2, non-listed libraries are actually prevented from executing.

Rationale:

Impact:

As long as the TE policies `STOP_UNTRUSTED=OFF` and `STOP_ON_CHKFAIL=OFF` the system will only log missing entries.

Audit:

- Run the command `trustchk -p`
The output needs to include the lines

```
TE=ON
CHKSHLIB=ON
CHKKERNEXT=ON
```

- Verify syslog is configured to collect `kern.info` data, e.g.
`kern.info /var/log/syslog/kern.log 1 month files 24 compress`
- audit should be configured to report on TE events.

The following events need to be included in the default: class




```
TE_Untrusted
TE_FileWrite
TE_Policies
TEAdd_Stnz
TEDel_Stnz
TESwitch_algo
TEQuery_Stnz
TE_VerifyAttr
```

Remediation:

Default Value:

TE=OFF

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.6 <u>Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v7	2.8 <u>Implement Application Whitelisting of Libraries</u> The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			

2.5 Allowlist Authorized Scripts and Report Violations (Automated)

Profile Applicability:

- Level 1

Description:

At Level 1, utilize Trusted Execution (TE) to log execution of applications not yet whitelisted. This can be used to update the whitelist (TSD - `/etc/security/tsd/tsd.dat`) so that, at Profile Level 2, non-listed scripts are actually prevented from executing.

Rationale:

Impact:

As long as the TE policies `STOP_UNTRUSTED=OFF` and `STOP_ON_CHKFAIL=OFF` the system will only log missing entries.

Audit:

- Run the command `trustchk -p`
The output needs to include the lines

```
TE=ON
CHKSCRIPT=ON
```

- Verify syslog is configured to collect `kern.info` data, e.g.
`kern.info /var/log/syslog/kern.log 1 month files 24 compress`
- audit should be configured to report on TE events.

The following events need to be included in the default: class

```
TE_Untrusted
TE_FileWrite
TE_Policies
TEAdd_Stnz
TEDel_Stnz
TESwitch_algo
TEQuery_Stnz
TE_VerifyAttr
```

Remediation:

Default Value:

```
TE=OFF
```

CIS Controls:

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

2.6 Enforce Allowlist aka Trusted Execution Checks (Automated)

Profile Applicability:

- Level 2

Description:

This takes allowlist aka whitelisting to the next level - where all software, libraries and scripts that are not in the trusted signature database (TSD) in `/etc/security/tsd/tsd.dat` are blocked.

Rationale:

At Level 1 (recommendations 2.3, 2.4 and 2.5) - nothing is stopped from being utilized, but the controls are active and logging so that missing entries can be added to the TSD so that Level 2 will not cause a breach of availability.

Impact:

The step is reversible. By returning the TE policies `STOP_UNTRUSTD` and `STOP_ON_CHKFAIL` back to `OFF` the system will be returned to the Level 1 Profile.

An intermediate Level would be to set `STOP_UNTRUSTD` to `TROJAN` rather than `ON` (Level 2) or `OFF` (Level 1).

```
TROJAN Stops the loading of files that do not belong to the TSD and have
one of the following security settings:
*   Have suid/sgid bit set
*   Linked to a file in the TSD
*   Have entry in the privcmds Database
*   Be linked to a file in the privcmds database
```

Audit:

- Execute the command:

```
# trustchk -p stop_untrustd stop_on_chkfail te
```

- This should return either:

```
STOP_UNTRUSTD=ON  
STOP_ON_CHKFAIL=ON  
TE=ON
```

or

```
STOP_UNTRUSTD=TROJAN  
STOP_ON_CHKFAIL=ON  
TE=ON
```

Remediation:

- Execute one of the following commands:

```
trustchk -p stop_untrustd=on stop_on_chkfail=on te=on
```









or

```
trustchk -p stop_untrustd=trojan stop_on_chkfail=on te=on
```

Default Value:

TE=OFF

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.5 <u>Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v8	2.6 <u>Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v8	2.7 <u>Allowlist Authorized Scripts</u> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			
v7	2.7 <u>Utilize Application Whitelisting</u> Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			
v7	2.8 <u>Implement Application Whitelisting of Libraries</u> The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc) are allowed to load into a system process.			
v7	2.9 <u>Implement Application Whitelisting of Scripts</u> The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc) are allowed to run on a system.			

2.7 Remove Unused Symbolic Links (Automated)

Profile Applicability:

- Level 1

Description:

This recommendation finds and removes symbolic links whose targets are missing. Symbolic Links that do not have a valid target are a risk to system integrity.

The recommendation is to scan frequently (weekly or daily) for symbolic links without a valid target object and remove them.

Rationale:

Do not assume that anyone responsible for maintaining system integrity is (actively) monitoring unknown software.

Symbolic links - pointing at nothing - are, by definition, *unauthorized* and/or belong on a **blocklist**.

Impact:

Symbolic Links, used properly, are a tremendous asset - enhancing system usability (ease of use). However, when pointing to nothing (i.e., whatever they pointed at has been removed but not replaced) system integrity is at the mercy of whatever process replaces that filesystem location later.

To reduce risk to *system integrity* any symbolic link that points at a non-existent file-system object is to be removed.

Note: most symbolic links that point at *no longer existent objects* exist due to incomplete software removal procedures. When an authorized application is (re-)installed it's installation process will (or should) re-create the symbolic link.

Audit:

The following command (long) lists all symbolic links without an existing file-system object.

```
find -L / \( -fstype jfs -o -fstype jfs2 \) -type l -ls
```

The desired result is **no stdout** (as there may be output to stderr). For example, **stderr** may report:







```
find: /some/link/to/something: Link to an already visited ancestor
```

Remediation:

The following command will remove all symbolic links that lack a valid target object:

```
find -L / \( -fstype jfs -o -fstype jfs2 \) -type l | xargs rm
```

CIS Controls:

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

2.8 Ensure the Trusted Execution Policies cannot be modified (Automated)

Profile Applicability:

- Level 2

Description:

Set trusted execution policy `LOCK_KERN_POLICIES` to enabled. All of the other policies will then be locked and cannot be changed without disabling the `LOCK_KERN_POLICIES` policy and then restarting the system.

Rationale:

When policies are locked, unauthorized users cannot make changes to the policies to allow them to execute unapproved tools and then revert the settings afterwards. An unplanned system reboot is likely to be noticed and investigated

Audit:

Run the command

```
trustchk -p | grep LOCK_KERN_POLICIES
```

The output should be

```
LOCK_KERN_POLICIES=ON
```

Remediation:

Execute the following command

```
trustchk -p LOCK_KERN_POLICIES=ON
```

3 Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

See: <https://workbench.cisecurity.org/benchmarks/6480/sections/698298>

Why is this Section Critical

Data is no longer only contained within an enterprise's border; it is in the cloud, on portable end-user devices where users work from home, and is often shared with partners or online services that might have it anywhere in the world. In addition to sensitive data an enterprise holds related to finances, intellectual property, and customer data, there also might be numerous international regulations for protection of personal data. Data privacy has become increasingly important, and enterprises are learning that privacy is about the appropriate use and management of data, not just encryption. Data must be appropriately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises of any size; however, there are fundamentals that can apply to all.

Once attackers have penetrated an enterprise's infrastructure, one of their first tasks is to find and exfiltrate data. Enterprises might not be aware that sensitive data is leaving their environment because they are not monitoring data outflows.

While many attacks occur on the network, others involve physical theft of portable end-user devices, attacks on service providers or other partners holding sensitive data. Other sensitive enterprise assets may also include non-computing devices that provide management and control of physical systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

The enterprise's loss of control over protected or sensitive data is a serious and often reportable business impact. While some data is compromised or lost as a result of theft or espionage, the vast majority are a result of poorly understood data management rules, and user error. The adoption of data encryption, both in transit and at rest, can provide mitigation against data compromise, and, even more important, it is a regulatory requirement for most controlled data.

3.1 Encryption: File System Level (EFS) (Automated)

Profile Applicability:

- Level 2

Description:

The recommendation, if there is a requirement for file based encryption aka encryption at rest, is to utilize EFS.

Rationale:

A security enhancement introduced with AIX 6.1 is **Encrypted Filesystems** (EFS). This technology enables an individual user to encrypt their own data within a jfs2 filesystem.

After enabling a filesystem to use EFS individual files can be encrypted or encryption can be set at the directory (all files within the directory, recursively) or by system administration at filesystem level. Encryption is performed by the kernel. Access to the kernel secret key is managed via keystore files. The standard AIX data and user management commands have been modified to work with encryption.

Data is only accessible in 'cleartext' when the active process has access to the secret key. Without this access the file system acts as if the file does not exist.

Impact:

The use of EFS enhances the file and directory security within AIX. If there are sensitive or confidential files, encryption provides that extra level of security in the event of an accidental `chmod` which may allow read or write access to other users.

The encryption operates at the filesystem level and each file is encrypted with a separate key. From a user perspective the encryption is transparent as the key can be automatically loaded during login.

Audit:

Validate the installation of the CLiC software:

```
lsldp -L |grep "clic"
```

The above command should yield the following output:

clic.rte.includes	4.3.0.0	C	F	CryptoLite for C Library Include File
clic.rte.kernext	4.3.0.0	C	F	CryptLite for C Kernel
clic.rte.lib	4.3.0.0	C	F	CyrptoLite for C Library
clic.rte.pkcs11	4.3.0.0	C	F	PKCS11 Software Token Support

NOTE: The version numbers may differ based on the source of the software

Validate that the CLiC kernel extension has loaded:

```
genkex |grep crypt
```

The above command should yield the following output:

```
438b000 39000 /usr/lib/drivers/crypto/clickext
```

Remediation:

There are two pre-requisite requirements for EFS, it requires RBAC and the installation of the CLiC cryptographic fileset. The fileset is located on the expansion pack, shipped with the AIX media.

Place the CLiC software into a convenient location, such as `/tmp` and install via:

```
/usr/lib/inst1/sm_inst installp_cmd -a -Q -d /tmp -f clic.rte -c -N -g -X -G -Y
```

NOTE: If the software is not located in `/tmp`, reflect the actual location in the command above.

Load the CLiC kernel extension:

```
/usr/lib/methods/loadkcllic
```

As the EFS administrator, create the initial keystore. This is typically the root user:

```
efsenable -a
```

An EFS enabled filesystem can be created with the following command:

```
chfs -v jfs2 -g <vg_name> -m <filesystem> -a size=<size> -a efs=yes
```

To enable EFS for an existing filesystem:

```
chfs -a efs=yes <filesystem>
```

To encrypt a file, load your keystore via:

```
efskeymgr -o ksh
```

Then encrypt via:

```
efsmgr -c AES_192_ECB -e <filename>
```

To decrypt:

```
efsmgr -d <filename>
```

Further details regarding planning and implementation of EFS can be found within the IBM AIX 7.1 Infocentre:

<https://www.ibm.com/docs/en/aix/7.1?topic=system-efs-encrypted-file>

NOTE: The configuration of EFS is completely dependent on the unique requirements of a given environment.

Default Value:

N/A

References:

1. <https://www.ibm.com/docs/en/aix/7.1?topic=system-efs-encrypted-file>

Additional Information:

Reversion:




De-install the CLiC fileset:

```
installp -u clic.rte
```

Decrypt all files:

```
efsmgr -d <filename>
```

CIS Controls:

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

3.2 Encryption: Logical Volume (ELV) (Manual)

Profile Applicability:

- Level 2

Description:

Starting with AIX 7.2 TL5, AIX adds LV encryption (encryption at logical volume level). This is an alternate *data at rest* encryption solution. Below is a blog about the feature.

In the references there is a link to one of the early blogs (written by an IBMer). The end of blog points to documentation in AIX 7.2 knowledge center.

Rationale:

Some organizations are required to show that *data at rest* is encrypted. A common example is the PCI (payment card industry) requirement to encrypt so-called *sensitive* data such as a direct link between card holder name and card number.

Using LV encryption is much like disk encryption of a PC. Once operational, the application environment does not even know the data is encrypted. The encryption is only noticeable when the (disk) storage is mounted somewhere else. Outside of the configured environment all information on the disk (read logical volume) is encrypted.

Impact:

For many uses LVE (logical volume encryption) is much easier to use - by applications - compared to an encryption solution such as EFS (encrypted file system). Once the system boots - and a valid (i.e., authorised) process or user is active on the system - they will have access to data, or not - depending on the classic access controls (e.g., inode DAC controls, ACLs, etc.).

LVE does have specific requirements on the management environment and the systems that can support it. See the blog for specifics. (EFS has no requirements other than it is enabled on AIX 6.1 or later).

No **audit** or **remediation** statements are provided. They will need to be provided by whoever implements LVE in your environment.

Audit:

Remediation:




Default Value:

Not enabled.

References:

1. ****BLOG****: [AIX 72 TL5: Logical Volume Encryption](<https://community.ibm.com/community/user/power/blogs/xiaohan-qin1/2020/11/23/aix-lv-encryption?CommunityKey=daa942cb-b783-4fd3-ba27-a2d7462f9530&tab=recentcommunityblogsdashboard>)

CIS Controls:

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

3.3 Ensure default user umask is 027 or more restrictive (Automated)

Profile Applicability:

- Level 1

Description:

The user file-creation mode mask (`umask`) is used to determine the file permission for newly created directories and files. In AIX, the default permissions for any newly created directory is 0755 (rwxr-xr-x), and for any newly created file it is 0644 (rw-r--r--). The `umask` modifies the default AIX 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.

Rationale:

Setting a very secure default value for `umask` ensures that users make a conscious choice about their file permissions. A default `umask` setting of 077 causes files and directories created by users to not be readable by any other user on the system. A `umask` of 027 would make files and directories readable by users in the same Unix group, while a `umask` of 022 would make files readable by every user on the system.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a umask
```

The above command should yield the following output:

```
default umask=27
```

Remediation:







Add the `umask` attribute to the default user stanza in `/etc/security/user`:

```
chsec -f /etc/security/user -s default -a umask=027
```

Default Value:

```
umask=022
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> 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.			

3.4 Remove group write permission from default groups - exceptions must be in TSD and audit (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for group writable files.

Rationale:

An audit should be performed on the system to search for the presence of group writable files.

In an extreme case - where this permission is required - the file needs to be added to the TSD and **audit** configurations.

The preference is **no** group writeable files.

Audit:

Re-execute the appropriate `find` command.

Use the following to find all group writable files on local JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -ls
```

NOTE: Review the output based on the performed remediation

Remediation:

- Review the currently mounted local filesystems using the following to find all group writable files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -ls
```

- Remedy any files in the list, e.g., `chmod g-w {filename}`
- Document any files, and motivate why they are group writeable, and also add documentation re: when/why this exception ceases.







Default Value:

N/A

Additional Information:

The **audit** procedure does not verify remote file systems (e.g., NFS). The expectation is that these are being audited on the file (e.g., NFS) server - rather than on all clients.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> 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.			

3.5 Application Data with requirement for world writable directories (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for world writable directories.

Rationale:

World writable directories are considered as a common application component - usually a location for temporary files.

An audit should be performed on the system to search for the presence of world writable directories. Directories should only be world writable when absolutely necessary, and only with the so-called `SVTX` bit set. This protects users files from being deleted or renamed.

Impact:

World writable directories exist on UNIX systems (e.g., `/tmp`, `/var/tmp`). These directories are needed for normal operations. To protect the files created in the directories the 'links to the inode' (ie, filename) need to be protected so that others may not accidentally, or maliciously - remove or modify the filename.

Audit:

Execute the `find` command.

Use the following to find all world writable directories on local JFS/JFS2 filesystems that do not have the `SVTX` bit:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type d -perm -o+w ! -perm -1000 -ls
```

The output should be empty.

Remediation:

- Review the local mounted JFS/JFS2 filesystems using the following command to find all world writable directories missing the SVTX bit:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type d -perm -o+w ! ! -perm -1000 -ls
```

- If a directory must retain world writable access, ensure that SVTX bit is set so that users can only remove the filenames they own:

```
chmod o+t ${dir}
```

NOTE: This will leave existing modes while adding the SVTX (also known as `sticky bit`) to the directory. The documented meaning of the flag for directories is:

Sets the link permission to directories.




- Otherwise, remove world-write permission - without modifying the other mode bits:

```
chmod o-w ${dir}
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			

3.6 Ensure there are no world writable files - exceptions must be in TSD and audit (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for world writable files.

Rationale:

An audit should be performed on the system to search for the presence of world writable files.

In an extreme case - where this permission is required - the file needs to be added to the TSD and **audit** configurations.

The preference is **no** world writeable files.

Audit:

Use the following to find all world writable files and directories on local JFS2 filesystems only:

```
PID=$$
CNT=$(find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -o+w | tee
/tmp/cis-3.6.${PID} | wc -l)
if [ ${CNT} -ne 0 ]; then
    find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -o+w -ls
fi
rm -f /tmp/cis-3.6.${PID}
```

NOTE: Review the output based on the performed remediation

Remediation:

- Review the currently mounted local filesystems using the following to find all world writable files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -o+w -ls
```

- Remedy any files in the list, e.g., `chmod o-w {filename}`
- Document any files, and motivate why they are world writeable, and also add documentation re: when/why this exception ceases.







Default Value:

N/A

Additional Information:

The **audit** procedure does not verify remote file systems (e.g., NFS). The expectation is that these are being audited on the file (e.g., NFS) server - rather than on all clients.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> 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.			

3.7 Ensure there are no 'staff' writable files - exceptions must be in TSD and audit (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for **group staff** writable files.

Rationale:

An audit should be performed on the system to search for files that can be modified by members of the group **staff**. As **staff** is the default group for user accounts any file that is *writable* via group *staff* is comparable to being writable by other aka world writable.

In a case - where this permission is required - the recommendation is to create a new group and appoint a group administrator.

The goal is **no group staff** writable files.

Audit:

Re-execute the appropriate `find` command.

Use the following to find all world writable files and directories on local JFS2 filesystems only:

```
PID=$$
CNT=$(find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -group
staff | tee /tmp/cis-3.7.${PID} | wc -l)
if [ ${CNT} -ne 0 ]; then
    # Need actions to report on actions, for now repeat find command to stdout
    # TBD: read tmp file just created
    # if file/directory is in TSD then continue
    # else - present ls -li of the object found
    # For now, just repeat the find command and show all related objects.
    find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -group staff -
ls
fi
rm -f /tmp/cis-3.7.${PID}
```

NOTE: Review the output based on the performed remediation

Remediation:

- Review the currently mounted local filesystems using the following to find all world writable files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -group staff -ls
```

- Remedy any files in the list, e.g., `chmod o-w {filename}`
- Document any files, and motivate why they are world writeable, and also add documentation re: when/why this exception ceases.







Default Value:

N/A

Additional Information:

The **audit** procedure does not verify remote file systems (e.g., NFS). The expectation is that these are being audited on the file (e.g., NFS) server - rather than on all clients.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> 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.			

3.8 Ensure all files and directories are owned by a user (uid) and assigned to a group (gid) (Automated)

Profile Applicability:

- Level 1

Description:

When a user or group identifier is removed from the system verify that any data associated with the ID removed is either removed or re-assigned.

Rationale:

Worst case: a previously removed UID/GID is re-instated. Data left behind suddenly is owned and/or accessible to the new ID - gaining unintended access to data left-behind.

Audit:

Re-execute the appropriate `find` command.

If there are non-local filesystems which cannot be un-mounted, use the following to find all un-owned files and directories on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) \( -nouser -o -nogroup \) -ls
```

- There should not be any output

Remediation:

Review the currently mounted `/ocal/` filesystems:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -type d -o -type f \) \( -nouser -o -nogroup \) -ls
```

- Either assign UID/GID:

```
chown <owner> <file>  
chgrp <group> <file>
```

- or remove the file/directory:




```
[[ -f <file> ]] && rm -f <file>  
[[ -d <file> ]] && rmdir <file>
```

- Repeat the audit

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.5 <u>Securely Dispose of Data</u> Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.			

4 Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of end-user devices (laptops, tablets, and smartphones), servers, applications, network infrastructure and service provider products.

See [CIS Control 4. Secure Configuration of Enterprise Assets and Software](#)

Why is this Section Critical?

As delivered from manufacturers and resellers, the default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security. Basic controls, open services and ports, default accounts or passwords, pre-configured Domain Name System (DNS) settings, older (vulnerable) protocols, and pre-installation of unnecessary software can all be exploitable if left in their default state. Further, these security configuration updates need to be managed and maintained over the life cycle of enterprise assets and software. Configuration updates need to be tracked and approved through configuration management workflow process to maintain a record that can be reviewed for compliance, leveraged for incident response, and to support audits. This CIS Control is important to on-premises devices, as well as remote devices, network devices, and cloud environments.

Service providers play a key role in modern infrastructures, especially for smaller enterprises. They often are not set up by default in the most secure configuration to provide flexibility for their customers to apply their own security policies. Therefore, the presence of default accounts or passwords, excessive access, or unnecessary services are common in default configurations. These could introduce weaknesses that are under the responsibility of the enterprise that is using the software, rather than the service provider. This extends to ongoing management and updates, as some Platform as a Service (PaaS) only extend to the operating system, so patching and updating hosted applications are under the responsibility of the enterprise.

Even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are “tweaked,” to allow the installation of new software or to support new operational requirements.

AIX 7.2 packaging changes for TCPIP

Starting with AIX 7.2 many standard tcp server and client applications are packaged in individual filesets. The preferred remediation will be to remove software rather than disable it. With AIX versions prior to AIX 7.2 removing TCPIP filesets was not feasible - working with TCPIP was all or nothing. Now there is the option to remove software filesets.

4.1 System Boot

The Boot phase, or IPL (Initial Program Load in many IBM documents) is critical to the security of the operating system.

The key software components of the boot process is the script `/sbin/rc.boot` that manages the first two phases of the boot process, and the programs called via `/etc/inittab`. The programs called via `/etc/inittab` are considered the final phase (3) of the boot process.

Key scripts called during this phase are `/etc/rc.tcpip` that starts many of the default SRC (System Resource Controller) managed processes. This script also initiates the IPv6 stack, if enabled as `autoconf6`. Another important service started by this script in the `inetd` (aka super daemon).

Another key script is the script `/etc/rc.d/rc` that - during a default boot (run-time level 2) calls all the scripts with character `s` as it's first character in the directory `/etc/rc.d/rc2.d`.

This section is divided into subsections focusing on these areas of interest.

4.1.1 Boot phase: `/etc/inittab`

These are applications managed by the `init` process.

Frequently, when the process started is a daemon process, it runs under the UID 0 (aka root) and their parent process id (PPID) is the process `init`, or PID 1.

In those cases, when these programs exit - `init` checks the process's entry in `/etc/inittab` (`init` table) to see if the process should be restarted, or not.

Review the commands: `lsitab`, `mkitab`, `chitab`, and `rmitab` to make modifications to `/etc/inittab`, preferably using RBAC (i.e., without the need for root access).

4.1.1.1 Disable writesrv (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to disable `writesrv`. This allows users to chat using the system write facility on a terminal.

Rationale:

`writesrv` allows users to chat using the system write facility on a terminal. The recommendation is that this service must be disabled.

Audit:

Ensure that `writesrv` is disabled:

```
lsitab writesrv  
lssrc -s writesrv | grep -v inoperative
```

The above commands should yield no output.

Remediation:

Identify if `writesrv` is enabled:

```
lsitab writesrv | wc -l
```

If the command output `!= "0"` stop the service and remove the entry from `/etc/inittab`

```
rmitab writesrv  
stopsrc -s writesrv
```

Default Value:

N/A





Additional Information:

Reversion:

Re-add the `writesrv` startup line to `/etc/inittab`:

```
mkitab "writesrv:2:wait:/usr/bin/startsrc -swritesrv"
```

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.			

4.1.1.2 Disable *ntalk*/*talk* (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to block *chat* via `talk` or `ntalk`. These services enable users to chat within terminal sessions.

Rationale:

These services use unsecured TCP and UDP protocols and can be snooped via the network.

Audit:

Ensure that `talk` and `ntalk` have been disabled:

```
#!/usr/bin/ksh -e$
TALK=$(egrep -v "^#" /etc/inetd.conf | grep talk | wc -l)$
INETD=$(lssrc -s inetd | grep active | wc -l)$
if [[ ${TALK} != "0" ]]; then$
  if [[ ${INETD} != "0" ]]; then$
    echo "Error: talk/ntalk daemon is active."$
  else$
    echo "WARN: talk/ntalk daemon will be activated with inetd."$
  fi$
fi$
```

NOTE: The command should not return any output.

Remediation:

Disable `talk` and `write`.





```
rmitab writesrv

chmod a-rwx /usr/sbin/writesrv
trustchk -u /usr/sbin/writesrv mode
```

Default Value:

`ntalk` is enabled

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.			

4.1.1.3 dt (Automated)

Profile Applicability:

- Level 1

Description:

This entry executes the CDE startup script which starts the AIX Common Desktop Environment.

Rationale:

If there is not an `lft` connected to the system and there are no other X11 clients that require CDE, remove the `dt` entry.

Audit:

From the command prompt, execute the following command:

```
lsitab dt
```

The above command should yield not yield output.

Remediation:

In `/etc/inittab`, remove the `dt` entry:

```
rmitab dt
```

Default Value:

Uncommented (if an `lft` is present)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.1.1.4 piobe (Automated)

Profile Applicability:

- Level 1

Description:

The `piobe` daemon is the I/O back end for the printing process, handling the job scheduling and spooling.

Rationale:

If there is not a requirement for the system to support either local or remote printing, remove the `piobe` entry.

Audit:

From the command prompt, execute the following command:

```
lsitab piobe
```

The above command should yield not yield output.

Remediation:

In `/etc/inittab`, remove the `piobe` entry:

```
rmitab piobe
```

Default Value:

Uncommented

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.1.1.5 qdaemon (Automated)

Profile Applicability:

- Level 1

Description:

This is the printing scheduling daemon that manages the submission of print jobs to piobe.

Rationale:

If there is not a requirement to support local or remote printing, remove the qdaemon entry from /etc/inittab.

Audit:

From the command prompt, execute the following command:

```
lsitab qdaemon
```

The above command should yield not yield output

Remediation:

In /etc/inittab, remove the qdaemon entry:

```
rmitab qdaemon
```

Default Value:

Enabled

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.		●	●

4.1.1.6 rc.nfs (Automated)

Profile Applicability:

- Level 1

Description:

The `rcnfs` entry starts the NFS, NIS and automount daemons during system boot. Additionally, it automounts filesystems with the attribute `vfs = nfs`.

Rationale:

NFS is a service with numerous historical vulnerabilities and **should not be enabled unless there is no alternative**.

Audit:

From the command prompt, execute the following command:

```
lsitab rcnfs
```

The above command should not yield output

Remediation:

Use the `rmitab` command to remove the NFS start-up script from `/etc/inittab`:

```
rmitab rcnfs
```

Also, to be certain NFS related services have been discounted - execute the following script:

```
/etc/nfs.clean
```

Default Value:





Uncommented

Additional Information:

If NFS related services are required, then read-only exports and mounts are recommended. NFS mounts should include the options `nodev` and `nosuid` to prevent unauthorized access. Further no filesystem or directory should be exported with root access.

Remember, Unless otherwise required the NFS related services should be disabled.

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.			

4.1.1.7 *cas_agent* (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/inittab` entry labeled `cas_agent` starts an agent that communicates with `FSM` and/or `IBM Director`. The agent is started by the `SRC` subsystem and is installed by the fileset `cas.agent`.

Rationale:

The products this agent communicates with are `depreciated` - no longer supported by IBM as `POWER` platform systems management software. While `harmless` when running the agent may trigger a security alert due to the way it initializes with `FSM` (`System Director`).

Audit:

Execute the following command:

```
(lslpp -L cas.agent >/dev/null 2>&1 && print "cas.agent is installed") ||  
  print "cas.agent is not installed"
```

The output should be:

```
cas.agent is not installed
```

Remediation:





The following command will deinstall the `cas.agent` fileset and also any filesets installed that depend on `cas.agent` (e.g., if `artex.base.agent` is also installed):

```
lslpp -L cas.agent >/dev/null 2>&1 && installp -ug cas.agent
```

Default Value:

:on: if agent is installed.

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.			

4.1.2 Boot phase: /etc/rc.tcpip: daemons

The file `/etc/rc.tcpip` is executed during the AIX IPL (Initial Program Load, aka boot). The programs started here are managed by the sub-system known as `src`, or [System Resource Controller](#).

4.1.2.1 *inetd* - aka Super Daemon (Automated)

Profile Applicability:

- Level 1

Description:

When none of the services run and managed by `inetd` are required then disable the `inetd` daemon itself.

This is the preferred state.

Rationale:

When no `inetd` managed services are required there is no need to start the daemon at boot time.

An administrator can manually start the `inetd` service post-IPL, should any of the `inetd` supported services are/become required.

Impact:

When an `inetd` service is required this service is permitted. Be sure to review the section 4.1.5 `Inetd (aka Super Daemon) Services` later in the document.

Audit:

Ensure that `inetd` startup has been commented out of `/etc/rc.tcpip`.

```
grep "^#start[[:blank:]]/usr/sbin/inetd" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/inetd "$src_running"
```

Remediation:

Review any active `inetd` services:

```
refresh -s inetd
lssrc -ls inetd
```

NOTE: If there are active services and the services are required, do not disable `inetd`. Skip to the next section and consider the implementation of TCP Wrappers to secure access to these active services. If the active services are not required disable them via the `chsubserver` command.

Disable `inetd` if there are no active services:

```
chrctcp -d inetd
stopsrc -s inetd
```

Default Value:

Enabled





Additional Information:

Reversion:

Comment in `inetd` startup in `/etc/rc.tcpip`:

```
chrctcp -a inetd
```

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.			

4.1.2.2 aixmibd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `aixmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `aixmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. The recommendation is to disable `aixmibd` Unless `snmpd` is required.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/aixmibd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/aixmibd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s aixmibd | grep tcpip
```

This should yield the following output:

aixmibd	tcpip	inoperative
---------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `aixmibd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d aixmibd  
stopsrc -s aixmibd
```

- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.snmpd
```

Default Value:





Uncommented

Additional Information:

The `aixmib` collects data from an AIX specific MIB. Further details relating to this MIB can be found in the URL below:

<https://www.ibm.com/docs/en/aix/7.1?topic=aixmib-daemon>

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.			

4.1.2.3 *dhcpcd* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `dhcpcd` daemon on system startup. The `dhcpcd` daemon receives address and configuration information from the DHCP server.

Rationale:

The `dhcpcd` daemon is the DHCP client that receives address and configuration information from the DHCP server. This must be disabled if DHCP is not used to serve IP address to the local system.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/dhcpcd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/dhcpcd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s dhcpcd
```

This should yield the following output:

```
dhcpcd          tcpip          inoperative
```

Remediation:

- On AIX 7.1 and earlier comment out the `dhcpcd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d dhcpcd
stopsrc -s dhcpcd
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.dhcpd
```

Default Value:

Commented out

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.			

4.1.2.4 dhcprd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `dhcprd` daemon on system startup. The `dhcprd` daemon listens for broadcast packets, receives them, and forwards them to the appropriate server.

Rationale:

The `dhcprd` daemon is the DHCP relay daemon that forwards the DHCP and BOOTP packets in the network. You must disable this service if DHCP is not enabled in the network.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/dhcprd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/dhcprd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s dhcprd
```

This should yield the following output:

```
dhcprd          tcpip          dhcprd          inoperative
```

Remediation:

- On AIX 7.1 and earlier comment out the `dhcprd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d dhcprd
stopsrc -s dhcprd
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.dhcpd
```

Default Value:

Commented out

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.			

4.1.2.5 *dhcpcsd* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `dhcpcsd` daemon on system startup. The `dhcpcsd` daemon is the DHCP server that serves addresses and configuration information to DHCP clients in the network.

Rationale:

The `dhcpcsd` daemon is the DHCP server that serves addresses and configuration information to DHCP clients in the network. You must disable this service if the server is not a DHCP server.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/dhcpcsd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/dhcpcsd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s dhcpcsd
```

This should yield the following output:

```
dhcpcsd          tcpip          inoperative
```

Remediation:

- On AIX 7.1 and earlier comment out the `dhcpcsd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d dhcpcsd
stopsrc -s dhcpcsd
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.dhcpd
```

Default Value:

Commented out

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.			

4.1.2.6 dpid2 (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `dpid2` daemon on system startup. The `dpid2` daemon acts as a protocol converter, which enables DPI (SNMP v2) sub-agents, such as `hostmibd`, to talk to a SNMP v1 agent that follows SNMP MUX protocol.

Rationale:

The `dpid2` daemon acts as a protocol converter, which enables DPI sub-agents, such as `hostmibd`, to talk to a SNMP v1 agent that follows SNMP MUX protocol. Unless the server hosts an SNMP agent, it is recommended that `dpid2` is disabled.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/dpid2" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/dpid2"$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s dpid2
```

This should yield the following output:

dpid2	tcpip	inoperative
-------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `dpid2` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d dpid2  
stopsrc -s dpid2
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.snmpd
```

Default Value:

Commented out

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.			

4.1.2.7 *gated* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `gated` daemon on system startup. This daemon provides gateway routing functions for protocols such as RIP OSPF and BGP.

Rationale:

The `gated` daemon provides gateway routing functions for protocols such as RIP, OSPF and BGP. The recommendation is that this daemon is disabled unless the server is acting as a network router, e.g., to support VIPA.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/gated" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/gated" $src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s gated
```

This should yield the following output:

gated	tcpip	inoperative
-------	-------	-------------

Remediation:

Choose one of the following:

- On AIX 7.1 and earlier comment out the `gated` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d gated  
stopsrc -s gated
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.gated
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.1.2.8 *hostmibd* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `hostmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `hostmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. If `snmpd` is not required, it is recommended that it is disabled.

The specific MIB variables which are managed by `hostmibd` are defined by RFC 2790. Details relating to these MIBS can be found in:

<https://www.ibm.com/docs/en/aix/7.1?topic=h-hostmibd-daemon>

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/hostmibd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/hostmibd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s hostmibd
```

This should yield the following output:

hostmibd	tcpip	inoperative
----------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `hostmib` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d hostmibd  
stopsrc -s hostmibd
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.snmpd
```

Default Value:

Enabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.1.2.9 *mrouted* (Manual)

Profile Applicability:

- Level 2

Description:

This entry starts the `mrouted` daemon on system startup. This daemon is an implementation of the multicast routing protocol.

Rationale:

The `mrouted` daemon is an implementation of the multicast routing protocol. The recommendation is to only permit this service when there is a documented need for the service.

The assumption of this recommendation is that the service is not needed - and the audit and remediation are written to disable the service (it's default setting).

Impact:

When this service's need is documented (include with assessment report) the audit and remediation for this service may be skipped.

The CIS controls are to disable **unneeded** software. When *needed* it's usage must be allowed.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/mROUTED" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/mROUTED "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s mROUTED
```

This should yield the following output:

mROUTED	tcpip	inoperative
---------	-------	-------------

Remediation:





In `/etc/rc.tcpip`, comment out the `mrouted` entry and stop a running service:

```
chrctcp -d mrouted
stopsrc -s mrouted
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.1.2.10 *named* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `named` daemon on system startup. This is the server for the DNS protocol and controls domain name resolution for its clients.

Rationale:

The `named` daemon is the server for the DNS protocol and controls domain name resolution for its clients. It is recommended that this daemon is disabled, unless the server is functioning as a DNS server. This entry starts the `named` daemon at system startup. This is the server for the DNS protocol and controls domain name resolution for its clients.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/named" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/named "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s named
```

This should yield the following output:

named	tcpip	inoperative
-------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `named` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d named  
stopsrc -s named
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.bind
```

Default Value:

disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.1.2.11 *portmap* (Manual)

Profile Applicability:

- Level 1

Description:

If all RPC services are disabled, disable the `portmap` daemon itself.

The `portmap` daemon is required for the RPC service. It converts the RPC program numbers into Internet port numbers. The daemon may be disabled if the server is not:

1. An NFS server
2. A NIS (YP) or NIS+ server
3. Running the CDE GUI
4. Running a third-party software application that relies on RPC support

Rationale:

If no RPC services are required then there is no need to start the `portmap` daemon at boot time.

A start of `portmap` can be done either manually, or scripted, should RPC port-mapping support be needed post-IPL.

Audit:

- Ensure that `portmap` services are not required.
- The command below provides information the status of `portmap` service.
- Ideally, there is no output - scored as +1.
- When there is output and it indicates an error, the score is -1, otherwise 0.

```

#!/usr/bin/ksh -e
# Author: Michael Felt, AIXTools
# Version: 1.01
action=$1
ret=0
set $(rpcinfo -p localhost 2>/dev/null | /usr/bin/egrep -v
"(portmap)|(status)|(nsm)|(pyramid)" | wc -l)
if [ $1 -gt 1 ] ; then
    # There are RPC services other than portmap related services
    # Unless specifically required for a business process this is considered a
    risk.
    # If there are RPC services active - will not disable portmap service
    if [[ $# -eq 0 || ${action} != "fix" ]]; then
        print "$0: Audit mode: Verify the services listed are actually needed."
        print "This should be scored as an error unless there is a documented
        need"
        print "for the following RPC based services."
    else
        print "$0: FIX mode: cannot fix portmap service activation"
        print "\tbefore the RPC services are deactivated."
        ret=-1
    fi
    print "++++ The following services (excluding portmap itself) are active
    +++++"
    rpcinfo -p localhost 2>/dev/null | /usr/bin/egrep -v
    "(portmap)|(status)|(nsm)|(pyramid)"
elif [ $1 -le 1 ] ; then
    if [[ ${action} != "fix" ]] ; then
        if [ $1 -eq 1 ] ; then
            print "portmap is active. This should be considered an error."
        fi
        # No RPC services were reported. Check if autostart is disabled.
        result=$(grep "start[:blank:]/usr/sbin/portmap" /etc/rc.tcpip)
        if [[ $result == '[ -z "$portmap_pid" ] && start /usr/sbin/portmap
        "${src_running}"' ]] ; then
            print "portmap is set to autostart. This should be considered an
            error."
        fi
    elif [[ $action == "fix" ]]; then
        print "Removing autostart of portmap."
        PID=$$
        umask 077
        cat /etc/rc.tcpip >/var/tmp/rctcpip.${PID}
        sed -e "s/^\[ -z \"\$portmap_pid\"/#&/" </var/tmp/rctcpip.${PID}
        >/etc/rc.tcpip
        rm -f /var/tmp/rctcpip.${PID}
        # Stop the portmapper, if active
        stopsrc -s portmap
        # Switch of automatic NFS services, if still in /etc/inittab
        chitab "rcnfs:23456789:off:/etc/rc.nfs > /dev/console 2>&1 # Start NFS
        Daemons"
    fi
fi

```

Remediation:

- Review any active RPC services:

```
rpcinfo -p localhost
```

- Run the program above (in Audit) with the argument `fix`
- check exit status (should be 0)

Default Value:

Enabled

Additional Information:

Reversion:

Restore in `portmap` startup in `/etc/rc.tcpip`:

```
chrctcp -a portmap  
startsrc -s portmap
```

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.		●	●

4.1.2.12 *routed* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `routed` daemon on system startup. The `routed` daemon manages the network routing tables in the kernel.

Rationale:

The `routed` daemon manages the network routing tables in the kernel. This daemon should not be used as it only supports RIP1. If the AIX server must communicate with routers use `gated` instead.

Impact:

Like `mrouted` this daemon is part of `bos.net.tcp.server_core` (AIX 7.2 and later) so it cannot be removed from the system.

Unlike `mrouted` this daemon should not be used. Should the AIX server need to communicate directly with routers (i.e., there is no default route but routes are managed by software) - the `gated` should be used.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/routed" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/routed "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s routed
```

This should yield the following output:

routed	tcpip	inoperative
--------	-------	-------------

Remediation:





In `/etc/rc.tcpip`, comment out the `routed` entry:

```
chrctcp -d routed  
stopsrc -s routed
```

Default Value:

Disabled

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.			

4.1.2.13 rwhod (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rwhod` daemon on system startup. This is the remote WHO service.

Rationale:

The `rwhod` daemon is the remote WHO service, which collects and broadcasts status information to peer servers on the same network. It is recommended that this daemon is disabled, unless it is required.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/rwhod" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/rwhod" $src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s rwhod
```

This should yield the following output:

rwhod	tcpip	inoperative
-------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `rwhod` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d rwhod  
stopsrc -s rwhod
```

- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.rcmd_server
```

Default Value:

Disabled

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.		●	●

4.1.2.14 sendmail (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `sendmail` daemon on system startup. This means that the system can operate as a mail server.

Rationale:

`sendmail` is a service with many historical vulnerabilities and where possible should be disabled. If the system is not required to operate as a mail server i.e. sending, receiving or processing e-mail, comment out the `sendmail` entry.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/lib/sendmail" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/lib/sendmail "$src_running" "-bd -q${qpi}"
```

- From the command prompt, execute the following command:

```
lssrc -s sendmail
```

This should yield the following output:

```
sendmail      mail      sendmail      inoperative
```

Remediation:

- On AIX 7.1 and earlier comment out the `sendmail` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d sendmail  
stopsrc -s sendmail
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.sendmail
```

Default Value:

Enabled

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.			

4.1.2.15 snmpd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `snmpd` daemon on system startup. This allows remote monitoring of network and server configuration.

Rationale:

The `snmpd` daemon is used by many 3rd party applications to monitor the health of the system. If `snmpd` is not required, it is recommended that it is disabled.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/snmpd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/snmpd"$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s snmpd
```

This should yield the following output:

snmpd	tcpip	inoperative
-------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `snmpd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d snmpd  
stopsrc -s snmpd
```

- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.snmpd
```

Default Value:

Uncommented

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.		●	●

4.1.2.16 snmpmibd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `snmpmibd` daemon on system startup. This is a dpi2 sub-agent that may be required if the server runs SNMP.

Rationale:

The `snmpmibd` daemon is a dpi2 sub-agent which manages a number of MIB variables. If `snmpd` is not required, it is recommended that it is disabled.

The specific MIB variables which are managed by `snmpmibd` are defined by numerous RFCs. Further details relating to these MIBS can be found in the URL below:

<https://www.ibm.com/docs/en/aix/7.1?topic=s-snmpmibd-daemon>

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/snmpmibd" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/snmpmibd "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s snmpmibd
```

This should yield the following output:

snmpmibd	tcpip	inoperative
----------	-------	-------------

Remediation:

- On AIX 7.1 and earlier comment out the `snmpmibd` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d snmpmibd
stopsrc -s snmpmibd
```

- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.snmpd
```





Default Value:

Enabled

References:

- <https://www.ibm.com/docs/en/aix/7.1?topic=s-snmpmibd-daemon>

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.			

4.1.2.17 *timed* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `timed` daemon on system startup. This is the old and obsolete UNIX time service.

Rationale:

The `timed` daemon is the old UNIX time service. Disable this service.

If time synchronization is required in your environment use `xntp`.

Audit:

- From the command prompt, execute the following command:

```
grep "start[[:blank:]]/usr/sbin/timed" /etc/rc.tcpip
```

This should yield the following output:

```
#start /usr/sbin/timed "$src_running"
```

- From the command prompt, execute the following command:

```
lssrc -s timed
```

This should yield the following output:

```
timed          tcpip          inoperative
```

Remediation:

- On AIX 7.1 and earlier comment out the `timed` entry in `/etc/rc.tcpip` and ensure service is stopped:

```
chrctcp -d timed  
stopsrc -s timed
```





- On AIX 7.2 and later remove the software:

```
installp -u bos.net.tcp.timed
```

Default Value:

Disabled

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.			

4.1.3 Boot phase: IPv6

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

IPv6, when active, is activated via calls in `/etc/rc.tcpip`

4.1.3.1 *autoconf6 (Automated)*

Profile Applicability:

- Level 2
- Level 1

Description:

This entry starts `autoconf6` on system startup. This is to automatically configure IPv6 interfaces at boot time.

Rationale:

`autoconf6` is used to automatically configure IPv6 interfaces at boot time. Running this service may allow other hosts on the same physical subnet to connect via IPv6, even when the network does not support it. You must disable this unless you utilize IPv6 on the server.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/autoconf6" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/autoconf6 ""
```

Remediation:








In `/etc/rc.tcpip`, comment out the `autoconf6` entry:

```
chrctcp -d autoconf6
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
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.			

4.1.3.2 *ndpd-host* (Automated)

Profile Applicability:

- Level 2
- Level 1

Description:

This entry starts `ndpd-host` on system startup. This is the Neighbor Discovery Protocol (NDP) daemon.

The `ndpd-host` command handles the default route, which includes the default router, the default interface, and the default interface address. However, the `ndpd-host` command does not overwrite the static default routes that are set on the host. When the daemon is stopped, the daemon cleans up the prefix addresses and the routes that are created during its lifetime.

Rationale:

The `ndpd-host` performs the client function of the NDP protocol.

- Unless the server utilizes (dynamic) IPv6 this utility is not required and should be disabled.
- Ipv6 static configuration is not affected by `ndpd-host`.

Impact:

When `IPv6` is active and `NDP` is used to get a non-link-local IPv6 address (link-local addresses begin with `fe80::`) it is also likely that the MTU size of the interface will change from **1500** to **1492**. Additionally, it may add default route to the IPv6 router it received it's address from. For example:

- BEFORE NDP

```

netstat -ni
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
...
en0 1500 192.168.129 192.168.129.71 105156791 0 49249083 1 0
en0 1500 fe80::dead:beef:fef7:6204 105156791 0 49249083 1 0

netstat -rn
Routing tables
Destination Gateway Flags Refs Use If Exp Groups

Route tree for Protocol Family 2 (Internet):
default 192.168.129.1 UG 23 35660110 en0 - -
127/8 127.0.0.1 U 2 22988 lo0 - -
192.168.129.0 192.168.129.71 UHSb 0 0 en0 - -
=>
192.168.129/24 192.168.129.71 U 12 13578475 en0 - -
192.168.129.71 127.0.0.1 UGHS 0 21471 lo0 - -
192.168.129.255 192.168.129.71 UHSb 0 0 en0 - -

Route tree for Protocol Family 24 (Internet v6):
default link#2 UC 0 0 en0 - -
::1%1 ::1%1 UH 0 19154 lo0 - -
...

```

- After NDP

```

netstat -ni
Name Mtu Network Address Ipkts Ierrs Opkts Oerrs Coll
...
en0 1492 192.168.129 192.168.129.71 105190883 0 49267729 1 0
en0 1492 BEEF:980:a9ea:1:dead:beef:fef7:6204 105190883 0 49267729
1 0
en0 1492 fe80::dead:beef:fef7:6204 105190883 0 49267729 1 0

netstat -nr
Routing tables
Destination Gateway Flags Refs Use If Exp Groups

Route tree for Protocol Family 2 (Internet):
default 192.168.129.1 UG 17 35724295 en0 - -
127/8 127.0.0.1 U 2 23044 lo0 - -
192.168.129.0 192.168.129.71 UHSb 0 0 en0 - -
=>
192.168.129/24 192.168.129.71 U 14 13622746 en0 - -
192.168.129.71 127.0.0.1 UGHS 0 21576 lo0 - -
192.168.129.255 192.168.129.71 UHSb 0 0 en0 - -

Route tree for Protocol Family 24 (Internet v6):
default fe80::dead:beef:fefa:4bfe UG 0 0 en0 -
-
::1%1 ::1%1 UH 0 19198 lo0 - -

```

Note: the IPv6 destination address is the link-local (fe80::) address of the IPv6 router.

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/ndpd-host" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/ndpd-host "$src_running"
```

Remediation:








In `/etc/rc.tcpip`, comment out the `ndpd-host` entry:

```
chrctcp -d ndpd-host
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
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.			

4.1.3.3 *ndpd-router* (Automated)

Profile Applicability:

- Level 2
- Level 1

Description:

This entry starts `ndpd-router` on system startup. This manages the Neighbor Discovery Protocol (NDP) for non kernel activities.

It receives Router Solicitations and sends Router Advertisements. It can also exchange routing information using the RIPng protocol.

Rationale:

The `ndpd-router` manages NDP for non-kernel activities. Unless the server utilizes IPv6, this is not required and should be disabled.

Impact:

This service is not needed unless the AIX host is actively exchanging routing information with IPv6 routers.

See: [manpage AIX 7.1 ndpd-router Daemon](#)

Audit:

From the command prompt, execute the following command:

```
grep "^#start[[:blank:]]/usr/sbin/ndpd-router" /etc/rc.tcpip
```

The above command should yield the following output:

```
#start /usr/sbin/ndpd-router "$src_running"
```

Remediation:








In `/etc/rc.tcpip`, comment out the `ndpd-router` entry:

```
chrctcp -d ndpd-router
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u></p> <p>Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></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><u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>			

4.1.4 NFS

Network File System (NFS) is a distributed filesystem protocol.

If a system does not need to act as either an NFS client or server, the first recommendations are to uninstall these services to reduce the attack surface. However, if the server acts as either an NFS server or NFS client there are further security recommendations to implement.

4.1.4.1 NFS - de-install NFS client (Automated)

Profile Applicability:

- Level 1

Description:

De-install NFS client if the server does not remotely mount NFS shares.

Rationale:

NFS is frequently exploited to gain unauthorized access to file and directories. Unless the server needs to act as an NFS server or client, the filesets should be de-installed.

Audit:

Ensure that the software has been successfully de-installed:

```
lsrpm -L |grep bos.net.nfs.client
```

The above command should yield no output.

Remediation:

Ensure that there are no current NFS client mounts:

```
mount |grep "nfs"  
cat /etc/filesystems |grep "nfs"
```

The above commands should yield no output.

De-install the NFS client software:

```
installp -u bos.net.nfs.client
```

Default Value:

N/A

Additional Information:

Reversion:

Re-install the software from the product DVD's

4.1.4.2 NFS - de-install NFS server (Automated)

Profile Applicability:

- Level 2

Description:

De-install NFS server if the server does not act as an NFS server to remote clients.

Rationale:

NFS is frequently exploited to gain unauthorized access to file and directories. Unless the server needs to act as an NFS server or client, the filesets should be de-installed.

Audit:

Ensure that the software has been successfully de-installed:

```
lsllpp -L |grep bos.net.nfs.server
```

The above command should yield no output.

Remediation:

Ensure that there are no current NFS exports:

```
cat /etc/exports
```

The above command should yield no output. Or the file should not exist.

De-install the NFS sever software:

```
installp -u bos.net.nfs.server
```

If there was an empty `/etc/exports` file, remove it:

```
rm /etc/exports
```

Default Value:

N/A

Additional Information:

Reversion:

Re-install the software from the product DVD's

4.1.4.3 NFS - enable both *nosuid* and *nodev* options on NFS client mounts (Automated)

Profile Applicability:

- Level 1

Description:

Disable suid/sgid program execution and/or access to system devices via permissions set on any mounted NFS filesystem.

Rationale:

Setting the `nosuid` and `nodev` options means that files on the NFS server cannot be used to gain privileged access on the client.

This hampers a malicious user from creating an attack vector on the server and then log onto an NFS client as a standard user and use the suid/sgid program to effectively become another user (especially root) on that client.

The `nodev` options blocks malicious/accidental (raw) access to system devices (e.g., `/dev/kmem`, `/dev/rhdisk0`). Access to devices is not exclusive to the `/dev` directory. Device access is so-called special-files that are defined as a Major, Minor device id's.

Audit:

For each NFS filesystem, ensure that the options have been changed to reflect the `nosuid` option:

```
lsnfsmnt -l | /usr/bin/egrep -v "^Name" | /usr/bin/grep -v "nosuid"  
lsnfsmnt -l | /usr/bin/egrep -v "^Name" | /usr/bin/grep -v "nodev"
```

Both commands should not yield the any output.

Remediation:

For each NFS mount, disable suid programs and device access. List the current NFS mounts:

```
lsnfsmnt -l | /usr/bin/egrep -v "^Name" | /usr/bin/grep -v "nosuid" | while  
read remote local host rest; do  
  chnfsmnt -d ${remote} -f ${local} -h ${host} -y -z  
done  
  
lsnfsmnt -l | /usr/bin/egrep -v "^Name" | /usr/bin/grep -v "nodev" | while  
read remote local host rest; do  
  chnfsmnt -d ${remote} -f ${local} -h ${host} -y -z  
done
```

NOTE: The NFS mount needs is re-mounted automatically by `chnfsmnt`.

NOTE: The second loop might not do anything as both loops set both `nosuid` (-y) and `nodev` (-z)

Default Value:

N/A

4.1.4.4 NFS - localhost removal (Automated)

Profile Applicability:

- Level 1

Description:

Remove any reference to localhost or localhost aliases from `/etc/exports`.

Rationale:

If the RPC portmapper has proxy forwarding enabled, which is a default setting in many vendor versions. You must not export your local filesystems back to the localhost, either by name or to the alias localhost, and you must not export to any netgroups of which your host is a member. If proxy forwarding is enabled, an attacker may carefully craft NFS packets and send them to the portmapper, which in turn, forwards them to the NFS server. As the packets come from the portmapper process, which runs as root, they appear to be coming from a trusted system. This configuration may allow anyone to alter and delete files at will.

Audit:

Re-review `/etc/exports` if the file was updated, to validate the changes:

```
cat /etc/exports
```

Remediation:

Remove any reference to localhost or localhost aliases in `/etc/exports`: Review the content of `/etc/exports` and check for localhost or localhost aliases:

```
cat /etc/exports
```

NOTE: If instances of localhost or localhost aliases are found, edit the file and remove them. Create a copy of `/etc/exports`:

```
cp -p /etc/exports /etc/exports.pre_cis
```

Edit the file:

```
vi /etc/exports
```

Edit the relevant NFS exports to remove the localhost access, for example:

```
/nfsexport sec=sys,rw,access=localhost:testserver
```

If `/etc/exports` is updated, as localhost references have been removed, update the current NFS export options:

```
exportfs -a
```

Default Value:

N/A

4.1.4.5 NFS - restrict NFS access (Automated)

Profile Applicability:

- Level 2

Description:

Only allow explicitly defined host access to NFS exported filesystems and directories.

Rationale:

The NFS server should be configured to only allow explicitly defined hosts to mount filesystems from the server. If an unauthorized host is denied the permission to mount a filesystem, then the unauthorized users on that host will not be able to access the server's files.

The default value of access allows any machine to mount any exported filesystems/directories.

Audit:

Examine exported directories for unmanaged (aka world) access:

```
showmount -e | grep "(everyone)" | wc -l
```

The desired output is:

```
0
```

Remediation:

Ensure that all exports defined in `/etc/exports` have explicit client access options which clearly define the host or hosts allowed access: Review the content of `/etc/exports` and that all exports have explicit access lists:

```
showmount -e | grep "(everyone)"
```

Ensure that each NFS export has an explicit access line, for example, modify:

```
/export/repo (everyone)
```

to:

```
/export/repo x071
```

- The option `-c` is used to specify clients permitted access:

```
chnfsexp -d /export/repo -c x071
```

Default Value:

N/A

Additional Information:

Reversion: Clear the client access specification by supplying the NULL string ("") as argument.

```
chnfsexp -d /export/repo -c ""
```

4.1.4.6 NFS - no_root_squash option (Automated)

Profile Applicability:

- Level 1

Description:

For each NFS export, ensure that the `anon` aka `root_squash` option is set to `-2` or `-1`.

Rationale:

Each NFS export on the server should have the `anon=-2` option set. With this (default) value `root` (`euclid==0`) is seen as the account `nobody`. When `anon=0` the remote root user has root access on the NFS mount.

By ensuring the export option `anon=-2` when a client process with `euclid==0` attempts to access (read, write, or delete) the NFS mount the server substitutes the UID to the server's `nobody` account. This means that the root user on the client cannot access or change files that only root on the server can access or change.

Many NFS servers call this `root_squash`. On AIX is is called `anon`. To be consistent with other benchmark terminology CIS recommends that `root_squash` is set on all exported filesystems.

On AIX the default value of any exported filesystem or directory for `anon` is `-2`. Thus, when `anon` is not set it's effective value is `-2`. Any other value has to be explicitly set.

As a more secure option you can set the option to `anon=-1`. This setting is accepted because it disables anonymous access. By default, secure NFS accepts non-secure requests as anonymous.

NOTE: The root user on the client can still use `su` to become any other user (change the `euclid`) and access and change that users files, assuming that the same user exists on the NFS server and owns files and/or directories in the NFS export.

Audit:

As `-2` is the default NFS export value, ensure that there are no explicit `anon=` options set in `/etc/exports`:

```
lsnfsexp | grep -v 'anon=-1' | grep anon=
```

The above should command should yield no output.

Remediation:

To change this value for all failing NFS exported filesystems:

```
lsnfsexp | grep -v 'anon=-1' | grep anon= | while read fs rest; do
  chnfsexp -d ${fs} -a -2
done
```

- The command `chnfsexp` re-exports the file or directory with the new settings active.

Default Value:

(blank) which is seen as -2 (nobody) effective setting `root_squash` by default.

4.1.4.7 NFS - secure NFS (Automated)

Profile Applicability:

- Level 2

Description:

For each NFS export, ensure that the secure option is selected.

Rationale:

Secure NFS uses DES encryption or Kerberos to authenticate hosts involved in RPC transactions. RPC is a protocol used by NFS to communicate requests between hosts. Secure NFS mitigates attempts by an attacker to spoof RPC requests by encrypting the time stamp in the RPC requests. A receiver successfully decrypts the time stamp and confirms that it is correct. This serves as a confirmation that the RPC request came from a trusted host.

Audit:

Ensure that the relevant `sec=` options set in `/etc/exports`:

```
lsnfsexp | grep sec=
```

The above command should return each export and the security mode of the export.

Remediation:

Use `chnfsexp` to change/validate this value for all NFS exported filesystems:

```
chnfsexp -d <fs> -S <sec>
```

The available security method options are:

- `sys` - UNIX authentication
- `dh` - DES authentication
- `none` - Use the anonymous ID if it has a value other than `-1`
- `krb5` - Kerberos. Authentication only
- `krb5i` - Kerberos. Authentication and integrity
- `krb5p` - Authentication, integrity, and privacy

Once all exported filesystems have been successfully validated or changed, re-export the filesystems and directories to activate the new options:

```
exportfs -a
```

Default Value:

N/A

Additional Information:

Reversion: Copy back the original `/etc/exports`:

```
cp -p /etc/exports.pre_cis /etc/exports
```

4.1.5 Inetd Services

The `inetd` service is initiated by `/etc/rc.tcpip` and, thereafter, managed by the AIX `SRC` subsystem.

The entries in this file (i.e., services managed by `inetd`) are started, on demand, when their registered IP protocol and port number are requested by a client (TCP connect).

Most, perhaps all, of these services may be either commented out, or even deleted from `/etc/inetd.conf`. In case all entries are disabled the activation of the `inetd` service (see sub-section `/etc/rc.tcpip` above) should also be disabled.

4.1.5.1 bootps (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the command `/usr/sbin/bootpd` when required. This service is used to provide boot partition data for a network boot. It uses the same UDP port as DHCP server `dhcpsd`.

The recommendation is to disable this service UNLESS you are operating a NIM server. When using NIM `bootps` as a service is accepted, but the preference would be to configure a DHCP server with the equivalent information.

Rationale:

The `bootpd` command implements an Internet Boot Protocol server.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep bootps| wc -l
```

The above command should yield the following output:

```
0
```

Remediation:





In `/etc/inetd.conf`, comment out the `bootps` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'daytime' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.2 *chargen* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `chargen` service when required. This service is used to test the integrity of TCP/IP packets arriving at the destination.

Rationale:

This `chargen` service is a character generator service and is used for testing the integrity of TCP/IP packets arriving at the destination. An attacker may spoof packets between machines running the `chargen` service and thus provide an opportunity for DoS attacks. You must disable this service unless you are testing your network.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep chargen | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:





In `/etc/inetd.conf`, comment out the `chargen` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'chargen' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.3 comsat (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `comsat` service.

The `comsat` daemon receives messages on a datagram port associated with the `biff` service specification.

The recommendation is to leave this service disabled.

Rationale:

The `comsat` daemon is the server that receives reports of incoming mail and notifies users if they have enabled this service with the `biff` command. Started by the `inetd` daemon, the `comsat` daemon is not meant to be used at the command line.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep comsat | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:





In `/etc/inetd.conf`, comment out the `comsat` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'comsat' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.4 daytime (Automated)

Profile Applicability:

- Level 1

Description:

The service should be disabled as it can leave the system vulnerable to DoS ping attacks.

This entry starts the `daytime` service when required. This provides the current date and time to other servers on a network.

Rationale:

This `daytime` service is a defunct time service, typically used for testing purposes only.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep daytime | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `daytime` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'daytime' -p tcp
chsubserver -r inetd -C /etc/inetd.conf -d -v 'daytime' -p udp
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.		●	●

4.1.5.5 discard (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `discard` service when required. This service is used as a debugging tool by setting up a listening socket which ignores the data it receives.

Rationale:

The `discard` service is used as a debugging and measurement tool. It sets up a listening socket and ignores data that it receives. This is a `/dev/null` service and is obsolete. This can be used in DoS attacks and therefore, must be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep discard | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `discard` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'discard' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Commented out

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.			

4.1.5.6 echo (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `echo` service when required. This service sends back data received by it on a specified port.

Rationale:

The `echo` service sends back data received by it on a specified port. This can be misused by an attacker to launch DoS attacks or Smurf attacks by initiating a data storm and causing network congestion. The service is used for testing purposes and therefore must be disabled if not required.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep echo | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `echo` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'echo' -p tcp
chsubserver -r inetd -C /etc/inetd.conf -d -v 'echo' -p udp
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.		●	●

4.1.5.7 exec (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is that `rexecd` is disabled. This service can be performed securely using OpenSSH.

This entry starts the `rexecd` daemon when required. This daemon executes a command from a remote system once the connection has been authenticated.

Rationale:

The `exec` service is used to execute a command sent from a remote server. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `rexecd` daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep exec | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `exec` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'exec' -p 'tcp6'  
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.8 finger (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `fingerd` daemon.

Rationale:

The `fingerd` daemon provides the server function for the `finger` command. This allows users to view real-time pertinent user login information on other remote systems. This service should be disabled as it may provide an attacker with a valid user list to target.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep finger | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `finger` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'finger' -p tcp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.1.5.9 ftp (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `ftpd` daemon when required. This service is used for transferring files from/to a remote machine.

The recommendation is that `ftp` is disabled and `sftp` is used as a replacement file and directory copying mechanism.

Rationale:

This `ftp` service is used to transfer files from or to a remote machine. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `ftpd` daemon should be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep -v tftp | grep ftp | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `ftp` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'ftp' -p 'tcp6'  
refresh -s inetd
```

Default Value:

Uncommented

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.		●	●

4.1.5.10 *imap2 (Automated)*

Profile Applicability:

- Level 1

Description:

This entry starts the `imap2` service when required.

Rationale:

The `imap2` service or Internet Message Access Protocol (IMAP) supports the IMAP4 remote mail access protocol. It works with `sendmail` and `bellmail`. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep imap2 | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `imap2` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'imap2' -p tcp
lssrc -s inetd && refresh -s inetd
```

Default Value:

Commented out

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.			

4.1.5.11 instsrv (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `instsrv` service when required. This service should be disabled.

Rationale:

The `instsrv` service is part of the Network Installation Tools, used for servicing servers running AIX 3.2.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep instsrv | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `instsrv` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'instsrv' -p 'tcp'
refresh -s inetd
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.1.5.12 klogin (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `klogin` service when required. This is a kerberized login service, which provides a higher degree of security over traditional `rlogin` and `telnet`.

Rationale:

The `klogin` service offers a higher degree of security than traditional `rlogin` or `telnet` by eliminating most clear-text password exchanges on the network. However, it is still not as secure as SSH, which encrypts all traffic. If you use `klogin` to login to a system, the password is not sent in clear text; however, if you `su` to another user, that password exchange is open to detection from network-sniffing programs. The recommendation is to utilize SSH wherever possible instead of `klogin`.

If the `klogin` service is used, you must use the latest kerberos version available and make sure that all the latest patches are installed.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep klogin | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `klogin` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'klogin' -p tcp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.13 kshell (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `kshell` service when required. This is a kerberized remote shell service, which provides a higher degree of security over traditional `rsh`.

Rationale:

The `kshell` service offers a higher degree of security than traditional `rsh` services. However, it still does not use encrypted communications. The recommendation is to utilize SSH wherever possible instead of `kshell`.

If the `kshell` service is used, you should use the latest kerberos version available and must make sure that all the latest patches are installed.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep kshell | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `kshell` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'kshell' -p tcp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.		●	●

4.1.5.14 login (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rlogin` daemon when required. This service authenticates remote user logins.

Rationale:

This `login` service is used to authenticate a remote user connection when logging in via the `rlogin` command. The username and password are passed over the network in clear text and therefore insecurely. Unless required the `rlogin` daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep rlogin | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `rlogin` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rlogin' -p tcp6  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Uncommented

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></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>			

4.1.5.15 netstat (Automated)

Profile Applicability:

- Level 1

Description:

This entry executes the command `netstat -f inet`. This service displays active IP connections on a server.

The recommendation is to leave this disabled.

Rationale:

The `netstat` command symbolically displays the contents of various network-related data structures for active connections.

This interface requests a report of statistics or address control blocks to those items specified by the `inet` aka `AF_INET` (ipv4) address family.

Audit:

The recommendation is that the `netstat` service is disabled. This command can be executed securely using OpenSSH.

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep netstat | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `netstat` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'netstat' -p 'tcp'
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.16 *ntalk* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `talkd` daemon when required. This service establishes a two-way communication link between two users, either locally or remotely.

Rationale:

This `ntalk` service is used to establish an interactive two-way communication link between two UNIX users. It is unlikely that there would be a requirement to run this type of service on a UNIX system. Unless required the `ntalk` service will be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep ntalk | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `ntalk` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'ntalk' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.		●	●

4.1.5.17 pcnfsd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `pcnfsd` daemon when required. This service is an authentication and printing program, which uses NFS to provide file transfer services.

Rationale:

The `pcnfsd` service is an authentication and printing program, which uses NFS to provide file transfer services. This service is vulnerable and exploitable and permits the machine to be compromised both locally and remotely. If PC NFS clients are required within the environment, Samba is recommended as an alternative software solution. The `pcnfsd` daemon predates Microsoft's release of SMB specifications. This service should therefore be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep pcnfsd | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `pcnfsd` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'pcnfsd' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.18 pop3 (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `pop3` service when required.

Rationale:

The `pop3` service provides a `pop3` server. It supports the `pop3` remote mail access protocol. It works with `sendmail` and `bellmail`. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
grep "^#pop3[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#pop3      stream  tcp        nowait    root      /usr/sbin/pop3d pop3d
```

Remediation:



In `/etc/inetd.conf`, comment out the `pop3` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'pop3' -p tcp
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.19 *rex*d (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rex`d service when required.

This service should be disabled if it is not required.

Rationale:

The `rex`d daemon executes programs for remote machines when a client issues a request to execute a program on a remote machine. The `inetd` daemon starts the `rex`d daemon from the `/etc/inetd.conf` file.

Non-interactive programs use standard file descriptors connected directly to TCP connections. Interactive programs use pseudo-terminals, similar to the login sessions provided by the `rlogin` command. The `rex`d daemon can use the network file system (NFS) to mount the file systems specified in the remote execution request. Diagnostic messages are normally printed on the console and returned to the requester.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]rex" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rex' -p 'tcp'
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.20 rquotad (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rquotad` service when required. This allows NFS clients to enforce disk quotas on locally mounted filesystems.

Rationale:

The `rquotad` service allows NFS clients to enforce disk quotas on file systems that are mounted on the local system. This service should be disabled if it is not required.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]rquotad" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf` and if running, refresh `inetd`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rquotad' -p 'udp'
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.21 rstatd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rstatd` daemon. This service is used to provide kernel statistics and other monitorable parameters such as CPU usage, system uptime, network usage etc.

This service should be disabled if not explicitly required by performance monitoring software to collect statistics.

Rationale:

The `rstatd` service is used to provide kernel statistics and other monitorable parameters pertinent to the system such as: CPU usage, system uptime, network usage etc.

An attacker may use this information in a DoS attack.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep rstatd | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `rstatd` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rstatd' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.22 rusersd (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rsusersd` daemon when required. This service provides a list of current users active on a system.

Rationale:

The `rusersd` service runs as `root` and provides a list of current users active on a system. An attacker may use this service to learn valid account names on the system. This is not an essential service and should be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]rusersd" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rusersd' -p 'udp'
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.23 rwalld (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rwalld` daemon when required. This service allows remote users to broadcast system wide messages.

Rationale:

The `rwalld` service allows remote users to broadcast system wide messages. The service runs as root and should be disabled unless absolutely necessary.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]rwalld" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'rwalld' -p 'udp'
refresh -s inetd
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.1.5.24 shell (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `rshd` daemon when required. This daemon executes a command from a remote system.

Rationale:

This `shell` service is used to execute a command from a remote server. The username and passwords are passed over the network in clear text and therefore insecurely. Unless required the `rshd` daemon will be disabled. This function, if required, should be facilitated through SSH.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]shell" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'shell' -p 'tcp6'  
refresh -s inetd
```

Default Value:

Enabled

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.			

4.1.5.25 *sprayd* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `sprayd` daemon when required. This service is used as a tool to generate UDP packets for testing and diagnosing network problems.

Rationale:

The `sprayd` service is used as a tool to generate UDP packets for testing and diagnosing network problems.

The service must be disabled if not explicitly required for network performance testing purposes as it can be used as a (Distributed) Denial of Service ((D)DoS) attack.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep sprayd | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `sprayd` entry and refresh the `inetd` process:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'sprayd' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.1.5.26 xmquery (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `xmquery` daemon when required.

Rationale:

This `xmquery` service provides near real-time network-based data monitoring and local recording from a given node.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]xmquery" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'xmquery' -p 'udp'
refresh -s inetd
```

Default Value:

Enabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.1.5.27 talk (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `talkd` daemon when required. This service establishes a two-way communication link between two users, either locally or remotely.

Rationale:

This `talk` service is used to establish an interactive two-way communication link between two UNIX users. It is unlikely that there would be a requirement to run this type of service on a UNIX system. Unless required the `talk` service will be disabled

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]talk" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'talk' -p 'udp'
refresh -s inetd
```

Default Value:

Enabled

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.			

4.1.5.28 telnet (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is that telnet is disabled and OpenSSH is used as a replacement mechanism.

This entry starts the `telnetd` daemon when required. This provides a protocol for command line access from a remote machine.

Rationale:

The `telnet` protocol passes username and password in clear text over the network in clear text and therefore insecurely.

This `telnet` service is used to service remote user connections. Historically, `telnet` was the most commonly used remote access method for UNIX servers. This has been replaced by OpenSSH (or no remote CLI access).

Unless required the `telnetd` daemon should be disabled.

Impact:

When OpenSSH is not available other steps should be examined, e.g., a bastion hosted environment where OpenSSH is used to get to the bastion host and then telnet from bastion to `telnet-only` server.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep telnet | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:



In `/etc/inetd.conf`, comment out the `telnet` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'telnet' -p 'tcp6'  
refresh -s inetd
```

Default Value:

Enabled

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.			

4.1.5.29 tftp (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `tftp` service when required.

Rationale:

The `tftp` service allows remote systems to download or upload files to the `tftp` server without any authentication. It is therefore a service that should not run, unless needed. One of the main reasons for requiring this service to be activated is if the host is a NIM master. However, the service can be enabled and then disabled once a NIM operation has completed, rather than left running permanently.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]tftp" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'tftp' -p 'udp6'  
refresh -s inetd
```

Default Value:

Disabled

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.			

4.1.5.30 time (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `time` service when required. This service can be used to synchronize system clocks.

Rationale:

The `time` service is an obsolete process used to synchronize system clocks at boot time. This has been superseded by NTP, which should be used if time synchronization is necessary. Unless required the `time` service will be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]time" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'time' -p 'tcp'
chsubserver -r inetd -C /etc/inetd.conf -d -v 'time' -p 'udp'
refresh -s inetd
```

Default Value:

Enabled

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.			

4.1.5.31 uucp (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `uucp` service when required. This service facilitates file copying between networked servers.

Rationale:

The `uucp` (UNIX to UNIX Copy Program), service allows users to copy files between networked machines. Unless an application or process requires UUCP this should be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep "[[:blank:]]uucp" | wc -l
```

The above command should yield:

```
0
```

Remediation:



Use `chsubserver` to disable this service in `/etc/inetd.conf`:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'uucp' -p 'tcp'
refresh -s inetd
```

Default Value:

Enabled

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.			

4.2 Network Options: '/usr/sbin/no'

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

We cannot rely on the infrastructure network defenses (CIS v8 Control #12 and #13) to be perfect. Adversaries continue to evolve and mature, as they share, or sell, information among their community on exploits and bypasses to security controls. Even if security tools work “as advertised,” it takes an understanding of the enterprise risk posture to configure, tune, and log them to be effective.

AIX Network Options Hardening

This section of the benchmark is limited to the hardening of standard TCP/IP tuning parameters using the command `no` (network options). These *host-based* settings can help mitigate risks such as SYN, source routing and smurf attacks. This is seen as a second line defense as infrastructure configuration (e.g., enterprise firewalls) should be configured as a first-line defense to safeguard against attacks via the network.

Being *host-based* these recommendations do not currently map directly to a CIS Control. However, they are directly related to the concept of a secure installation and system integrity.

The recommendations here are all managed by the program `/usr/sbin/no`.

We do not make a difference between IPv4 and IPv6 for these settings.

4.2.1 *clean_partial_conns* (Automated)

Profile Applicability:

- Level 1

Description:

The `clean_partial_conns` parameter determines whether or not the system is open to SYN attacks. This parameter, when enabled, clears down connections in the SYN RECEIVED state after a set period of time. This attempts to stop DoS attacks when a hacker may flood a system with SYN flag set packets.

Rationale:

The `clean_partial_conns` parameter will be set to 1, to clear down pending SYN received connections after a set period of time.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "clean_partial_conns[[:blank:]]=[[:blank:]]1"
```

The above command should yield the following output:

```
clean_partial_conns = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `clean_partial_conns` entry:

```
no -p -o clean_partial_conns=1
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

0

4.2.2 *bcastping* (Automated)

Profile Applicability:

- Level 1

Description:

The `bcastping` parameter determines whether the system responds to ICMP echo packets sent to the broadcast address.

Rationale:

The `bcastping` parameter will be set to 0. This means that the system will not respond to ICMP packets sent to the broadcast address. By default, when this is enabled the system is susceptible to smurf attacks, where a hacker utilizes this tool to send a small number of ICMP echo packets. These packets can generate huge numbers of ICMP echo replies and seriously affect the performance of the targeted host and network. This parameter will be disabled to ensure protection from this type of attack.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "bcastping[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
bcastping = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `bcastping` entry:

```
no -p -o bcastping=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.3 *directed_broadcast* (Automated)

Profile Applicability:

- Level 1

Description:

The `directed_broadcast` parameter determines whether or not the system allows a directed broadcast to a network gateway.

Rationale:

The `directed_broadcast` parameter will be set to 0, to prevent directed broadcasts being sent network gateways. This would prevent a redirected packet from reaching a remote network.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "directed_broadcast[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
directed_broadcast = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `directed_broadcast` entry:

```
no -p -o directed_broadcast=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.4 icmpaddressmask (Automated)

Profile Applicability:

- Level 1

Description:

The `icmpaddressmask` parameter determines whether the system responds to an ICMP address mask ping.

Rationale:

The `icmpaddressmask` parameter will be set to 0, This means that the system will not respond to ICMP address mask request pings. By default, when this is enabled the system is susceptible to source routing attacks. This is typically a feature performed by a device such as a network router and should not be enabled within the operating system.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "icmpaddressmask[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
icmpaddressmask = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `icmpaddressmask` entry:

```
no -p -o icmpaddressmask=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.5 *ipforwarding* (Automated)

Profile Applicability:

- Level 1

Description:

The `ipforwarding` parameter determines whether or not the system forwards TCP/IP packets.

Rationale:

The `ipforwarding` parameter will be set to 0, to ensure that redirected packets do not reach remote networks. This should only be enabled if the system is performing the function of an IP router. This is typically handled by a dedicated network device.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipforwarding[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipforwarding = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipforwarding` entry:

```
no -p -o ipforwarding=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

0

4.2.6 *ipignoreredirects* (Automated)

Profile Applicability:

- Level 1

Description:

The `ipignoreredirects` parameter determines whether or not the system will process IP redirects.

Rationale:

The `ipignoreredirects` will be set to 1, to prevent IP re-directs being processed by the system.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipignoreredirects[[:blank:]]=[[:blank:]]1"
```

The above command should yield the following output:

```
ipignoreredirects = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipignoreredirects` entry:

```
no -p -o ipignoreredirects=1
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

0

4.2.7 *ipsendredirects* (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsendredirects` parameter determines whether or not the system forwards re-directed TCP/IP packets.

Rationale:

The `ipsendredirects` parameter will be set to 0, to ensure that redirected packets do not reach remote networks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsendredirects[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsendredirects = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsendredirects` entry:

```
no -p -o ipsendredirects=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.8 *ipsrouteforward* (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsrouteforward` parameter determines whether or not the system forwards IPV4 source-routed packets.

Rationale:

The `ipsrouteforward` will be set to 0, to prevent source-routed packets being forwarded by the system. This would prevent a hacker from using source-routed packets to bridge an external facing server to an internal LAN, possibly even through a firewall.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrouteforward[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrouteforward = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrouteforward` entry:

```
no -p -o ipsrouteforward=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.9 ipsrcrouterecv (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsrcrouterecv` parameter determines whether the system accepts source routed packets.

Rationale:

The `ipsrcrouterecv` parameter will be set to 0, This means that the system will not accept source routed packets. By default, when this is enabled the system is susceptible to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcrouterecv[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcrouterecv = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcrouterecv` entry:

```
no -p -o ipsrcrouterecv=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.10 ipsrcroutesend (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsrcroutesend` parameter determines whether or not the system can send source-routed packets.

Rationale:

The `ipsrcroutesend` parameter will be set to 0, to ensure that any local applications cannot send source routed packets.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcroutesend[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcroutesend = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcroutesend` entry:

```
no -p -o ipsrcroutesend=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.11 *ip6srcrouteforward* (Automated)

Profile Applicability:

- Level 1

Description:

The `ip6srcrouteforward` parameter determines whether or not the system forwards IPV6 source-routed packets.

Rationale:

The `ip6srcrouteforward` parameter will be set to 0, to prevent source-routed packets being forwarded by the system. This would prevent a hacker from using source-routed packets to bridge an external facing server to an internal LAN, possibly even through a firewall.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ip6srcrouteforward[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ip6srcrouteforward = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ip6srcrouteforward` entry:

```
no -p -o ip6srcrouteforward=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.12 *nfs_use_reserved_ports* (Automated)

Profile Applicability:

- Level 1

Description:

The `portcheck` and `nfs_use_reserved_ports` parameters force the NFS server process on the local system to ignore NFS client requests that do not originate from the privileged ports range (ports less than 1024).

Rationale:

The `portcheck` and `nfs_use_reserved_ports` parameters will both be set to 1. This value means that NFS client requests that do not originate from the privileged ports range (ports less than 1024) will be ignored by the local system.

Audit:

From the command prompt, execute the following commands:

```
nfsso -a |egrep "(portcheck|nfs_use_reserved_ports)[:,blank:]=[:,blank:::]1"
```

The above commands should yield the following output:

```
portcheck = 1
nfs_use_reserved_ports = 1
```

Remediation:

In `/etc/tunables/nextboot`, add the `portcheck` and `nfs_use_reserved_ports` entries:

```
nfsso -p -o portcheck=1
nfsso -p -o nfs_use_reserved_ports=1
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

0

4.2.13 *nonlocsrcroute* (Automated)

Profile Applicability:

- Level 1

Description:

The `nonlocsrcroute` parameter determines whether the system allows source routed packets to be addressed to hosts outside of the LAN.

Rationale:

The `nonlocsrcroute` parameter will be set to 0. This means that the system will not allow source routed packets to be addressed to hosts outside of the LAN. By default, when this is enabled the system is susceptible to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "nonlocsrcroute[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
nonlocsrcroute = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `nonlocsrcroute` entry:

```
no -p -o nonlocsrcroute=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.14 sockthresh (Automated)

Profile Applicability:

- Level 1

Description:

The `sockthresh` parameter value determines what percentage of the total memory allocated to networking, set via `thewall`, can be used for sockets.

Rationale:

The `sockthresh` parameter will be set to `60`. This means that 60% of network memory can be used to service new socket connections, the remaining 40% is reserved for existing sockets. This ensures a quality of service for existing connections.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "sockthresh[[:blank:]]=[[:blank:]]60"
```

The above command should yield the following output:

```
sockthresh = 60
```

Remediation:

In `/etc/tunables/nextboot`, add the `sockthresh` entry:

```
no -p -o sockthresh=60
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

N/A

4.2.15 *tcp_pmtu_discover* (Automated)

Profile Applicability:

- Level 1

Description:

The `tcp_pmtu_discover` parameter controls whether TCP MTU discovery is enabled.

Rationale:

The `tcp_pmtu_discover` parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When `tcp_pmtu_discover` is enabled, it leaves the system vulnerable to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "tcp_pmtu_discover[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
tcp_pmtu_discover = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_pmtu_discover` entry:

```
no -p -o tcp_pmtu_discover=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.16 *tcp_tcpsecure* (Automated)

Profile Applicability:

- Level 1

Description:

The `tcp_tcpsecure` parameter value determines if the system is protected from three specific TCP vulnerabilities: The values are **OR**ed together. If all three values are to be set the value to set is: 1|2|4 (or 7).

- Fake SYN - This is used to terminate an established connection. A `tcp_tcpsecure` bit-value of 1 protects the system from this vulnerability.
- Fake RST - As above, this is used to terminate an established connection. A `tcp_tcpsecure` bit-value of 2 protects the system from this vulnerability.
- Fake data - A hacker may inject fake data into an established connection. A `tcp_tcpsecure` bit-value of 4 protects the system from this vulnerability.

Rationale:

The `tcp_tcpsecure` parameter should be set to 7. This means that the system will be protected from TCP connection reset and data integrity attacks.

Audit:

From the command prompt, execute the following command:

```
no -o tcp_tcpsecure
```

The above command should yield the following output:

```
tcp_tcpsecure = 7
```

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_tcpsecure` entry:

```
no -p -o tcp_tcpsecure=7
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`.

Default Value:

```
tcp_tcpsecure = 0
```

4.2.17 *udp_pmtu_discover* (Automated)

Profile Applicability:

- Level 1

Description:

The `udp_pmtu_discover` parameter controls whether MTU discovery is enabled.

Rationale:

The `udp_pmtu_discover` parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When `udp_pmtu_discover` is enabled, it leaves the system vulnerable to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "udp_pmtu_discover[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
udp_pmtu_discover = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `udp_pmtu_discover` entry:

```
no -p -o udp_pmtu_discover=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

4.2.18 ip6forwarding (Automated)

Profile Applicability:

- Level 1

Description:

The `ip6forwarding` parameter determines whether or not the system forwards IPv6 TCP/IP packets.

Rationale:

The `ip6forwarding` parameter will be set to 0, to ensure that redirected packets do not reach remote networks. This should only be enabled if the system is performing the function of an IP router. This is typically handled by a dedicated network device.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ip6forwarding[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ip6forwarding = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ip6forwarding` entry:




```
no -p -o ip6forwarding=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

4.3 Implement and Manage a Firewall (bos.net.ipsec)

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, AIX uses the fileset `bos.net.ipsec`.

4.3.1 Ensure that IP Security is available (Automated)

Profile Applicability:

- Level 1

Description:

In order to configure IP Security, the kernel extension and devices must first be loaded

Rationale:

IP Security is not enabled out of the box on an AIX install, so must be enabled before further changes can be made

Impact:

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

Audit:

Execute the following command:

```
lsdev -C -c ipsec
```

It should return

```
ipsec_v4 Available IP Version 4 Security Extension
ipsec_v6 Available IP Version 6 Security Extension
```

Remediation:




Enable IP Security with default Rule Permit and activate IPsec logging to syslog

```
# Create the IPsec devices
mkdev -c ipsec -t 4
mkdev -c ipsec -t 6
# Activate with default rule Permit
mkfilt -v4 -z p
mkfilt -v6 -z p
# Start IPsec filtering
mkfilt -g start
```

References:

1. <https://www.ibm.com/docs/en/aix/7.2?topic=feature-loading-ip-security>

CIS Controls:

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

4.3.2 Ensure loopback traffic is blocked on external interfaces (Automated)

Profile Applicability:

- Level 1

Description:

The loopback interface will accept traffic unconditionally. 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 traffic is denied on all interfaces:

```
lsfilt -v 4 -O | grep 127.0.0.0
lsfilt -v 6 -O | grep ::1
```

Remediation:

```
genfilt -v 4 -a D -s 127.0.0.0 -m 255.0.0.0 -l Y -i all
genfilt -v 6 -a D -s ::1 -m 128 -l Y -i all
```

CIS Controls:

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

4.3.3 Ensure that IPsec filters are active (Automated)

Profile Applicability:

- Level 1

Description:

Rules added to the filter list are not enabled automatically. Filters need to be activated and/or updated after changes to the ODM filter database.

Rationale:

The filters must be active in order for IP Security to protect the system.

Impact:

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

Ensure you have access to the console (e.g., via HMC) while developing and testing IPsec rule modifications.

Audit:

Execute both commands. There should not be any output.

```
lsfilt -v4 -O -a | grep -q inactive && print IPv4 ipsec filtering inactive
lsfilt -v6 -O -a | grep -q inactive && print IPv6 ipsec filtering inactive
```




Remediation:

```
mkfilt -u
mkfilt -g start
```

Additional Information:

In the event that you are locked out of the system by firewall rules, run `mkfilt -d` from the console to deactivate all filters

CIS Controls:

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

4.4 Remove or Disable Weak/Defunct Network Services

This section provides guidance on the so-called historical services. These are services that are still installed - often by default - but the base recommendation is to uninstall the services whenever possible, and disable them when they cannot be removed.

The basic recommendations: remove or disable falls under IG1. Some of these services may be used, after proper configuration. Such a service should be viewed as part of an IG2 or IG3 solution.

In another section recommendations have already been made to disable the remote services in `/etc/inetd.conf`. While this stops the server from accepting connections disabling the binaries themselves ensures connections from the server to another host are further restricted, i.e., the daemons themselves are fully disabled.

There are many (well) known security vulnerabilities related to these services and they are a primary target for any DoS attack.

In short, unless otherwise required, the IG1 recommendation is that the services and daemons covered in this section and its subsections are either removed from the system or have their file mode permissions removed.

4.4.1 NIS

Network Information Service (NIS) or Yellow Pages (YP), is a client/server directory service protocol used for distributing system configuration data, such as: users, groups, passwords and hosts between computers in a network. This is typically done in larger environments to centralize the management of this data. If the NIS software is installed but not configured, an attacker can cripple a machine by starting NIS. In environments where NIS is utilized, tools like ypsnarf allow an attacker to grab the contents of your NIS maps, providing large amounts of information about your site.

The first recommendation in this section is to de-install NIS, if it is installed, to lockdown this service. However, if NIS is used in the environment it is recommended that NIS+ is used instead. NIS+ is structured differently from NIS and supports secure and encrypted RPC, which resolves many of the security issues.

The configuration of NIS+ is not within the scope of this benchmark; however the links below can be used for initial reference:

AIX 7.1:

[NIS+ transition](#)

4.4.1.1 NIS - de-install NIS client (Automated)

Profile Applicability:

- Level 2

Description:

If NIS is not used in the environment, disable the NIS client and de-install the software.

Rationale:

As NIS is extremely insecure, the NIS client packages must be removed from the system unless absolutely needed.

Audit:

Ensure that the software has been successfully de-installed:

```
lsrpm -L |grep "bos.net.nis.client"
```

The above command should yield no output.

Remediation:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS client software:

```
installp -u bos.net.nis.client
```

Default Value:

N/A

Additional Information:

Reversion:

Re-install the software from the product DVD's.

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.		●	●

4.4.1.2 NIS - de-install NIS server (Automated)

Profile Applicability:

- Level 2

Description:

If NIS is not used in the environment, disable the NIS server and de-install the software.

Rationale:

As NIS is extremely insecure, the NIS server packages must be removed from the system unless absolutely needed.

Audit:

Ensure that the software has been successfully de-installed:

```
lsrpm -L |grep "bos.net.nis.server"
```

The above command should yield no output.

Remediation:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS server software:

```
installp -u bos.net.nis.server
```

Default Value:

N/A

Additional Information:

Reversion:

Re-install the software from the product DVD's.

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.		●	●

4.4.1.3 NIS - remove NIS markers from password and group files (Automated)

Profile Applicability:

- Level 2

Description:

If NIS has been de-installed in the environment, or has historically been used, ensure the + markers are removed from `/etc/passwd` and `/etc/group`.

Rationale:

The + entries in `/etc/passwd` and `/etc/group` were used as markers to insert data from a NIS map. These entries may provide an avenue for attackers to gain privileged access on the system. The + entries must be deleted if they still exist.

Audit:

Re-run the command:

```
grep "^+" /etc/passwd /etc/group
```

The command above should yield no output.

Remediation:

Examine the `/etc/passwd` and `/etc/group` files:

```
grep "^+" /etc/passwd /etc/group
```

If the above command yields output, delete the + line:

```
vi /etc/passwd
vi /etc/group
```

Default Value:

N/A

Additional Information:

Reversion:

Add the + line back to the same point in the file/s:

```
vi /etc/passwd
vi /etc/group
```

4.4.1.4 NIS - restrict NIS server communication (Automated)

Profile Applicability:

- Level 2

Description:

If NIS must be used in the environment, limit access to the NIS data to specific subnets.

Rationale:

By default the NIS server will authenticate all IP addresses if the `/var/yp/securenets` file does not exist, or exists without any subnets defined. The `/var/yp/securenets` file contains a list of subnets that are considered trusted and are allowed to access NIS data using the `ypserv` and `ypxfrd` daemons. This is a user-created file that resides on a NIS master server and any slave servers. Without configuring this file, anyone with knowledge of the NIS server address and the domain name, can obtain NIS served data, including the contents of the `/etc/passwd` file. Hence, it is recommended that the `/var/yp/securenets` file is configured to restrict access.

Audit:

Review the content of the `/var/yp/securenets` file:

```
cat /var/yp/securenets
```

NOTE: A test should be performed from an allowed client and non-allowed subnet to validate the `securenets` configuration

Remediation:

Create and secure the `/var/yp/securenets` file (if it does not already exist):

```
touch /var/yp/securenets
chmod u=rw,go= /var/yp/securenets
chown root:system /var/yp/securenets
```

Edit the file:

```
vi /var/yp/securenets
```

Add the allowed subnets:

```
255.255.255.0 128.311.10.0
```

NOTE: The format of the file is netmask netaddr as shown in the example above.
Explicitly define all valid network subnets (one entry per line).
Stop and start NIS to implement the configuration changes:

```
stopsrc -g yp
startsrc -g yp
```

Default Value:

N/A

Additional Information:

Reversion:

Remove the `/var/yp/securenets` file:

```
rm /var/yp/securenets
```

4.4.2 Remote command lockdown (Automated)

Profile Applicability:

- Level 2

Description:

Removes all permissions from the remote service commands: `rsh`, `rlogin` and `rcp`.

Rationale:

This effectively disables the following commands, for all users:

- `/usr/bin/rcp`
- `/usr/bin/rlogin`
- `/usr/bin/rsh`

These remote services send usernames and passwords in clear text and should not be used. Unless required these binaries will be disabled for all users. The SSH suite of commands should be utilized to provide equivalent functionality

Audit:

From the command prompt, execute the following commands:

```
ls -l /usr/bin/rcp | awk '{print $1}'
ls -l /usr/bin/rlogin | awk '{print $1}'
ls -l /usr/bin/rsh | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
-----
```

Remediation:

Use the `chmod` command to remove all permissions on the remote services:

```
chmod ugo= /usr/bin/rcp
chmod ugo= /usr/bin/rlogin
chmod ugo= /usr/bin/rsh
```

Default Value:

N/A

4.4.3 Removal of entries from /etc/hosts.equiv (Automated)

Profile Applicability:

- Level 2

Description:

This process removes all entries from the `/etc/hosts.equiv` file.

Rationale:

The `/etc/hosts.equiv` file can be used to circumvent normal login or change control procedures. The existence of this file, with the relevant entries, can allow remote user access to a system bypassing local user and password authentication. Unless required all entries will be removed from this file.

Audit:

From the command prompt, execute the following command:

```
grep -v "^s*#" /etc/hosts.equiv
```

The above command should not yield output

Remediation:

Remove all entries from the `/etc/hosts.equiv` file:

```
sed '/^s*$/d; s/^\(s*[^#].*\)/#\1/' /etc/hosts.equiv >
/etc/hosts.equiv.work
mv hosts.equiv.work hosts.equiv
chown root:system /etc/hosts.equiv
chmod 644 /etc/hosts.equiv
```

Note: the above command removes blank lines and comments out any non commented entries.

Default Value:

N/A

4.4.4 Removal of `.rhosts` and `.netrc` files (Automated)

Profile Applicability:

- Level 2

Description:

This recommendation removes all instances of `.rhosts` and `.netrc` files from the system.

Rationale:

The `.rhosts` and `.netrc` files can be used to circumvent normal login or change control procedures. The existence of such files, with the relevant entries, can allow remote user access to a system bypassing local user and password authentication. Unless required these files will be removed from all user home directories.

Audit:

From the command prompt, execute the following commands:

```
find / -name ".netrc" -print
find / -name ".rhosts" -print
```

The above commands should not yield output

Remediation:

Remove the `.rhosts` and `.netrc` files from all user home directories:

```
find / -name ".netrc" -exec rm {} \;
find / -name ".rhosts" -exec rm {} \;
```

Default Value:

N/A

4.4.5 Remote daemon lockdown (Automated)

Profile Applicability:

- Level 2

Description:

Removes all permissions from the remote service daemons: `rlogind`, `rshd` and also `tftpd`.

Rationale:

This effectively disables the following daemons, for all users:

- `/usr/sbin/rlogind`
- `/usr/sbin/rshd`
- `/usr/sbin/tftpd`

These remote services both send and receive usernames and passwords in clear text and should not be used. Unless required these daemons will be disabled for all users.

Audit:

From the command prompt, execute the following commands:

```
ls -l /usr/sbin/rlogind | awk '{print $1}'
ls -l /usr/sbin/rshd | awk '{print $1}'
ls -l /usr/sbin/tftpd | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
-----
```

Remediation:



Use the `chmod` command to remove all permissions on the remote services:

```
chmod ugo= /usr/sbin/rlogind
chmod ugo= /usr/sbin/rshd
chmod ugo= /usr/sbin/tftpd
```

Default Value:

N/A

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.			

4.5 Standard Services and Applications

This sub-section presents recommendations on the configuration of standard applications and/or services.

The focus is on Application settings that enhance application security (thereby indirectly enhancing system integrity).

4.5.1 Common Desktop Environment (CDE)

CDE has a history of security problems and should be disabled or removed. However, if the server, better workstation, has a graphics adapter and CDE is used as the graphical user interface (GUI) then the recommendations in this section should be followed to enhance security.

If CDE is not required the recommendation is that the filesets are de-installed to avoid exposure to potential security vulnerabilities. The recommendations that remain are only scored when CDE is installed.

4.5.1.1 CDE - de-installing CDE (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to de-install CDE aka X11.Dt from the system, assuming that it is not required and is already installed.

Rationale:

CDE has a history of security problems and should be disabled.

NOTE: If CDE is required, it is vital to patch the software and consider TCP Wrappers to further enhance security.

Audit:

Validate the de-installation of the software:

```
lslpp -L |grep -i X11.Dt
```

The above command should yield no output.

Remediation:

Identity if **CDE** is already installed:

```
lslpp -L |grep -i X11.Dt
```

If there are CDE filesets installed - de-install them if CDE is not required. For each fileset preview the de-installation:

```
installp -up <fileset name>
```

Review the fileset removal preview output, paying particular attention to the other pre-requisites that will also be removed. Typically only `X11.Dt` filesets should be de-installed as pre-requisites. Once reviewed, de-install the fileset and pre-requisites:

```
installp -ug <fileset name>
```

NOTE: Repeat until all CDE related filesets are de-installed

Default Value:

N/A

Additional Information:

Reversion:

Re-install the CDE software from the AIX media.

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>2.6 Address unapproved software</u> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

4.5.1.2 /etc/inetd.conf - cmsd (Automated)

Profile Applicability:

- Level 2

Description:

This entry starts the `cmsd` service when required. This is a calendar and appointment service.

Rationale:

The `cmsd` service is utilized by CDE to provide calendar functionality. If CDE is not required, this service should be disabled.

Audit:

From the command prompt, execute the following command:

```
lssrc -s inetd -l | grep cms | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:

In `/etc/inetd.conf`, comment out the `cmsd` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'cmsd' -p 'tcsunrpc_udp'  
refresh -s inetd
```

Default Value:

Uncommented

4.5.1.3 CDE - disabling dtlogin (Automated)

Profile Applicability:

- Level 2

Description:

Do not start CDE automatically on system boot.

Rationale:

The implementation of the customized aixpert XML file disables CDE if there is not a graphical console attached to the system. If there is a graphical console or the XML file has not been executed, consider disabling CDE anyway.

Audit:

Validate that CDE start-up is disabled

```
lsitab dt
```

The above command should yield no output.

Remediation:

Disable CDE start up:

```
/usr/dt/bin/dtconfig -d
```

NOTE: If CDE is not installed the command will not be found

Default Value:

N/A



Additional Information:

Reversion:

To re-configure the auto-start of the CDE software:

```
/usr/dt/bin/dtconfig -e
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.5.1.4 /etc/inetd.conf - dtspc (Automated)

Profile Applicability:

- Level 2

Description:

This entry starts the `dtspc` service when required. This service is used in response to a CDE client request.

Rationale:

The `dtspc` service deals with the CDE interface of the X11 daemon. It is started automatically by the `inetd` daemon in response to a CDE client requesting a process to be started on the daemon's host. This makes it vulnerable to buffer overflow attacks, which may allow an attacker to gain root privileges on a host. This service must be disabled unless it is absolutely required.

Audit:

From the command prompt, execute the following command:

```
grep "^#dtspc[[:blank:]]" /etc/inetd.conf
```

The above command should yield the following output:

```
#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

Remediation:



In `/etc/inetd.conf`, comment out the `dtspc` entry:

```
chsubserver -r inetd -C /etc/inetd.conf -d -v 'dtspc' -p 'tcp'
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 <u>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.			

4.5.1.5 CDE - sgid/suid binary lockdown (Automated)

Profile Applicability:

- Level 1

Description:

CDE buffer overflow vulnerabilities may be exploited by a local user to obtain root privilege via `suid/sgid` programs owned by `root:bin` or `root:sys`.

Rationale:

CDE has been associated with major security risks, most of which are buffer overflow vulnerabilities. These vulnerabilities may be exploited by a local user to obtain root privilege via `suid/sgid` programs owned by `root:bin` or `root:sys`. It is recommended that the CDE binaries have the `suid/sgid` removed.

Audit:

Validate the permissions of the binaries:

```
ls -l /usr/dt/bin/dtaction | awk '{print $1 " " $3 " " $4 " " $9}'  
ls -l /usr/dt/bin/dtappgather | awk '{print $1 " " $3 " " $4 " " $9}'  
ls -l /usr/dt/bin/dtprintinfo | awk '{print $1 " " $3 " " $4 " " $9}'  
ls -l /usr/dt/bin/dtsession | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

-r-xr-xr-x	root	sys	/usr/dt/bin/dtaction
-r-xr-xr-x	root	bin	/usr/dt/bin/dtappgather
-r-xr-xr-x	root	bin	/usr/dt/bin/dtprintinfo
-r-xr-xr-x	root	bin	/usr/dt/bin/dtsession

Remediation:

Remove the `suid/sgid` from the following CDE binaries:

```
chmod ug-s /usr/dt/bin/dtaction  
chmod ug-s /usr/dt/bin/dtappgather  
chmod ug-s /usr/dt/bin/dtprintinfo  
chmod ug-s /usr/dt/bin/dtsession
```

Default Value:

N/A

4.5.1.6 CDE - remote GUI login disabled (Automated)

Profile Applicability:

- Level 2

Description:

The XDMCP service allows remote systems to start local X login sessions.

Rationale:

The XDMCP service should be disabled unless there is a requirement to allow remote X servers to start login sessions. If the ability to host remote X servers is not required, disable the service.

Audit:

Validate the change to `/etc/dt/config/Xconfig`:

```
grep "^Dtlogin.requestPort:[[:space:]]" /etc/dt/config/Xconfig
```

The command above should yield the following output:

```
Dtlogin.requestPort:      0
```

Remediation:

Copy `/usr/dt/config/Xconfig` to `/etc/dt/config` if it does not already exist:

```
ls -l /etc/dt/config/Xconfig
```

If the file does not exist, create it:

```
mkdir -p /etc/dt/config  
cp /usr/dt/config/Xconfig /etc/dt/config
```

Disable remote X sessions from being started:

```
vi /etc/dt/config/Xconfig
```

Replace:

```
# Dtlogin.requestPort:      0
```

With:

```
Dtlogin.requestPort:      0
```

Default Value:

Enabled

Additional Information:

Reversion:



Comment out the option:

```
vi /etc/dt/config/Xconfig
```

Reflect:

```
# Dtlogin.requestPort: 0
```

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.			

4.5.1.7 CDE - screensaver lock (Automated)

Profile Applicability:

- Level 1

Description:

The default timeout is 30 minutes of keyboard and mouse inactivity before a password protected screensaver is invoked by the CDE session manager.

Rationale:

The default timeout of 30 minutes prior to a password protected screensaver being invoked is too long. The recommendation is to set this to 10 minutes to protect from unauthorized access on unattended systems.

Audit:

Validate the changes to the `sys.resources` files:

```
egrep "dtsession\*saverTimeout:|dtsession\*lockTimeout:"  
/etc/dt/config/*/sys.resources
```

The above command should yield a similar output to the following:

```
/etc/dt/config/en_US/sys.resources:dtsession*saverTimeout: 10  
/etc/dt/config/en_US/sys.resources:dtsession*lockTimeout: 10
```

Remediation:




Set the default timeout parameters `dtsession*saverTimeout:` and `dtsession*lockTimeout:`

```
for file in /usr/dt/config/*/sys.resources; do  
    dir=`dirname $file | sed -e s/usr/etc/`  
    mkdir -p $dir  
    echo 'dtsession*saverTimeout: 10' >> $dir/sys.resources  
    echo 'dtsession*lockTimeout: 10' >> $dir/sys.resources  
done
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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.			

4.5.1.8 CDE - login screen hostname masking (Automated)

Profile Applicability:

- Level 1

Description:

The `Dtlogin*greeting.labelString` parameter is the message displayed in the first dialogue box on the CDE login screen. This is where the username is entered.

The `Dtlogin*greeting.persLabelString` is the message displayed in the second dialogue box on the CDE login screen. This is where the password is entered.

Rationale:

Potential hackers may gain access to valuable information such as the hostname and the version of the operating system from the default AIX login screen. This information would assist hackers in choosing the exploitation methods to break into the system. For security reasons, change the login screen default messages.

Audit:

Validate the changes to the `Xresources` files:

```
egrep "Dtlogin*greeting.labelString|Dtlogin*greeting.persLabelString:"  
/etc/dt/config/*/Xresources
```

The above command should yield a similar output to the following:

```
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.labelString: Authorized  
uses only. All activity may be monitored and reported.  
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.persLabelString:  
Authorized uses only. All activity may be monitored and reported.
```

Remediation:

Copy the files from `/usr/dt/config/*/Xresources` to `/etc/dt/config/*/Xresources` and add the `Dtlogin*greeting.labelString` and `Dtlogin*greeting.persLabelString` parameters to all copied `Xresources` files:

```
for file in /usr/dt/config/*/Xresources; do
    dir=`dirname $file | sed s/usr/etc/`
    mkdir -p $dir
    if [ ! -f $dir/Xresources ]; then
        cp $file $dir/Xresources
    fi
    WARN="Authorized uses only. All activity may be monitored and reported."
    echo "Dtlogin*greeting.labelString: $WARN" >> $dir/Xresources
    echo "Dtlogin*greeting.persLabelString: $WARN" >> $dir/Xresources
done
```

Default Value:

N/A

4.5.1.9 CDE - /etc/dt/config/Xconfig permissions and ownership (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/dt/config/Xconfig` file is used to customize CDE DT login attributes. Ensure this file is owned by `root:bin` and permissions prevent `group` and `other` from writing to the file.

Rationale:

The `/etc/dt/config/Xconfig` file can be used to customize CDE DT login attributes. The default file, `/usr/dt/config/Xconfig`, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/Xconfig | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r--r--r--  root      bin          /etc/dt/config/Xconfig
```

Remediation:

Check to see if the `/etc/dt/config/Xconfig` exists:

```
ls -l /etc/dt/config/Xconfig
```

Apply the appropriate ownership and permissions to `/etc/dt/config/Xconfig`:

```
chown root:bin /etc/dt/config/Xconfig  
chmod go-w /etc/dt/config/Xconfig
```

Default Value:

N/A

4.5.1.10 CDE - /etc/dt/config/Xservers permissions and ownership (Automated)

Profile Applicability:

- Level 1

Description:

The /etc/dt/config/Xservers contains entries to start the Xserver on the local display. Ensure this file is owned by root:bin and prevents group and other from writing to it.

Rationale:

The /etc/dt/config/Xservers contains entries to start the Xserver on the local display. The default file, /usr/dt/config/Xservers, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/Xservers | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--  root      bin          /etc/dt/config/Xservers
```

Remediation:

Check to see if the /etc/dt/config/Xservers exists:

```
ls -l /etc/dt/config/Xservers
```

If it exists ensure that it is explicitly defined in /etc/dt/config/Xconfig:

```
vi /etc/dt/config/Xconfig
```

Replace:

```
Dtlogin*servers:          Xservers
```

With:

```
Dtlogin*servers: /etc/dt/config/Xservers
```

Apply the appropriate ownership and permissions to /etc/dt/config/Xservers:

```
chown root:bin /etc/dt/config/Xservers
chmod go-w /etc/dt/config/Xservers
```

Default Value:

N/A

4.5.1.11 CDE - /etc/dt/config/*/Xresources permissions and ownership (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/dt/config/*/Xresources` file contains appearance and behavior resources for the `Dtlogin` login screen.

Rationale:

The `/etc/dt/config/*/Xresources` file defines the customization of the `Dtlogin` screen. The default file, `/usr/dt/config/*/Xresources`, is unconditionally overwritten upon subsequent installation. It is recommended that the appropriate permissions and ownership are applied to secure the file.

Audit:

Validate the ownership and permissions:

```
ls -l /etc/dt/config/*/Xresources | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield a similar output to the following:

```
-rw-r--r-- root sys /etc/dt/config/en_GB/Xresources
-rw-r--r-- root sys /etc/dt/config/en_US/Xresources
```

Remediation:

Set the appropriate permissions and ownership on all `Xresources` files:

```
chown root:sys /etc/dt/config/*/Xresources
chmod u=rw,go=r /etc/dt/config/*/Xresources
```

Default Value:

N/A

4.5.2 FTPD

4.5.2.1 FTPD: Disable root access to ftpd (Automated)

Profile Applicability:

- Level 1

Description:

This change adds the root user to the `/etc/ftpusers` file, which disables `ftp` for root.

Rationale:

This change ensures that direct root `ftp` access is disabled. As detailed previously, `ftp` as a service should be disabled. If the service has to be enabled then this change must be implemented to ensure that remote root file transfer access is not enabled.

Audit:

From the command prompt, execute the following command:

```
grep "root" /etc/ftpusers
```

The above command should yield the following output:

```
root
```

Remediation:




Add root to the `/etc/ftpusers` file:

```
echo "root" >> /etc/ftpusers
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

4.5.2.2 FTPD: Display acceptable usage policy during login (Automated)

Profile Applicability:

- Level 1

Description:

Set an `ftpd` login banner which displays the acceptable usage policy.

Rationale:

The message in `banner.msg` is displayed for FTP logins. Banners display necessary warnings to users trying to gain unauthorized access to the system and are required for legal purposes. The recommendation is to set the banner as:

"Authorized uses only. All activity will be monitored and reported".

The content may be changed to reflect any corporate AUP.

Audit:

If `ftpd` is active verify the catalog is installed and the login banner has been updated:

```
if [[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]]; then
    lslpp -L "bos.msg.en_US.net.tcp.client" >/dev/null && print $(dspcat
/usr/lib/nls/msg/en_US/ftpd.cat 1 9)
else
    RC=0
fi
```

The above command should yield the following output:

```
"%s Authorized uses only. All activity may be monitored and reported"
```

Remediation:

Ensure that the `bos.msg.en_US.net.tcp.client` fileset is installed:

```
lsllpp -L "bos.msg.en_US.net.tcp.client"
```

NOTE: If the fileset is not installed, install it from the AIX media or another software repository. The fileset should reflect the language used on the server.




Once installed set the `ftp` AUP banner:

```
dsppcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.tmp
sed "s/\"\\%s FTP server (\\%s) ready.\\\"/\"\\%s Authorized uses only. All
activity may be monitored and reported\\\"/" /tmp/ftpd.tmp > /tmp/ftpd.msg
gencat /usr/lib/nls/msg/en_US/ftpd.cat /tmp/ftpd.msg
rm /tmp/ftpd.tmp /tmp/ftpd.msg
```

Default Value:

%s FTP server (%s) ready.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

4.5.2.3 FTPD: Prevent world access and group write to files (Automated)

Profile Applicability:

- Level 1

Description:

The umask of the `ftpd` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-accessable, group-writeable files by default.

Rationale:

The umask of the `ftpd` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-accessable and group-writeable files by default. These files could then be transferred over the network which could result in compromise of the critical information.

Audit:

Validate the umask setting:

```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && grep  
"^ftp[[:blank:]]" /etc/inetd.conf |awk '{print $6, $7, $8, $9, 10}' || RC=0
```

The above command should yield the following output (only if the ftp daemon is not disabled):

```
/usr/sbin/ftpd ftpd -l -u 027
```

Remediation:

Set the default umask of the `ftp` daemon:




```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && chsubserver -c -v  
ftp -p tcp "ftpd -l -u 027" && refresh -s inetd || RC=0`
```

NOTE: The umask above restricts write permissions for both group and other. All access for other is removed.

Default Value:

```
/usr/sbin/ftpd ftpd -l
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

4.5.3 OpenSSH

SSH is a secure, encrypted replacement for common clear-text login services such as telnet, ftp, rlogin, rsh, and rcp. Wherever remote access is required, SSH should be utilized to protect communications from unauthorized interception.

Other sections in this benchmark recommend disabling clear-text protocols. Although some legacy applications may still require clear-text protocols, SSH should still be used alongside the non-encrypted services.

This section contains recommendations for the secure configuration of OpenSSH.

Note: Some of the recommendations are default values. The best practice is to include the settings in the configuration file with an explicit statement - rather than implicit - as defaults may change. In other words: explicit declaration ensures that recommendations remain constant over time.

OpenSSH requires each side (client/server) to negotiate multiple connection parameters. These are corresponding `ssh_config`/`sshd_config` keywords:

- `KexAlgorithms`: the key exchange methods that are used to generate *per-connection keys*.
- `HostkeyAlgorithms`: the public key algorithms accepted for an SSH server to *authenticate itself to an SSH client*.
- `Ciphers`: the *ciphers to encrypt* the connection.
- `MACs`: the message authentication *codes used to detect traffic modification*.

4.5.3.1 OpenSSH: Minimum version is 8.1 (Automated)

Profile Applicability:

- Level 1

Description:

OpenSSH is the expected program for remote command line access. It provides encrypted protocols such as SSH and SCP/SFTP.

Rationale:

The recommended mechanism for remote access is to use encrypted protocols such as OpenSSH that are designed to prevent the interception of communications. OpenSSH is the standard replacement for clear-text protocols, such as Telnet and FTP.

Clear-text protocols can be snooped and expose credentials and/or sensitive data to unauthorized parties. Additionally, servers that are configured with unique PKI keys can circumvent host impersonation and assure remote hosts/users that they are communicating with the intended device.

Impact:

OpenBSD maintains the OpenSSH project regularly updates OpenSSH. The Major/Minor numbers OpenBSD publishes may be higher than the Major/Minor numbers an OS platform uses - due to differences in how they manage packages.

The current OpenBSD release is: OpenSSH 8.6 released April 19, 2021. IBM's policy is to stay at a constant level (currently 8.1) and maintain a more stable set of configuration keywords or feature set. OpenBSD, *never* patches a release. Instead, OpenBSD releases a new version with the latest security fixes and/or feature changes. This means IBM does not automatically push OpenSSH feature changes - but does look at new OpenBSD releases and incorporates security fixes, if any.

The current OpenSSH version maintained by IBM is OpenSSH 8.1. The `openssh` fileset VRMF number should start with 8.1.

Audit:

The following command should return `Version 8+`

```
test $(sshd -i </dev/null | cut -d _ -f 2) -ge 8.1 && print "Version 8+" ||  
print "Insufficient"
```

Remediation:






Install OpenSSH version 8.1 (or later), depending on package source.

The current version available from IBM via

[AIX Web Download Pack Programs](#)

is 8.1.102.2103.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.2 OpenSSH: Remove `/etc/shosts.equiv` and `/etc/rhosts.equiv` (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to remove both the `/etc/shosts.equiv` and `/etc/rhosts.equiv` file. This is a consequence of the recommendation to not use `HostbasedAuthentication`.

Rationale:

The recommendation is to not use `HostbasedAuthentication` unless there is a documented need already exists the logical consequence is to remove these files, if they exist, to lower the risk of accidental activation.

In any case - the file `/etc/rhosts.equiv` should be removed - period. (**Note:** This is also recommended elsewhere.)

Impact:

The file `/etc/shosts.equiv`, in combination with the OpenSSH `sshd_config`: `HostbasedAuthentication`, can allow passwordless authentication between servers.

Without `HostbasedAuthentication` the file `/etc/shosts.equiv` has no purpose.

Audit:

Ensure that the files `/etc/shosts.equiv` and `/etc/rhosts.equiv` have been removed:

```
ls -l /etc/[rs]hosts.equiv && /usr/bin/printf "Remove file: %s\n"
/etc/[rs]hosts.equiv
```

The above command should yield no output.

Remediation:

Print (for review) and then remove the content of the `/etc/[rs]hosts.equiv` files:

```
for file in /etc/[rs]hosts.equiv; do
    print "+++ ${file} +++"
    /usr/bin/cat -n ${file}
    /usr/bin/rm -f ${file}
done
```

Default Value:

N/A

Additional Information:**Reversion:**

- The `/etc/shosts.equiv` file would need to be restored from a backup or from the remediation log.
- The file `/etc/rhosts.equiv` should not be restored.

4.5.3.3 OpenSSH: Remove `.shosts` files (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to remove any existing `.shosts` files from all user home directories.

Rationale:

The existence of `.shosts` files in a user home directory, combined with the correct SSH parameter can allow passwordless authentication between servers. As previous recommendations in this section disable this authentication method, these files, if they exist, should be removed.

Audit:

Ensure that the all of the `.shost` files have been successfully removed:

```
find / -name ".shosts" -print
```

The above command should yield no output.

Remediation:

List out all of the existing `.shost` files:

```
find / -name ".shosts" -print
```

Review the list of `.shost` files and remove them individually, or all at once:

Individually:

```
rm <full pathname>
```

All at once:

```
find / -name ".shosts" -exec rm {} \;
```

Default Value:

N/A

Additional Information:

Reversion:

Any deleted files would need to be restored from a backup.

4.5.3.4 *sshd_config*: Restrict users and groups allowed access via OpenSSH (Manual)

Profile Applicability:

- Level 2

Description:

There are multiple options available to regulate access to a server via OpenSSH. At least of the following options should be implemented. **Note:** The allow/deny users directives are processed in the following order: DenyUsers, AllowUsers. The allow/deny groups directives are processed in the following order: DenyGroups, AllowGroups. **Note:** If a *DenyUser* or *DenyGroup* matches the *associated Allow directive* is not processed. To implement **DenyAll except** use *only* Allow* directives. To implement **PermitALL except** use *only* Deny* directives. It is advised not to combine Allow and Deny directives as this can make the configuration harder to debug.

- **DenyUsers:** The `DenyUsers` variable specifies user names not permitted to access the system via `sshd`. The definition is a list `username pattern(s)` separated by spaces. *Numeric userIDs* are not are not allowed (recognized). Patterns can be narrowed to restrict access from specific hosts using the form `username@host`.
- **AllowUsers:** The `AllowUsers` variable specifies user names permitted to access the system via `sshd`. The definition is a list `username pattern(s)` separated by spaces. *Numeric userIDs* are not are not allowed (recognized). Patterns can be narrowed to permit access only from specific host(s) using the form `username@host`.
- **DenyGroups:** The `DenyGroups` variable specifies group names not permitted to access the system via `sshd`. The definition is a list `groupname pattern(s)` separated by spaces. *Numeric groupIDs* are not allowed (recognized). Login is disallowed for users whose primary group or supplementary group list matches one of the patterns.
- **AllowGroups:** The `AllowGroups` variable specifies group names permitted to access the system via `sshd`. The definition is a list `groupname pattern(s)` separated by spaces. *Numeric groupIDs* are not allowed (recognized). Login is allowed for users whose primary group or supplementary group list matches one of the patterns.

Rationale:

By default, login is allowed for all users and all groups.

Restricting which users can access the system via OpenSSH will help ensure that only authorized users access the system.

Impact:

When implemented - no longer can any user connect from any host. They must satisfy the connection requirements.

As this is new to most AIX installations for this version of the benchmark we are setting it at Level 2 - for scoring - but we recommend your organization implements it as soon as possible.

Note: your organization may already have a OpenSSH restricted access model as this recommendation is already Level 1 for `Linux*` benchmarks.

Audit:

Ensure that the AllowUsers, AllowGroups, DenyUsers, or DenyGroups is set:

```
/usr/bin/egrep "^(AllowUsers|AllowGroups|DenyUsers|DenyGroups) [[:blank:]]"
/etc/ssh/sshd_config
```

The above command should yield at least one of the following output:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set one (or more) of the following parameters:

```
AllowUsers <userlist>
AllowGroups <grouplist>
DenyUsers <userlist>
DenyGroups <grouplist>
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
startsrc -s sshd
```






Default Value:

All users from any host are permitted.

Additional Information:

Subsequent releases of AIX benchmarks are expected to have this recommendation scored at Level 1

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.5 sshd_config: PermitRootLogin is 'prohibit-password' or 'no' (Automated)

Profile Applicability:

- Level 2

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to disable direct root login. Direct root login via SSH was enabled by default with prior versions of OpenSSH. To be absolutely certain direct login is disabled the recommendation is to set this variable specifically rather than rely on a new, changeable, default.

Rationale:

All root access should be facilitated through a local logon with a unique and identifiable user ID and then via the `su` command once locally authenticated.

Direct root login using passwords is insecure and does not provide sufficient logging or audit trailing for accountability.

Impact:

While this sounds simple - setting the attribute to `no` requires either sharing a root password (to use `su`), the installation of `sudo`, or a configuration using extended RBAC for actions that require enhanced privileges.

The recommendation specifies a `LOG_LEVEL` of `INFO` or `DEBUG`.

To resolve, partially, the accountability concerns, permitting `publickey` authentication as root together with **LogLevel INFO** (minimum) provides the following `syslog` information:

```
Jun 25 09:26:41 x071 auth|security:info sshd[8323282]: Accepted publickey for michael from 192.168.129.11 port 54278 ssh2: RSA  
SHA256:drHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk  
Jun 25 09:26:52 x071 auth|security:info sshd[8847396]: Accepted publickey for root from 192.168.129.11 port 54279 ssh2: RSA  
SHA256:drHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk  
Jun 25 09:26:53 x071 auth|security:info sshd[9044142]: Accepted publickey for root from 192.168.129.11 port 54280 ssh2: RSA  
SHA256:drHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk
```

Local site policy might decide that `publickey` accountability is sufficient and a setting of `PermitRootLogin prohibit-password` (the new default) provides sufficient accountability and security.

Note: only public keys in a file such as `~root/.ssh/authorized_keys` will be able to connect.

Audit:

Ensure that the `PermitRootLogin` parameter has been changed:

```
/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config
```

The above command should yield one of the following:

```
PermitRootLogin prohibit-password
PermitRootLogin no
PermitRootLogin forced-commands-only
```

Remediation:

```
#!/usr/bin/ksh
PREFERRED_SETTING="prohibit-password"
umask 077
set $(/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config)
echo $?
if [[ ! -z $1 ]]; then
    # Look for a setting and change to no if anything else
    if [[ $2 != ${PREFERRED_SETTING} ]]; then
        sed "s/^PermitRootLogin \\{1\\}[^ ]\\{1,\\}/PermitRootLogin
${PREFERRED_SETTING}/" /etc/ssh/sshd_config >/tmp/sshd_config.$$
    fi
else
    # Look for a comment and append
    sed "/^# \\{0,\\}PermitRootLogin/ a\\^JPermitRootLogin ${PREFERRED_SETTING}/"
/etc/ssh/sshd_config >/tmp/sshd_config.$$
fi

if [[ -e /tmp/sshd_config.$$ ]]; then
    diff -u /tmp/sshd_config.$$ /etc/ssh/sshd_config
    rm /tmp/sshd_config.$$
elif
    # Verify setting is specified
    /usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config >>/dev/null
    if [[ $? -ne 0 ]]; then
        print "PermitRootLogin ${PREFERRED_SETTING}" >> /etc/ssh/sshd_config
    fi
fi
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd
sleep 5
startsrc -s sshd
```

Default Value:

`PermitRootLogin prohibit-password`






Additional Information:

The values for this parameter have been `yes` (not recommended), `no` (not recommended, but accepted), `prohibit-password` (recommended setting), `forced-commands-only` (not recommended, but accepted) and `without-password` (deprecated setting).

PermitRootLogin:

Specifies whether root can log in using `ssh(1)`. The argument must be `yes`, `prohibit-password`, `forced-commands-only`, or `no`. The default is `prohibit-password`. If this option is set to `prohibit-password` (or its deprecated alias, `without-password`), password and keyboard-interactive authentication are disabled for root. If this option is set to `forced-commands-only`, root login with public key authentication will be allowed, but only if the `command` option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root. If this option is set to `no`, root is not allowed to log in.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.6 sshd_config: Banner exists and message contains "Only authorized users allowed" (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file and configure a path to a login herald message.

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:

Ensure that the `Banner` parameter has been changed:

```
grep "^Banner[[:blank:]]" /etc/ssh/sshd_config && cat /etc/ssh/ssh_banner
```

The above command should yield the following output:

```
Banner /etc/ssh/ssh_banner
Unauthorized use of this system is prohibited.
```

NOTE: The content of the banner file can reflect any internal acceptable usage policy standards

Remediation:

- Create an SSH banner file:

```
printf "Unauthorized use of this system is prohibited.\n" >  
/etc/ssh/ssh_banner
```

NOTE: The content of the banner file can reflect any internal acceptable usage policy standards

- Edit the `/etc/ssh/sshd_config` file and customize the `Banner` parameter

```
vi /etc/ssh/sshd_config
```

- Replace:

```
#Banner /some/path
```

With:

```
Banner /etc/ssh/ssh_banner
```






- Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
sleep 5  
startsrc -s sshd
```

Default Value:

No banner is configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.7 sshd_config: HostbasedAuthentication is 'no' (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to ensure the `sshd` daemon is configured to prevent host-based authentication.

Rationale:

Host-based authentication is a method to authenticate users (rather than requiring password or key-based authentication method). Used at a system level by OpenSSH requires the file `/etc/shosts.equiv` to contain a list of so-called *trusted* hosts. When this method is active any user on a trusted host can login to the server as *authenticated* because the server identity the user imitates the connection from (aka the OpenSSH client) authenticates the user as *trusted*.

Since this feature disables **user-based** authentication from some hosts - our recommendation is to disable host-based authentication.

Audit:

Ensure that the `HostbasedAuthentication` parameter has been changed:

```
grep "^HostbasedAuthentication[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
HostbasedAuthentication no
```


Remediation:

Edit the `/etc/ssh/sshd_config` file to ensure that host based authentication is disallowed:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#HostbasedAuthentication no
```

With:

```
HostbasedAuthentication no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
startsrc -s sshd
```

Default Value:

HostbasedAuthentication no

Additional Information:

Reversion:

Revert to the default setting for the `HostBasedAuthentication` parameter:

```
vi /etc/ssh/sshd_config
```

Replace:

```
HostbasedAuthentication no
```








With:

```
# HostbasedAuthentication no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
startsrc -s sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.8 sshd_config: IgnoreRhosts is 'yes' or 'shosts-only' (Automated)

Profile Applicability:

- Level 1

Description:

The `IgnoreRhosts` parameter controls whether `.rhosts` and `.shosts` files will be used in `RhostsRSAAuthentication` Or `HostbasedAuthentication`.

Rationale:

A user can logon to a remote system without authenticating themselves if `.rhosts` or `.shosts` files exist in the remote home directory and if the client machine name and user name are present in these files.

This method presents a risk as the system could be exploited by IP, DNS (Domain Name Server) and routing spoofing attacks. Additionally, this authentication method relies on the integrity of the client machine.

These weaknesses are well known and have been exploited. Since this authentication method entails a risk the primary recommendation is to disable the method (setting is `yes`). Only with documented cases - including steps to mitigate the accepted risk - may `shosts` mechanism be activated.

Impact:

The title of this recommendation implies acceptance of `shosts-only`. This is only expected for particular hosts.

Further, the addition of `shosts-only` requires OpenSSH 8.2 and later.

Since AIX is currently operating with OpenSSH 8.1 the `audit` and `remediation` paragraphs are written to implement the preferred setting - `yes` `IgnoreRhosts` in any form.

Audit:

Ensure that the `IgnoreRhosts` parameter has been set (even though the default is `yes`):

```
grep "^IgnoreRhosts[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
IgnoreRhosts yes
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to disable the `.shosts` and `.rhosts` authentication parameter:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#IgnoreRhosts yes
```

With:

```
IgnoreRhosts yes
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
startsrc -s sshd
```








Default Value:

`IgnoreRhosts yes`

References:

1. `sshd_config(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.9 sshd_config: PermitEmptyPasswords is 'no' (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that the SSH daemon does not authenticate users with a null password.

Rationale:

If password authentication is used and an account has an empty password, the SSH server must be configured to disallow access to the account. Permitting empty passwords could create an easy path of access for hackers to enter the system.

Audit:

Ensure that the `PermitEmptyPasswords` parameter has been changed:

```
grep "^PermitEmptyPasswords[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitEmptyPasswords no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to disable the acceptance null passwords:

```
vi /etc/ssh/sshd_config
```

Replace:

```
#PermitEmptyPasswords no
```

With:

```
PermitEmptyPasswords no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
startsrc -s sshd
```






Default Value:

`PermitEmptyPasswords no`

References:

1. `sshd_config(5)`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.10 sshd_config: LogLevel is 'INFO' or 'VERBOSE' (Automated)

Profile Applicability:

- Level 1

Description:

The `INFO` parameter specifies that record login and logout activity will be logged. While this is the default setting for OpenSSH we believe it is better to explicitly set the value in the configuration file.

Rationale:

SSH provides several logging levels with varying amounts of verbosity.

LogLevel

Gives the verbosity level that is used when logging messages from `sshd(8)`. The possible values are: `QUIET`, `FATAL`, `ERROR`, `INFO`, `VERBOSE`, `DEBUG`, `DEBUG1`, `DEBUG2`, and `DEBUG3`. The default is `INFO`. `DEBUG` and `DEBUG1` are equivalent. `DEBUG2` and `DEBUG3` each specify higher levels of debugging output. Logging with a `DEBUG` level violates the privacy of users and is not recommended.

- `DEBUG` (and `VERBOSE`) is specifically *not* recommended other than strictly for debugging SSH communications. `INFO` level is the default level and records login/logout activity of SSH users. Login information includes the fingerprint of their SSH keys, when used.

In situations, such as Incident Response, an SSH fingerprint may be 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.

Note: the default action of OpenSSH is to propagate this key for every ssh login.

Audit:

Ensure that the `LogLevel` parameter is set to `INFO`:

```
grep "^LogLevel[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
LogLevel INFO
```


Remediation:

- Edit the `/etc/ssh/sshd_config`:

```
vi /etc/ssh/sshd_config
```

- Set:

```
LogLevel INFO
```






- Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrv -s sshd  
sleep 2  
startsrc -s sshd
```

Default Value:

#LogLevel INFO

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.11 *sshd_config*: *sftp-server* arguments include '-u 027 -f AUTH -l INFO' (Automated)

Profile Applicability:

- Level 1

Description:

The `sftp-server` is started by the `sshd` server after authentication has been completed successfully. The process runs with the `euid` of the authenticated user.

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. `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.

Like `sshd` (see Recommendation: OpenSSH: LogLevel) the `sftp-server` needs to be configured with `syslog` information. Additionally, the `umask` value needs specification.

Audit:

Ensure that the `sftp-server` parameter is configured to `umask 027` and `syslog` logging at either `INFO` (preferred), or `DEBUG`.

The following command should return either:

```
grep "^Subsystem[[:blank:]]sftp[[:blank:]]sftp-server[[:blank:]]"
/etc/ssh/sshd_config
```

The above command should yield one of the following output:

```
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l INFO
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l DEBUG
```

Remediation:

- Edit the `/etc/ssh/sshd_config`:

```
vi /etc/ssh/sshd_config
```

- Set:

```
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l VERBOSE
```






or

```
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l DEBUG
```

- Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
sleep 5  
startsrc -s sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.12 sshd_config: MaxAuthTries is '4' (Automated)

Profile Applicability:

- Level 1

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 for `MaxAuthTries` is 4 or less:

```
sshd -T | grep maxauthtries
```

Remediation:






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

```
MaxAuthTries 4
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrc -s sshd  
startsrc -s sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.13 sshd_config: PermitUserEnvironment is 'no' (Automated)

Profile Applicability:

- Level 1

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).

Impact:

The general condition is to specify `no` while the recommendation leaves room for specific User(s) or Group(s) to use this feature in controlled ways.

Audit:

Ensure that the `PermitUserEnvironment` parameter has been changed:

```
grep "^PermitUserEnvironment[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitUserEnvironment no
```

Remediation:

Edit the `/etc/ssh/sshd_config` file:

```
vi /etc/ssh/sshd_config
```






Set:

```
PermitUserEnvironment no
```

Re-cycle the `sshd` daemon to pick up the configuration changes:

```
stopsrv -s sshd  
startsrc -s sshd
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.5.3.14 *sshd_config*: Use Conditional exception(s). (Manual)

Profile Applicability:

- Level 2

Description:

There are several options available to regulate access to a server via OpenSSH. There are settings that are set at a global level only and there are settings that have a global default but can be modified to meet specific client (from) requirements for the server (to) being configured.

These overrides are specified via a conditional block that starts with the directive `Match`. When all the *MATCH* criteria (*User*, *Group*, *Host*, *LocalAddress*, *LocalPort*, *RDomain*, and *Address*, **or** the single token *ALL* that matches by definition) the following settings can be redefined (overwrite) previous setting values:

AcceptEnv, AllowAgentForwarding, AllowGroups,
AllowStreamLocalForwarding, AllowTcpForwarding, AllowUsers,
AuthenticationMethods, AuthorizedKeysCommand,
AuthorizedKeysCommandUser, AuthorizedKeysFile,
AuthorizedPrincipalsCommand, AuthorizedPrincipalsCommandUser,
AuthorizedPrincipalsFile, Banner, CASignatureAlgorithms,
ChrootDirectory, ClientAliveCountMax, ClientAliveInterval, DenyGroups,
DenyUsers, DisableForwarding, ExposeAuthInfo, ForceCommand,
GatewayPorts, GSSAPIAuthentication, HostbasedAcceptedAlgorithms,
HostbasedAuthentication, HostbasedUsesNameFromPacketOnly,
IgnoreRhosts, Include, IPQoS, KbdInteractiveAuthentication,
KerberosAuthentication, LogLevel, MaxAuthTries, MaxSessions,
PasswordAuthentication, PermitEmptyPasswords, PermitListen,
PermitOpen, PermitRootLogin, PermitTTY, PermitTunnel, PermitUserRC,
PubkeyAcceptedAlgorithms, PubkeyAuthentication, PubkeyAuthOptions,
RekeyLimit, RevokedKeys, RDomain, SetEnv, StreamLocalBindMask,
StreamLocalBindUnlink, TrustedUserCAKeys, X11DisplayOffset,
X11Forwarding and X11UseLocalhost.

Rationale:

There are situations where *exceptions* to the corporate security policy are required.

Match is the mechanism that permits the configuration - and documentation - of exceptions.

```
# Example of overriding settings on a per-user basis
# anoncvs does not get a command prompt, instead a specific command is
# started.
#Match User anoncvs
#       X11Forwarding no
#       AllowTcpForwarding no
#       PermitTTY no
#       ForceCommand cvs server

# The user michael requires, and is permitted (see support ticket X123456),
# the use of X11Forwarding.
# Match User michael
#       X11Forwarding yes
```

Audit:

Notes for audit

- grep for active Match statement,
- if any exceptions found, print message and exceptions found






```
exceptions=$(egrep "^Match " /etc/ssh/sshd_config | wc -l)
if [[ ${exceptions} != "0" ]]; then
    print "Verify the following Match statements are properly documented and
    still permitted/required"
    /usr/bin/egrep -p "^Match " /etc/ssh/sshd_config
fi
```

Remediation:

Default Value:

No *MATCH* statements are used.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.15 sshd_config, ssh_config: KexAlgorithms (Automated)

Profile Applicability:

- Level 1

Description:

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

Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140-2 approved are: - ecdh-sha2-nistp256 - ecdh-sha2-nistp384 - ecdh-sha2-nistp521 - diffie-hellman-group-exchange-sha256 - diffie-hellman-group16-sha512 - diffie-hellman-group18-sha512 - diffie-hellman-group14-sha256
- The Key Exchange algorithms supported by OpenSSH 8.2 are:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
sntrup4591761x25519-sha512@tinyssh.org
```

Rationale:

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

Impact:

Weak clients no longer connect.

Audit:

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

Weak Key Exchange Algorithms:

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

Remediation:

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

Example:

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










Default Value:

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

References:

1. For more information on the Counter mode algorithms, read RFC4344 at <http://www.ietf.org/rfc/rfc4344.txt>.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

4.5.3.16 sshd_config, ssh_config: Ciphers (Automated)

Profile Applicability:

- Level 1

Description:

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

Notes:

- Some organizations may have stricter requirements for approved ciphers
- Ensure that ciphers used are in compliance with site policy
- The only "strong" ciphers currently FIPS 140-2 compliant are: - aes256-ctr - aes192-ctr - aes128-ctr
- Supported ciphers in OpenSSH 8.2:

```
3des-cbc  
aes128-cbc  
aes192-cbc  
aes256-cbc  
aes128-ctr  
aes192-ctr  
aes256-ctr  
aes128-gcm@openssh.com  
aes256-gcm@openssh.com  
chacha20-poly1305@openssh.com
```

Rationale:

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

Research conducted at various institutions determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBC) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors

Audit:

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep ciphers
```

Weak Ciphers:

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

Remediation:

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

Example

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

Re-cycle the `sshd` daemon to pick up the configuration changes:






```
stopsrc -s sshd  
startsrc -s sshd
```

Default Value:

AIX with OpenSSH 8.1

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
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.			

4.5.3.17 sshd_config, ssh_config: MACs - Message Authentication Codes (Automated)

Profile Applicability:

- Level 1

Description:

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

Notes:

- Some organizations may have stricter requirements for approved MACs
- Ensure that MACs used are in compliance with site policy
- The only "strong" MACs currently FIPS 140-2 approved are:
 - hmac-sha2-256
 - hmac-sha2-512
- The Supported MACs are:

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

Rationale:

Clients that expect the weak MACs will often use/expect weak encryption keys as well.

Like CipherKeys the `sshd` **MACs** need to be configured to exclude weak message authentication codes.

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

Impact:

Weak clients will not connect and/or lose the ability to connect.

Audit:

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep -i "MACs"
```

Weak MAC algorithms:

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

Remediation:

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

Example:

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

Default Value:

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

References:

1. For more information on the Counter mode algorithms, read RFC4344 at <http://www.ietf.org/rfc/rfc4344.txt>.

Additional Information:

Following CIS Debian Family Linux benchmarks.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v8	16.5 <u>Use Up-to-Date and Trusted Third-Party Software Components</u> Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.		●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.		●	●
v7	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●
v7	18.4 <u>Only Use Up-to-date And Trusted Third-Party Components</u> Only use up-to-date and trusted third-party components for the software developed by the organization.		●	●
v7	18.5 <u>Use Only Standardized and Extensively Reviewed Encryption Algorithms</u> Use only standardized and extensively reviewed encryption algorithms.		●	●

4.5.3.18 sshd_config, ssh_config: ReKeyLimit (Automated)

Profile Applicability:

- Level 1

Description:

This variable specifies the maximum amount of data that may be transmitted before the session key is renegotiated, optionally followed by a maximum amount of time that may pass before the session key is renegotiated.

Rationale:

This recommendation is based on the guidelines outlined in Chapter 9 in [RFC4253], i.e. the recommendation is to release/renew Session keys after one hour or after the transfer of one gigabyte (depending on whichever comes first).

Audit:

Run the following command:

```
sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep rekeylimit
```

Verify the output matches:

```
rekeylimit 1G 3600
```

Remediation:

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

```
RekeyLimit 1G 3600
```










Default Value:

RekeyLimit default None

References:

1. For more information on the Counter mode algorithms, read RFC4344 at <http://www.ietf.org/rfc/rfc4344.txt>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

4.5.4 Sendmail Configuration

The base recommendation is to not run `sendmail` on any server not specifically configured and hardened as a MTA (mail transfer agent).

The basic exception - *for a not specifically MTA hardened servers* is to permit MSP (mail submission program) via `localhost` (127.0.0.1).

4.5.4.1 /etc/mail/sendmail.cf - Hide sendmail version information (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to change both the default `sendmail` greeting and HELP output to not display the `sendmail` version.

Rationale:

The `sendmail` daemon has a history of security vulnerabilities. The recommendation is to change the default `sendmail` settings that display the `sendmail` version and other related information. Sendmail version information can be used by an attacker for fingerprinting purposes.

Audit:

- Validate the configuration of the software:
 - The command should **NOT** yield: `O SmtgGreetingMessage=$j Sendmail $b`
 - **Note:** No output is also an error.

```
/usr/bin/egrep -i "^O SmtgGreetingMessage" /etc/mail/sendmail.cf
```

- Verify a sendmail helpfile exists:

```
test -e /etc/mail/helpfile || echo "Sendmail HELP file is missing"
```

Remediation:

Create a backup copy of `/etc/mail/sendmail.cf`:

```
cp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf.pre_cis
```

Edit:

```
vi /etc/mail/sendmail.cf
```

Replace:

```
O SmtgGreetingMessage=$j Sendmail $b
```

With:

```
O SmtgGreetingMessage=mailerready
```

- Ensure Sendmail helpfile exists

```
test -e /etc/mail/helpfile || touch /etc/mail/helpfile
```

Default Value:

```
SmtgGreetingMessage=$j Sendmail $b
```

Additional Information:

Reversion:

Copy back the original `/etc/sendmail.cf` file:

```
cp -p /etc/mail/sendmail.cf.pre_cis /etc/mail/sendmail.cf
```

4.5.4.2 /etc/mail/sendmail.cf - PrivacyOptions (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to ensure that PrivacyOptions includes at least three settings:

- authwarnings (a default)
- novrfy
- noexpn

Rationale:

The `sendmail` daemon has a history of security vulnerabilities. The recommendation is to modify default `sendmail` settings that otherwise may provide information that can be used by an attacker.

- novrfy: No Verify: do not verify valid email addresses. This can be used by attackers, e.g., phishing attacks.
- noexpn: no expansion: do not verify/expand email list addresses - providing attackers with a list of valid email addresses.

Audit:

- Validate the configuration of the software:

```
popt=$(/usr/bin/egrep -i "^O PrivacyOptions" /etc/mail/sendmail.cf)
for option in authwarnings novrfy noexpn; do
echo ${popt} | /usr/bin/grep -i ${option} >/dev/null && continue
echo Missing sendmail PrivacyOption: $option
done
```


Remediation:

Create a backup copy of `/etc/mail/sendmail.cf`:

```
cp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf.pre_cis
```

Edit:

```
vi /etc/mail/sendmail.cf
```

Replace:

```
O PrivacyOptions=authwarnings
```

With:

```
O PrivacyOptions=authwarnings,noexpn,novrfy
```

Or - append

`noexpn,novrfy`

at the end of the current `PrivacyOptions` settings (assuming `authwarnings` is already included).

Default Value:

```
SmtgGreetingMessage=$j Sendmail $b
```

Additional Information:

Reversion:

Copy back the original `/etc/sendmail.cf` file:

```
cp -p /etc/mail/sendmail.cf.pre_cis /etc/mail/sendmail.cf
```

4.5.4.3 /etc/mail/sendmail.cf - DaemonPortOptions (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to enable running `sendmail` in MTA mode to support local applications that require legacy **MTA** (i.e., connection via port 25) support.

*Recall the preferred recommendation is to not run sendmail **locally**.*

Rationale:

Audit:

- Validate the configuration of the software: **(Work In progress)**

```
typeset -i poptwc
portopt=$( /usr/bin/egrep -i "^O DaemonPortOptions" /etc/mail/sendmail.cf)
poptwc=$(echo ${portopt} | /usr/bin/wc -l)
hasaddr=$(echo ${portopt} | /usr/bin/grep -i "addr=")

if test "${hasaddr}0" == "0"; then
    echo "Missing sendmail DaemonPortOption to limit connection to localhost
(127.0.0.1)"
    exit 1
elif test $poptwc -ne 1; then
    echo "Multiple sendmail DaemonPortOption settings: MANUALLY verify only
localhost is active"
    exit 2
fi

popthost=$(echo $portopt | sed 's/.*Addr=\(.*\) [^ ,]* /\1/' | tr 'A-Z' 'a-z')

if [[ ${popthost} == "127.0.0.1" ]] || test ${popthost} == "localhost" ; then
    exit 0
else
    echo "sendmail DaemonPortOption Addr setting is not set to either 127.0.0.1
or localhost"
    exit 3
fi
```

Remediation:

Create a backup copy of `/etc/mail/sendmail.cf`:

```
cp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf.pre_cis
```

Edit:

```
vi /etc/mail/sendmail.cf
```

Replace: (assuming the default configuration)

```
O DaemonPortOptions=Name=MTA
```

with

```
O DaemonPortOptions=Name=MTA,Addr=localhost
```

Additional Information:

Reversion:

Copy back the original `/etc/sendmail.cf` file:

```
cp -p /etc/mail/sendmail.cf.pre_cis /etc/mail/sendmail.cf
```

4.5.4.4 /etc/mail/sendmail.cf - access control (Automated)

Profile Applicability:

- Level 1

Description:

The access controls for `/etc/mail/sendmail.cf` are applied.

Rationale:

The `/etc/mail/sendmail.cf` file is used by the `sendmail` daemon to determine its default configuration. This file must be protected from unauthorized access and modifications.

Audit:

From the command prompt, execute the following command:

```
ls -l /etc/mail/sendmail.cf | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system sendmail.cf
```

Remediation:

Set the recommended permissions and ownership on `/etc/mail/sendmail.cf`:

```
chmod u=rw,g=r,o= /etc/mail/sendmail.cf  
chown root.system /etc/mail/sendmail.cf  
trustchk -u /etc/mail/sendmail.cf mode owner group
```

Default Value:

```
-rw-r--r-- root system sendmail.cf
```

4.5.4.5 /var/spool/clientmqueue - access control (Automated)

Profile Applicability:

- Level 1

Description:

The recommended DAC (discretionary access control) settings for the /var/spool/clientmqueue directory are applied.

Rationale:

Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access. The clientmqueue (/var/spool/clientmqueue) is the mail queue for handling locally generated outbound emails. This queue is used when mail is submitted to `sendmail` as an **MSP** rather than as an **MTA**.

NOTE: It is possible to specify an alternate spool directory in the `/etc/mail/submit.cf` file via the `QueueDirectory` parameter. When this is used **that** directory name needs identical DAC settings.

Audit:

From the command prompt, execute the following command:

```
ls -ld /var/spool/clientmqueue | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxrwx--- smmsp smmsp /var/spool/clientmqueue
```

Remediation:

Set the recommended permissions and ownership on /var/spool/mqueue:

```
chmod ug=rwx,o= /var/spool/clientmqueue  
chown smmsp.smmsp /var/spool/clientmqueue
```

Default Value:

```
drwxrwx--- smmsp smmsp /var/spool/clientmqueue
```

4.5.4.6 /var/spool/mqueue - access control (Automated)

Profile Applicability:

- Level 1

Description:

The recommended DAC (discretionary access control) settings for the /var/spool/mqueue directory are applied.

Rationale:

The `sendmail` daemon stores its queued mail in the /var/spool/mqueue directory. Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access.

NOTE: It is possible to specify an alternate spool directory in the /etc/mail/sendmail.cf file via the `QueueDirectory` parameter. When this is used **that** directory name needs identical DAC settings.

Audit:

From the command prompt, execute the following command:

```
ls -ld /var/spool/mqueue | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwx-----  root      system    /var/spool/mqueue
```

Remediation:

Set the recommended permissions and ownership on /var/spool/mqueue:

```
chmod u=rwx,go= /var/spool/mqueue
chown root /var/spool/mqueue
```

Default Value:

```
drwxrwx---  root      system    /var/spool/mqueue
```

4.5.5 SNMP Configuration

The Simple Network Management Protocol (SNMP) is a commonly used service that provides network management and monitoring capabilities. SNMP offers the capability to poll networked devices and monitor data such as utilization and errors from various subsystems on the host. SNMP is also capable of changing the configurations on the host, allowing remote management of the system. The protocol uses a community string for authentication from the SNMP client to the SNMP agent on the managed device.

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but only allow access from localhost connections. Nevertheless, a local user may install an SNMP client and modify sensitive variables. If SNMP is required, the community strings must be greater than six characters and include a combination of letters, numbers, and special characters to avoid a brute force attack.

4.5.5.1 SNMP - disable private community string (Automated)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable the `private` community string.

Rationale:

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from localhost connections. As these SNMP names are the default, they must not be used. Any SNMP community name should be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the `private` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*private" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community      private 127.0.0.1 255.255.255.255 readWrite
```

Remediation:

Create a backup of `/etc/snmpd.conf`:

```
cp -p /etc/snmpd.conf /etc/snmpd.conf.pre_cis
```

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `private` entry:

```
#community      private 127.0.0.1 255.255.255.255 readWrite
```

Default Value:

Commented in

Additional Information:

Reversion:

Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```


4.5.5.2 SNMP - disable system community string (Automated)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable the system community string.

Rationale:

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from localhost connections. As these SNMP names are the default, they must not be used. Any SNMP community name should be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the system entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*system" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community      system 127.0.0.1 255.255.255.255 readWrite 1.17.2
```

Remediation:

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the system entry:

```
#community      system 127.0.0.1 255.255.255.255 readWrite 1.17.2
```

Default Value:

Commented in

Additional Information:

Reversion:

Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

4.5.5.3 SNMP - disable public community string (Automated)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable or change the `public` community string.

Rationale:

The `public` community string can be polled by remote SNMP devices and pertinent information can be read or changed on the host. The `public` community string should be commented out, or if SNMP is a required service the `public` community name should be changed to be a combination of letters, numbers and special characters to enhance security.

Audit:

Ensure the `public` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community[[:blank:]]*public" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community public
```

Remediation:

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `public` entry:

```
#community public
```

Default Value:

Commented in

Additional Information:

Reversion:

Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

4.5.5.4 SNMP - disable Readwrite community access (Automated)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, disable `readWrite` permissions for all active community strings.

Rationale:

If SNMP is required, none of the available community strings should have global `readWrite` permissions defined. This would allow any remote client to query and to set system configuration parameters. SNMP `readWrite` communities must be disabled unless absolutely necessary. If a `readWrite` community is enabled, then access must be granted to only trusted machines in your network. As SNMP uses community names as part of authentication, you must ensure that all community names are greater than six characters and is a mix of characters, numbers, and special characters.

Audit:

Review the community lines in `/etc/snmpd.conf`:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

NOTE: ensure that there is no `readWrite` access.

Remediation:

Identify if there are any currently configured community strings:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

If there are active community strings, edit the configuration file:

```
vi /etc/snmpd.conf
```

Replace all instances of:

```
community <community name> <IP addresses> <netmask> [ readWrite <view>]
```

With:

```
community <community name> <IP addresses> <netmask> [ readOnly <view>]
```

Default Value:

N/A

Additional Information:

Reversion:

Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

4.5.5.5 SNMP - restrict community access (Automated)

Profile Applicability:

- Level 2

Description:

If `snmpd` is required within the environment, implement IP access restrictions on the available community strings.

Rationale:

If SNMP is required, IP access restrictions should be put into place to limit which hosts or networks subnets are able to remotely poll the server.

Audit:

Review the available community strings IP access control configuration:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

NOTE: validate the allowed IP address and netmasks

Remediation:

Identify if there are any currently configured community strings:

```
grep "^community[[:blank:]]" /etc/snmpd.conf
```

If there are active community strings, edit the configuration file:

```
vi /etc/snmpd.conf
```

Implement IP access restrictions to ALL of the available community names e.g.:

```
community      tivoli  192.132.10.0 255.255.255.0 readOnly
```

The format of each line should reflect:

```
community <community name> <IP addresses> <netmask> [ <permissions> <view>]
```

Default Value:

N/A

Additional Information:

Reversion:

Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

4.5.6 Uninstall snmp (Automated)

Profile Applicability:

- Level 1

Description:

On AIX 7.2 and later, unless otherwise needed - uninstall `snmp` and `snmpd` support.

Rationale:

Impact:

If not installed, the rest of the recommendations in this section titled **SNMP Configuration** may be ignored.

Audit:

Execute the following command:

```
lslpp -Lcq bos.net.tcp.snmp 2>/dev/null
SNMP=$?
lslpp -Lcq bos.net.tcp.snmp 2>/dev/null
SNMPD=$?
if [[ ${SNMP} -eq 0 || ${SNMPD} -eq 0 ]]; then
    echo "SNMP and/or SNMPD support is installed, review section 'SNMP
    Configuartion'"
else
    echo "SNMP software is not installed, section 'SNMP Configuartion' may be
    ignored"
fi
```

Remediation:

Execute the following command:

```
typeset -i SNMP
SNMP=$(lslpp -Lcq | grep bos.net.tcp.snmp | wc -l)
if [[ $SNMP -ne 0 ]]; then
    installp -ug bos.net.tcp.snmp bos.net.tcp.snmpd
fi
```

4.5.7 Uninstall/Disable sendmail (Automated)

Profile Applicability:

- Level 1

Description:

On AIX, unless otherwise needed - uninstall or disable `sendmail` support.

ALSO: if the version installed does not display support for SASLv2 - remove `sendmail` on AIX 7.2 and `chmod` to 0 (zero) otherwise.

Rationale:

Maintaining a secure sendmail MTA (mail transfer agent) is a complex process. While, historically, *NIX systems have run a (localhost) **MTA** (mail transmission agent) or **MSP** (mail submission program) - there is no real need these days for every system to have this software installed.

Note: Historically, the AIX sendmail build has not supported the AUTH feature. Since AIX 7.2 TL4 a new packaging of sendmail (still as version 8.15.2, so version number is not the way to verify suitability) allows AUTH support *indirectly* via the SASLv2 (Simple Authentication and Security Layer) API interface. Our recommendation is to disable/remove `sendmail` programs that do not provide **SASLv2** support.

Impact:

- If not installed, the rest of the recommendations in this section titled **Sendmail Configuration** may be ignored.
- Applications configured to speak to a `localhost` MTA or MSP may fail to send mail. These applications should be (re-)configured to use STARTTLS or SSL and send their mail messages via a hardened MTA host.

Audit:

Execute the following command:

```
# AIX 7.2 installation check
(lslpp -Lcq bos.net.tcp.sendmail 2>/dev/null && echo "Sendmail is installed,
review section \'Sendmail Configuartion\'" && exit

AIX 7.1 installation check (or third party)
if test -e /usr/sbin/sendmail ; then
    (/usr/sbin/sendmail -d0 </dev/null | grep SASLv2 >/dev/null) || echo
sendmail too old/weak- remove or disable.
else
    echo "Sendmail is installed, review section \'Sendmail Configuartion\'"
    exit
fi

# Did not find sendmail in the standard location - assume not installed
echo "Sendmail is not installed, section \'Sendmail Configuartion\' may be
ignored"
exit
```

Remediation:

Execute the following command:

```
(lslpp -Lcq bos.net.tcp.sendmail >/dev/null && installp -u
bos.net.tcp.sendmail) || \
    echo bos.net.tcp.sendmail is not installed

# If AIX 7.1 or thirdparty software, i.e., fileset bos.net.tcp.sendmail does
not exist but sendmail does ...
if test -e /usr/sbin/sendmail ; then
    (/usr/sbin/sendmail -d0 </dev/null | grep SASLv2 >/dev/null) || \
    chmod a= /usr/sbin/sendmail
    trustchk -u /usr/sbin/sendmail mode
fi
```


4.6 Login Controls

The files `/etc/security/login.cfg` and `/etc/security/user` manages several settings for managing the login process.

The related CIS controls include: [4.3 Configure Automatic Session Locking on Enterprise Assets](#) and [4.10 Enforce Automatic Device Lockout on Portable End-User Devices](#)

4.6.1 /etc/security/login.cfg - logintimeout (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of seconds during which the password must be typed at login.

Rationale:

In setting the `logintimeout` attribute, a password must be entered within a specified time period.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s usw -a logintimeout
```

The above command should yield the following output:

```
usw logintimeout=30
```

Remediation:

In `/etc/security/login.cfg`, set the `usw` stanza `logintimeout` attribute to 30 or less:

```
chsec -f /etc/security/login.cfg -s usw -a logintimeout=30
```

This means that a user will have 30 seconds, from prompting, in which to type in their password.

Default Value:

60

4.6.2 /etc/security/login.cfg - logindelay (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of seconds delay between each failed login attempt. This works as a multiplier, so if the parameter is set to 10, after the first failed login it would delay for 10 seconds, after the second failed login 20 seconds etc.

Rationale:

In setting the `logindelay` attribute, this implements a delay multiplier in-between unsuccessful login attempts.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logindelay
```

The above command should yield the following output:

```
default logindelay=10
```

Remediation:

In `/etc/security/login.cfg`, set the default stanza `logindelay` attribute to 10 or greater:

```
chsec -f /etc/security/login.cfg -s default -a logindelay=10
```

This means that a user will have to wait 10 seconds before being able to re-enter their password. During subsequent attempts this delay will increase as a multiplier of (the number of failed login attempts * logindelay)

Default Value:

No limit

4.6.3 herald (logon message) (Automated)

Profile Applicability:

- Level 1

Description:

This change adds a default herald to `/etc/security/login.cfg`.

Rationale:

This change puts into place a suggested login herald to replace the default entry. A `herald` should not provide any information about the operating system or version. Instead, it should detail a company standard acceptable use policy.

This *suggestion* for a herald should be tailored to reflect your corporate standard policy.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a herald | read stanza herald  
print ${herald}
```

The above command should yield the following output:

```
herald="Unauthorized use of this system is prohibited.\nlogin:"
```

Remediation:

Add a default login herald to `/etc/security/login.cfg`:

```
chsec -f /etc/security/login.cfg -s default -a herald="Unauthorized use of  
this system is prohibited.\\nlogin:"
```

Default Value:

N/A

4.6.4 loginretries (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of attempts a user has to login to the system before their account is disabled.

Rationale:

In setting the `loginretries` attribute, this ensures that a user can have a pre-defined number of attempts to get their password right, prior to locking the account.

Impact:

The setting chosen here (5) is a group consensus as secure enough. However, a local site-policy may have a more strict requirement for all, or some systems.

While the audit and artifact currently test for exactly 5 - the actual recommendation is: greater than 0 (zero) AND (less than or equal to 5 (five) **OR** greater than 0 (zero) AND not greater than 5 (five)

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a loginretries
```

The above command should yield the following output:

```
default loginretries=5
```

Remediation:

In `/etc/security/user`, set the default stanza `loginretries` attribute to 5:



```
chsec -f /etc/security/user -s default -a loginretries=5
```

This means that a user will have 5 attempts to enter the correct password. This does not apply to the root user, which has its own stanza entry disabling this feature.

Default Value:

No limit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</u></p> <p>Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.</p>			

4.6.5 Unattended terminal session timeout is 900 seconds (or less) (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

`TMOUT` and `TIMEOUT` are environmental setting that activate the timeout of a shell. The value is in seconds.

- `TMOUT=n` - Sets the shell timeout to *n* seconds. A setting of `TMOUT=0`, or `unset TMOUT` disables the automatic session timeout.
- `readonly TMOUT`- Both `export` and `lock` `TMOUT` environmental variable to it's present value, preventing unwanted modification during run-time.

Rationale:

All systems are vulnerable if terminals are left logged in and unattended. The most serious problem occurs when a system manager leaves a terminal unattended that has been enabled with root authority. In general, users should log out anytime they leave their terminals.

You can force a terminal to log out after a period of inactivity by setting the `TMOUT` and `TIMEOUT` parameters in the `/etc/profile` file. The `TMOUT` parameter works in the `ksh` (Korn) shell, and the `TIMEOUT` parameter works in the `bsh` (Bourne) shell.

Impact:

This recommendation is set at Level 2 (using `readonly`).

The recommendation - at Level 1, would use `export` instead.

Audit:

Execute the following command:

```
readonly | /usr/bin/egrep -e "TMOUT|TIMEOUT"
```

This should return:

```
TIMEOUT=900
TMOUT=900
```

Note: Depending on company policy the value may also be less than 900.

Remediation:

Review `/etc/profile` to verify that `TMOUT` is configured to:

- include a timeout of no more than 900 seconds
- to be `readonly`
- verify `readonly` statement is the last statement

```
/usr/bin/egrep -n -e "TMOUT|TIMEOUT" /etc/profile
```

This should return something similar to:

```
40:# TMOUT=120
41:TMOUT=900
42:TIMEOUT=900
43:readonly TMOUT TIMEOUT
```

If either setting is missing, and/or the `readonly` statement, add these to `/etc/profile`.







Default Value:

`TMOUT=0`

References:

1. <https://www.ibm.com/docs/en/aix/7.1?topic=security-unattended-terminals>

CIS Controls:

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

4.7 Trusted Files and Directories

This section of the benchmark will focus on locking down access to specific key configuration files, log files and directories. If these critical files and directories have incorrect ownership and permissions, they can provide an attacker with a method of attack, or with pertinent system information.

Some of the files and directories changed in this section may not exist on your system. In this instance the recommendation can be ignored.

These files and directories should be included in the TSD (Trusted Signature Database). In any case, that provides a process to regularly verify correct ownership and file/directory mode. In TE (Trusted Execution) mode unauthorized modification of files can be prevented and all access (attempts) can be logged.

4.7.1 Trusted Directories

The key element here is that the directories have a specific owner and mode.

Their entry in the TSD will look something like this:

```
trustchk -q /etc/security
/etc/security:
    type = DIRECTORY
    owner = root
    group = security
    mode = 750
    size = 4096
```

- NOTE: IBM AIX, sadly, does not include directories in the TSD by default. Fortunately, adding a directory to the TSD is an easy process.

4.7.1.1 Home directory must exist (Manual)

Profile Applicability:

- Level 1

Description:

All accounts must have a trusted started point - a **HOME** directory.

Rationale:

A missing home directory on many systems places the account in a default directory. Examples include: / and /home/guest.

This recommendation is specifically about *locally* administered accounts (in AIX terms, – R files). If an account exists in the local registry it must have a home directory that is accessible. This is to ensure it is not an invalid account (e.g., restored via a backup accidentally). If a valid account - it still needs a home directory.

As the difference between: *valid* account but missing a HOME directory and *invalid* account but missing a HOME directory cannot be made by a script - the recommendation is to lock the account.

Impact:

A valid user can open a ticket and get a HOME directory created or restored.

The risk of an *invalid user* gaining access via an old username is reduced.

Audit:

Ensure HOME directories exists for **local** administered accounts.

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "Recommend Lock Account [%s]: Missing \${HOME} at: %-
32s\n" ${name} ${home}
        fi
    fi
done
```







- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (`uid`) greater or equal to 200.

Remediation:

Lock local accounts with UID >= 200 when HOME directory does not exist:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "Locked Account [%s]: Missing \${HOME} at: %-32s\n"
${name} ${home}
            /usr/bin/chuser -R files account_locked=true ${name}
        fi
    fi
done
```

CIS Controls:

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

4.7.1.2 Home directory must be owned by account, or special account (Manual)

Profile Applicability:

- Level 1

Description:

All user home directories must have a suitable owner UID.

Rationale:

Manipulating home directories may enable malicious users to steal or modify data, or to gain other user's system privileges. The UID (or owner) of the HOME directory needs to be either the account or a special account defined for this purpose.

When the account is the owner - the security policy must specify that (some) accounts may have DAC authorization to modify HOME directory contents. Security policy may also specify a special UID used to own HOME directories to prevent accounts from modifying the layout and/or content of the HOME directory.

The assumption of this recommendation is that security policy has not specified either. The recommendation is to lock accounts when the HOME directory is not owned by the user or by *root*.

Impact:

Locally* administered accounts with HOME directories owned by a **random userid will be locked.

Valid users can open a ticket to get the UID of their HOME directory corrected.

The risk of a malicious user modifying an accounts HOME directory is reduced.

Audit:

Ensure HOME directory exists and is owned by account (or root)

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; Recommend Lock Account
[%s]\n" ${home} ${name}
            continue
        else
            /usr/bin/perl -e '
                $user=$ARGV[0]; $hd=$ARGV[1]; $uid=$ARGV[2]; $huid=((stat
$hd)[4]);
                if ($huid != $uid && $huid != 0) {
                    exit(1); # triggers command after OR (||)
                }' ${name} ${home} ${uid} || \
                /usr/bin/printf "Recommend Lock Account: %s does not own
%s\n" ${name} ${home}
            fi
        fi
    fi
done
```







- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (`uid`) greater or equal to 200.
Also, if the **HOME** directory has already been defined to something *special* (here, `/dev/null`) no `audit` is performed.

Remediation:

For all local accounts with UID >= 200:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; Run appropriate CIS
remediation\n" ${home} ${name}
            continue
        else
            /usr/bin/perl -e '
                $user=$ARGV[0]; $hd=$ARGV[1]; $uid=$ARGV[2]; $huid=((stat
$hd)[4]);
                if ($huid != $uid && $huid != 0) {
                    printf("Locked Account: %s does not own %s.\n",
${user},${hd});
                    exit(1); # triggers command after OR (||)
                }' ${name} ${home} ${uid} || \
                /usr/bin/chuser -R files account_locked=true $name
        fi
    fi
done
```

CIS Controls:

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

4.7.1.3 Home directory: write access restricted to 'owner' (Automated)

Profile Applicability:

- Level 1

Description:

Home directories must be writeable only by the `owner`. This recommendation audits (or removes) any write permission given via traditional file mode permissions (using `chmod`). Neither should a home directory have any permissions managed (whether permit or deny) via ACL's.

Rationale:

HOME directories with *group* or *world* write access enable malicious users to add files or directories, or even remove them if the directory 'T' (SVTX) bit is not also set. While this does not necessarily allow access to data - existing data might be destroyed (`unlink()`) or replaced (new file added with same name). These modifications could be used, e.g., to use the users authorizations to gain other system privileges.

Disabling read and execute access for *world* and/or *group* might be part of a company security policy - and the audit and remediation scripts will need to be modified to reflect this addition.

The use of ACL's is discouraged because their effect is not immediately visible using standard tools. They must be identified (locating inodes with permission bit 0200000000 set) as active and read using `aclget` before the actual permissions granted or denied are known. Better is to deny outside access to home (ie, user) related data. When data must be shared create an area outside of `${HOME}`.

Impact:

There should be no impact - at least as far a *world* permissions are concerned. There is a potential that all members in the `group` `staff` or `system` might see minimal impact - if their systems have, or had, a default `umask` of `002` when their accounts were created.

Accounts created with a default `umask` of `022` or stricter will not be impacted, unless a user account modified their HOME directory mode bits to permit *group* and/or *other* write access.

Audit:

Validate the permissions of all of the directories changed:

```
#!/usr/bin/ksh -e
lsuser -R files -a id home ALL | while read name ids homes rest;
do
    uid_check=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid_check} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; recommend to lock account
named [%s]\n" ${home} ${name}
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            /usr/bin/perl -e '$f=$ARGV[0]; $m=(stat $f)[2]; \
printf("Recommend chmod on: %s: to remove group or world write
mode\n", $f) if $m & 022; \
printf("Recommend remove ACL on: %s\n ", $f) if $m & 0200000000; \
exit($m & 0200000022)' ${home} \
|| (ls -led ${home} && (aclget ${home} | grep -ip Enabled))
        fi
    fi
done
```

- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (`uid`) greater or equal to 200. Also, if the **HOME** directory has already been defined to something *special* (here, `/dev/null`) no audit is performed.

Remediation:

For all local accounts with UID >= 200:

- Remove write permission from home directories that have group or world write access:

```
#!/usr/bin/ksh -e
# home_mode_acl: 4.8.1.3
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
typeset -i UIDCK=$1
typeset -i ret=0
if test $UIDCK == 0; then
    UIDCK=200
fi
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid_check=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid_check} -ge ${UIDCK} ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; locking account named [%s]\n"
            ${home} ${name}
            chuser -R files account_locked=true $name
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            perl -e '$f=$ARGV[0]; $m=(stat $f)[2];\
                exit (($m & 022) + 1) if ($m & 0200000000);\
                exit($m & 022);' $home
            # exit($m&022 +1) if ($m & 0200000000) else exit ($m &022); ' $home
            ret=?
            [[ $ret == 0 ]] && continue
            if (( $ret & 022 )); then
                printf "%s: had group or world write mode\n" $home
                chmod og-w ${home}
            fi
            if (($ret & 1)); then
                printf "%s: had ACL defined and enabled\n" $home
                rm -rf /tmp/${}/${home}
                mkdir -p /tmp/${}/${home}
                aclget /tmp/${}/${home} | aclput ${home}
                rm -rf /tmp/${}/${home}
            fi
        fi
    fi
done
```

- NOTE: The permission change is automatically applied to all accounts with a user ID (uid) greater or equal to 200. Also, if the **HOME** directory has already

been defined to something *special* (here, `/dev/null`) no change is made to the account attributes.

- To automate the process for new users see **Additional Information** below.

Default Value:

`drwxr-wr-w` (or Directory, 755)

Additional Information:

To automate this during account creation (`mkuser`) a customized `mkuser.sys` script named `/etc/security/mkuser.sys.custom` must be created and ensure that `chmod` is called with either

```
chmod u=rwx,g=rx,o= $1
```







or

```
chmod og=-w $1
```

Likely the command will look something like:

```
mkdir -p $1 && chmod og-w $1
```

CIS Controls:

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

4.7.1.4 AUDIT subsystem: /audit and /etc/security/audit (Automated)

Profile Applicability:

- Level 1

Description:

The `/audit` directory is the default location for output produced from the audit subsystem. The audit subsystem configuration files are in `/etc/security/audit`.

Rationale:

The `/etc/security/audit` and `/audit` directories stores the audit configuration and output files. Access controls must prevent unauthorized access.

Audit:

Validate the permissions of `/etc/security/audit` and `/audit`:

```
#!/usr/bin/ksh -e
# audit_subsys:4.8.1.4
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
typeset -i ret
# Expected output is:
mkdir /tmp/$$
cat - <<EOF >/tmp/$$/audit_subsys.expected
drwxr-s---- root audit /audit
drwxr-s---- root audit /etc/security/audit
EOF

# Live output is:
ls -led /etc/security/audit /audit | \
  /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}' \
  >/tmp/$$/audit_subsys.live

# Compare expected and live and report if not matching
cmp /tmp/$$/audit_subsys.expected /tmp/$$/audit_subsys.live >/dev/null
ret=$?
rm -rf /tmp/$$
[[ $ret != 0 ]] && print -- AUDIT Subsystem permissions incorrect
exit $ret
```

Remediation:







Ensure correct ownership and permissions are in place for `/etc/security/audit` and `/audit`.

```
#!/usr/bin/ksh -e
# audit_subsys:4.8.1.4
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
for AUDITDIR in /etc/security/audit /audit; do
    find ${AUDITDIR} | grep -v 'lost+found' | xargs chown root:audit
    find ${AUDITDIR} -type d | grep -v 'lost+found' | xargs chmod u=rwx,g=rs,o=
    find ${AUDITDIR} ! -type d | grep -v 'lost+found' | xargs chmod -R
u=rw,g=r,o=
done
```

Default Value:

N/A

CIS Controls:

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

4.7.1.5 SECURITY Subsystems: /etc/security (Automated)

Profile Applicability:

- Level 1

Description:

This `/etc/security` directory contains multiple files and directories used to keep the targeted AIX system secure. Most subsystems are owned by `root:security` (UID:GID). However, additional systems such as **AUDIT** and **AIXPERT** have their own permissions (and recommendations).

Traditionally, `/etc/security` has been identified as **USER** administration - including the shadow password file. But there is much more under `/etc/security`. Normal installations also have configuration files for security subsystems including: `aixpert`, `tsd`, `ice`, `ldap`, `rbac`, `audit`, `ipsec`, `fpm`, and trusted computing (`tsd`).

While these subsystems may not be enabled - their files need to be secured to ensure no unauthorized access.

Rationale:

The `/etc/security` directory contains sensitive files for multiple security systems. For the **USER** subsystem there are files such as `/etc/security/passwd`, `/etc/security/user` that must be secured from unauthorized access and modification.

Audit:

Validate the permissions of `/etc/security`:

```
#!/usr/bin/ksh -e
# security_subsys:4.8.1.5
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

EXCLUDE="security/(aixpert|audit|ice)"
find /etc/security -type d | \
  /usr/bin/egrep -v ${EXCLUDE} | \
  /usr/bin/sort | xargs ls -led | \
  /usr/bin/awk '{print $1 " " " $3 " " " $4 " " " $9}' | \
  /usr/bin/grep -v drwxr-s----
```

The command should not yield any output:

Remediation:

Ensure correct access control settings for security subsystem configuration files installed in /etc/security:

```
#!/usr/bin/ksh -e
# security_subsys:4.8.1.5
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022







EXCLUDE="security/(aixpert|audit|ice)"

find /etc/security -type d | \
  /usr/bin/egrep -v ${EXCLUDE} | \
  /usr/bin/sort | xargs ls -led | \
  /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}' | \
  /usr/bin/grep -v drwxr-s---- | \
  awk '{print $NF}' | while read SECDIR; do
    find ${SECDIR} | grep -v ${EXCLUDE} | xargs chown root:security
    find ${SECDIR} -type d | grep -v ${EXCLUDE} | xargs chmod u=rwx,g=rxs,o=
    find ${SECDIR} -type f | grep -v ${EXCLUDE} | xargs chmod -R u=rw,g=r,o=
  done
```

Default Value:

N/A

CIS Controls:

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

4.7.1.6 /var/adm/ras (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/ras` directory contains log files which contain sensitive information such as login times and IP addresses.

Rationale:

The log files in the `/var/adm/ras` directory can contain sensitive information such as login times and IP addresses, which may be altered by an attacker when removing traces of system access. All files in this directory must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of the files in `/var/adm/ras`:

```
ls -l /var/adm/ras | awk '{print $1 " " $3 " " $4 " " $9}'
```

NOTE: The output from the command above will contain numerous files. No files should have read or write permission for other

Remediation:







Remove world read and write access from all files in `/var/adm/ras`:

```
chmod o-rw /var/adm/ras/*
```

Default Value:

N/A

CIS Controls:

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

4.7.1.7 /var/adm/sa (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/sa` directory holds the performance data produced by the `sar` utility.

Rationale:

The `/var/adm/sa` directory contains the report files produced by the `sar` utility. This directory must be secured from unauthorized access.

Audit:

Validate the permissions of `/var/adm/sa`:

```
ls -ld /var/adm/sa | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
rwxr-xr-x  adm  adm  /var/adm/sa
```

Remediation:







Set the recommended ownership and permissions on `/var/adm/sa`:

```
chown adm:adm /var/adm/sa
chmod u=rwx,go=rx /var/adm/sa
```

Default Value:

N/A

CIS Controls:

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

4.7.1.8 /var/spool/cron/crontabs (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/spool/cron/crontabs` directory contains all of the `crontabs` for the users on the system.

Rationale:

The `/var/spool/cron/crontabs` directory contains all of the `crontabs` for the users on the system. Crontab files present a security problem because they are run by the `cron` daemon, which runs with super user rights. Allowing other users to have read/write permissions on these files may allow them to escalate their privileges. To negate this risk, the directory and all the files that it contains must be secured.

Audit:

Validate the permissions of `/var/spool/cron/crontabs`:

```
ls -ld /var/spool/cron/crontabs | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxrwx---  root  cron  /var/spool/cron/crontabs
```

Remediation:







Apply the appropriate permissions to `/var/spool/cron/crontabs`:

```
chmod -R o= /var/spool/cron/crontabs
chmod ug=rwx,o= /var/spool/cron/crontabs
chgrp -R cron /var/spool/cron/crontabs
```

Default Value:

N/A

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>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.7.1.9 Ensure all directories in root PATH deny write access to all (Automated)

Profile Applicability:

- Level 1

Description:

To secure the root users executable PATH, all directories must not be group and world writable.

Rationale:

There should not be group or world writable directories in the root user's executable path. This may allow an attacker to gain super user access by forcing an administrator operating as root to execute a Trojan horse program.

Audit:

Execute the following code as the `root` user:

```
echo "/*:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd)}
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && print " WARNING ${DIR} is world
writable"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && print " WARNING ${DIR} is group
writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

The above command should yield no output

Remediation:

Search and report on group or world writable directories in root's PATH. The command must be run as the root user. The script below traverses up each individual directory PATH, ensuring that all directories are not group/world writable and that they are owned by root or the bin user:

```
echo "/*:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd)}
print "Checking ${DIR}"
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && print " WARNING ${DIR} is world
writable" || print " ${DIR} is not world writable"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && print " WARNING ${DIR} is group
writable" || print " ${DIR} is not group writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

NOTE: Review the output and manually change the directories, if possible. Directories which are group and/or world writable are marked with "WARNING"

To manually change permissions on the directories:

To remove group writable access:

```
chmod g-w <dir name>
```

To remove world writable access:

```
chmod o-w <dir name>
```

To remove both group and world writable access:

```
chmod go-w <dir name>
```

To change the owner of a directory:

```
chown <owner> <dir name>
```

To fully automate the PATH directory permission changes execute the following code as the root user:

```







echo "/*:${PATH}" | tr ':' '\n' | grep "^/" | sort -u | while read DIR
do
DIR=${DIR:-$(pwd) }
while [[ -d ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(d???????w? *) ]] && chmod o-w ${DIR} && print
"Removing world write from ${DIR}"
[[ "$(ls -ld ${DIR})" = @(d????w???? *) ]] && chmod g-w ${DIR} && print
"Removing group write from ${DIR}"
DIR=${DIR%/*}
done
done

```

Default Value:

N/A

CIS Controls:

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

4.7.1.10 *Ensure root user has a dedicated home directory (Automated)*

Profile Applicability:

- Level 1

Description:

The root user must have a dedicated home directory and not use / as their home directory.

Rationale:

By default, the home directory for the root user on AIX is /. This means that all configuration files and directories it creates are visible to all users and may be accessible if the root user has a weak umask setting.

Moving these files to a dedicated home directory and setting appropriate file permissions allows for appropriate use of discretionary access control to these files.

Audit:

Run the following command

```
lsuser -a home root
```

It should NOT return

```
root home=/
```

Remediation:

Create a new home directory for the root user

```
mkdir /root
```

Set ownership and permissions on this directory







```
chown root:system /root  
chmod 0700 /root
```

Update the home directory for the root user

```
chuser home=/root root
```

Move any necessary configuration files or directories to this new directory

CIS Controls:

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

4.7.1.11 /etc/security/audit (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/security/audit` directory contains the system audit configuration files.

Rationale:

The `/etc/security/audit` directory stores the audit configuration files. This directory must have adequate access controls to prevent unauthorized access.

Audit:

Validate the permissions of `/etc/security/audit`:

```
ls -ld /etc/security/audit | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---  root  audit  /etc/security/audit
```

Remediation:







Ensure correct ownership and permissions are in place for `/etc/security/audit`:

```
chown -R root:audit /etc/security/audit
chmod u=rwx,g=rx,o= /etc/security/audit
chmod -R u=rw,g=r,o= /etc/security/audit/*
```

Default Value:

N/A

CIS Controls:

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

4.7.2 Trusted Files

Trusted Files are files that are key to maintaining system integrity. Two common groups of trusted files are: a) user/application configuration files and b) log files.

Configuration Files should be added to the TSD database. If they are not meant to be changed under normal operations they should be added with a signature, otherwise add with SIZE=VOLATILE.

In all cases the file owner/group ids, and file mode should be specified.

- An excerpt of a VOLATILE file entry:

```
trustchk -q /etc/passwd
/etc/passwd:
    owner = root
    group = security
    mode = TCB,644
    type = FILE
    hardlinks =
    symlinks =
    size = VOLATILE
    cert_tag =
    signature = VOLATILE
    hash_value = VOLATILE
```

- An excerpt of a signed configuration file:

```
/usr/lib/boot/chrp.cd.proto:
    owner = root
    group = system
    mode = 400
    type = FILE
    hardlinks =
    symlinks =
    size = 3933
    cert_tag = 00d3cbd2922627b209
    signature =
7b41ae27dd44b543c35640e3e64c77ed7302c15e207855caa20e23f4fcf27db56dbfb854a24ee
a37fec15372a0f7c36467f325f5d8ad3a8256151a6a722d
416ad6b8676bcf70823ffb9fd3f890af0d8d8de51421e2fa2cb791556564873e605e4e455c587
42422c4f9580b6e44e0597ceb0f2fd6635af7f0b5bcc7d45d992600
    hash_value =
9f7592e3889cdb8825b641006bbdc855a9b036d3b9b11e6036d9faffda07eb3c
```

4.7.2.1 New configuration file for sendmail /etc/mail/submit.cf (Manual)

Profile Applicability:

- Level 1

Description:

From 7.2.4, sendmail is updated to version 8.15.2, there is a new configuration file /etc/mail/submit.cf. Need the permission changed to 640?

Rationale:

Privileged access to make changes to this configuration file /etc/mail/submit.cf.

Impact:

It will not impact the usability of application or system.

Audit:

```
perl -e 'printf "%o\n", (stat shift)[2] & 07777' /etc/mail/submit.cf
```





Remediation:

```
chmod 640 /etc/mail/submit.cf
```

References:

1. Reference to manpage

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.5 <u>Implement DMARC</u> To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.			
v7	7.8 <u>Implement DMARC and Enable Receiver-Side Verification</u> To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.			

4.7.2.2 Verify Trust of suid, sgid, acl, and trusted-bit files and programs (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for both `suid` and `sgid` files and programs.

Rationale:

An audit should be performed on the system to search for the presence of both `suid` and `sgid` files and programs. In order to prevent these files from being potentially exploited the `suid` and `sgid` permissions should be removed wherever possible.

Audit:

Re-execute the appropriate find command and review the output. This should reflect the changes made in the remediation section.

If there are non-local filesystems which cannot be un-mounted, use the following to find all `suid` and `sgid` files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -type f -ls
```

If all non-local filesystems are un-mounted:

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Remediation:

Review the currently mounted filesystems:

```
mount
```

Un-mount all non-local filesystems and cdrom media:

```
umount <mount point>
```

If there are non-local filesystems which cannot be un-mounted, use the following to find all `suid` and `sgid` files on local JFS/JFS2 filesystems only:

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -type f -ls
```

If all non-local filesystems have been un-mounted:

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Review the files and where possible, use the `chmod` command to remove the appropriate `suid` or `sgid` bits:

```
chmod u-s <file>  
chmod g-s <file>
```

Default Value:

N/A







Additional Information:

Reversion:

Use the `chmod` command to re-instate the `suid` and `sgid` bits to the relevant files:

```
chmod u+s <file>  
chmod g+s <file>
```

CIS Controls:

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

4.7.2.3 crontab entries - owned by userid (Automated)

Profile Applicability:

- Level 1

Description:

This script checks the permissions of all the root `crontab` entries, to ensure that they are owned and writable by the root user only.

Rationale:

All root `crontab` entries must be owned and writable by the root user only. If a script had group or world writable access, it could be replaced or edited with malicious content, which would then subsequently run on the system with root authority.

Audit:

From the command prompt, execute the following script:

```
crontab -l |egrep -v '^#' |awk '{print $6}' |grep "^/" |sort -u | while read
DIR
do
DIR=${DIR:-$(pwd) }
while [[ -a ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(((((((w? *) )) && print " WARNING ${DIR} is world
writable"
[[ "$(ls -ld ${DIR})" = @((((w???? *) )) && print " WARNING ${DIR} is group
writable"
[[ "$(ls -ld ${DIR} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

Remediation:

Ensure that all root crontab entries are owned and writable by root only.

The script below traverses up each individual directory path, ensuring that all directories are not group/world writable and that they are owned by the root or bin user:

```
crontab -l | egrep -v '^#' | awk '{print $6}' | grep "^/" | sort -u | while read
DIR
do
DIR=${DIR:-$(pwd) }
while [[ -a ${DIR} ]]
do
[[ "$(ls -ld ${DIR})" = @(((((((w? *) )) && print " WARNING ${DIR} is world
writable"
[[ "$(ls -ld ${DIR})" = @((((w???? *) )) && print " WARNING ${DIR} is group
writable"
[[ "$(ls -ld ${DIR} | awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${DIR} is not owned by root or bin"
DIR=${DIR%/*}
done
done
```

NOTE: Review the output and manually change the directories, if possible. Directories which are group and/or world writable or not owned by root are marked with "WARNING"

To manually change permissions on the files or directories:

To remove group writable access:

```
chmod g-w <name>
```

To remove world writable access:

```
chmod o-w <name>
```

To remove both group and world writable access:

```
chmod go-w <name>
```

To change the owner of a file or directory:

```
chown <new user> <name>
```

Default Value:

N/A

Additional Information:







Default AIX Security Expert policy values:

High Level policy Permissions checked

Medium Level policy Permissions checked

Low Level policy Permissions checked

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>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.7.2.4 Home directory configuration files (Automated)

Profile Applicability:

- Level 1

Description:

The user configuration files in each home directory e.g. `$HOME/.profile`, must not be group or world writable.

Rationale:

Group or world-writable user configuration files may enable malicious users to steal or modify other user's data, or to gain elevated privileges.

Audit:

Validate the permissions of all user configuration files:

```
lsuser -a home ALL |cut -f2 -d= |egrep -v "^/$|/etc|/bin|/var|/usr|/usr/sys"
|while read homedir;
do
if [[ -d ${homedir} ]];
then
echo "Listing all user configuration files in '${homedir}'"
ls -a ${homedir} |egrep "^\. [a-z]" |while read file;
do
if [[ -f "${homedir}/${file}" ]];
then
ls -l "${homedir}/${file}"
fi
done
else
echo "ERROR - no home directory for '${homedir}'"
fi
done
```

Remediation:

Search and remediate any user configuration files which have group or world writable access:







```
lsuser -a home ALL |cut -f2 -d= |egrep -v "^/$|/etc|/bin|/var|/usr|/usr/sys"
|while read homedir;
do
if [[ -d ${homedir} ]];
then
echo "Removing 'go-w' from all user configuration files in '${homedir}'"
ls -a ${homedir} |egrep "^\. [a-z]" |while read file;
do
if [[ -f "${homedir}/${file}" ]];
then
echo "Running 'chmod go-w' on '${homedir}/${file}'"
chmod go-w "${homedir}/${file}"
fi
done
else
echo "ERROR - no home directory for '${homedir}'"
fi
done
```

NOTE: The permission change is automatically applied

Default Value:

N/A

CIS Controls:

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

4.7.2.5 /smit.log (Automated)

Profile Applicability:

- Level 1

Description:

The /smit.log file maintains a history of all smit commands run as root.

Rationale:

The /smit.log file may contain sensitive information regarding system configuration, which may be of interest to an attacker. This log file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of /smit.log:

```
ls -l /smit.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /smit.log
```

Remediation:







Remove world read and write access to /smit.log:

```
chmod o-rw /smit.log
```

Default Value:

644

CIS Controls:

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

4.7.2.6 /etc/group (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/group` file contains a list of the groups defined within the system.

Rationale:

The `/etc/group` file defines basic group attributes. Since the file contains sensitive information, it must be properly secured.

Audit:

Validate the permissions of `/etc/group`:

```
ls -l /etc/group | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--  root      security  /etc/group
```

Remediation:







Ensure correct ownership and permissions are in place for `/etc/group`:

```
chown root:security /etc/group
chmod u=rw,go=r /etc/group
```

Default Value:

644

CIS Controls:

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

4.7.2.7 /etc/inetd.conf (Automated)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership for `/etc/inetd.conf` are applied.

Rationale:

The `/etc/inetd.conf` file contains the list of services that `inetd` controls and determines their current status i.e. active or disabled. This file must be protected from unauthorized access and modifications to ensure that the services disabled in this benchmark remain locked down.

Audit:

From the command prompt, execute the following command:

```
ls -l /etc/inetd.conf | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--  root      system /etc/inetd.conf
```

Remediation:







Set the recommended permissions and ownership to `/etc/inetd.conf`:

```
chmod u=rw,go=r /etc/inetd.conf
chown root:system /etc/inetd.conf
trustchk -u /etc/inetd.conf mode=644
```

Default Value:

664, root:system

CIS Controls:

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

4.7.2.8 /etc/motd (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/motd` file contains the message of the day, shown after successful initial login.

Rationale:

The `/etc/motd` file contains the message of the day, shown after successful initial login. The file should only be editable by its owner.

Audit:

Validate the permissions of `/etc/motd`:

```
ls -l /etc/motd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--  bin  bin  /etc/motd
```

Remediation:







Apply the appropriate permissions to `/etc/motd`:

```
chown bin:bin /etc/motd
chmod u=rw,go=r /etc/motd
```

Default Value:

644

CIS Controls:

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

4.7.2.9 /etc/passwd (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/passwd` file contains a list of the users defined within the system.

Rationale:

The `/etc/passwd` file defines all users within the system. Since the file contains sensitive information, it must be properly secured.

Audit:

Validate the permissions of `/etc/passwd`:

```
ls -l /etc/passwd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r--  root      security  /etc/passwd
```

Remediation:







Ensure correct ownership and permissions are in place for `/etc/passwd`:

```
chown root:security /etc/passwd
chmod u=rw,go=r /etc/passwd
```

Default Value:

644

CIS Controls:

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

4.7.2.10 /etc/ssh/ssh_config (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/ssh_config` file defines SSH client behavior.

Rationale:

The `/etc/ssh/ssh_config` file is the system-wide client configuration file for OpenSSH, which allows you to set options that modify the operation of the client programs. The recommended value is not to provide any writable access rights for any user other than `root`.

Audit:

Ensure that the `/etc/ssh/ssh_config` permissions are correct, and also that there are no ACL's set that might be providing otherwise unnoticed access:

```
ls -le /etc/ssh/ssh_config | awk '{print $1 " " $3 " " $4 " " $9}' `
```

The above command should yield the following output:

```
-rw-r--r-- root system /etc/ssh/ssh_config `
```

Remediation:

Change the permissions of the `/etc/ssh/ssh_config` file to ensure that only the owner can read and write to the file:

```
chmod 644 /etc/ssh/ssh_config
```







Default Value:

640

Additional Information:

Using the octal mode to (re)set the mode will also disable any ACL's that might have been set.

CIS Controls:

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

4.7.2.11 /etc/ssh/sshd_config (Automated)

Profile Applicability:

- Level 1

Description:

The `/etc/ssh/sshd_config` file defines SSH server behavior.

Rationale:

The SSH daemon reads the configuration information from this file and includes the authentication mode and cryptographic levels to use during SSH communication.

Impact:

Some organizations feel all configuration information for OpenSSH server must be confidential - and many other benchmarks recommend exclusive root access to the file `/etc/ssh/sshd_config`. This configuration will work **UNLESS** `sftp` access is required by non-root users.

Non-root users (when mode is octal 0600) cannot `load_server_config` and the connection closes even though authentication succeeded.

```
Jun 25 14:42:45 x071 auth|security:info sshd[12255378]: Accepted password for
michael from 192.168.129.65 port 32810 ssh2
Jun 25 14:42:45 x071 auth|security:info sftp-server[7077962]: session opened
for local user michael from [192.168.129.65]
Jun 25 14:42:45 x071 auth|security:debug sftp-server[7077962]: debug2:
load_server_config: filename /etc/ssh/sshd_config
Jun 25 14:42:45 x071 auth|security:info sshd[8847468]: Received disconnect
from 192.168.129.65 port 32810:11: disconnected by user
Jun 25 14:42:45 x071 auth|security:info sshd[8847468]: Disconnected from user
michael 192.168.129.65 port 32810
```

- This is what is needed for the `sftp-server` to start:

```

Jun 25 14:45:10 x071 auth|security:info sshd[7077994]: Accepted password for
michael from 192.168.129.65 port 32812 ssh2
Jun 25 14:45:10 x071 auth|security:info sftp-server[11272308]: session opened
for local user michael from [192.168.129.65]
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug2:
load_server_config: filename /etc/ssh/sshd_config
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug2:
load_server_config: done config len = 288
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug2:
parse_server_config: config /etc/ssh/sshd_config len 288
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug3:
/etc/ssh/sshd_config:34 setting SyslogFacility AUTH
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug3:
/etc/ssh/sshd_config:36 setting LogLevel INFO
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug3:
/etc/ssh/sshd_config:114 setting Banner /etc/banner
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug3:
/etc/ssh/sshd_config:117 setting Subsystem sftp\t/usr/sbin/sftp-server -l
DEBUG3 -f AUTH
Jun 25 14:45:10 x071 auth|security:info sftp-server[11272308]: received
client version 3
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug3:
request 0: realpath
Jun 25 14:45:10 x071 auth|security:info sftp-server[11272308]: realpath "."
Jun 25 14:45:10 x071 auth|security:debug sftp-server[11272308]: debug1:
request 0: sent names count 1

```

- The recommendation is to stay with the default file mode (octal 0644) unless site policy requires octal 0600 AND it is acceptable that `sftp` will not function.
- Choosing octal 0600 is considered a Level 2 recommendation

Audit:

Ensure that the `/etc/ssh/sshd_config` permissions have been successfully changed:

```
ls -le /etc/ssh/sshd_config | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r--r-- root system /etc/ssh/sshd_config
```

Remediation:







Change the permissions of the `/etc/ssh/sshd_config` file to ensure all accounts can read the file but only the owner (root) can modify it:

```
chmod u=rw,go=r /etc/ssh/sshd_config
```

Default Value:

644

CIS Controls:

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

4.7.2.12 /var/adm/cron/at.allow (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/at.allow` file contains a list of users who can schedule jobs via the `at` command.

Rationale:

The `/var/adm/cron/at.allow` file controls which users can schedule jobs via the `at` command. Only the root user should have permissions to create, edit, or delete this file.

Audit:

Validate the permissions of `/var/adm/cron/at.allow`:

```
ls -l /var/adm/cron/at.allow | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r----- root sys /var/adm/cron/at.allow
```

Remediation:

Apply the appropriate permissions to `/var/adm/cron/at.allow`:

```
chown root:sys /var/adm/cron/at.allow  
chmod u=r,go= /var/adm/cron/at.allow
```

Default Value:

N/A

4.7.2.13 /var/adm/cron/cron.allow (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/cron.allow` file contains a list of users who can schedule jobs via the `cron` command.

Rationale:

The `/var/adm/cron/cron.allow` file controls which users can schedule jobs via `cron`. Only the root user should have permissions to create, edit, or delete this file.

Audit:

Validate the permissions of `/var/adm/cron/cron.allow`:

```
ls -l /var/adm/cron/cron.allow | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r----- root sys /var/adm/cron/cron.allow
```

Remediation:







Apply the appropriate permissions to `/var/adm/cron/cron.allow`:

```
chown root:sys /var/adm/cron/cron.allow  
chmod u=r,go= /var/adm/cron/cron.allow
```

Default Value:

N/A

CIS Controls:

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

4.7.2.14 /var/ct/RMstart.log (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/ct/RMstart.log` is the logfile used by RMC and can contain sensitive data that must be secured.

Rationale:

RMC provides a single monitoring and management infrastructure for both RSCT peer domains and management domains. Its generalized framework is used by cluster management tools to monitor, query, modify, and control cluster resources, `/var/ct/RMstart.log` is the logfile used by RMC and can contain sensitive data that must be secured.

Audit:

Validate the permissions of `/var/ct/RMstart.log`:

```
ls -l /var/ct/RMstart.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/ct/RMstart.log
```

Remediation:







Remove world read and write from `/var/ct/RMstart.log`:

```
chmod o-rw /var/ct/RMstart.log
```

Default Value:

644

CIS Controls:

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

4.7.2.15 /var/adm/cron/log (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/log` file contains a log of all `cron` jobs run on the system.

Rationale:

The `/var/adm/cron/log`, records all `cron` jobs run on the system. The file permissions must ensure that it is accessible only to its owner and group.

Audit:

Validate the permissions of `/var/adm/cron/log`:

```
ls -l /var/adm/cron/log | awk '{print $1, $3, $4, $9}'
```

The above command should yield the following output:

```
-rw-rw---- bin cron /var/adm/cron/log
```

Remediation:







Specify exact permissions and user.group ids to `/var/adm/cron/log`:

```
chmod ug=rw /var/adm/cron/log  
chown bin.cron /var/adm/cron/log
```

Default Value:

660

CIS Controls:

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

4.7.2.16 /var/tmp/dpid2.log (Automated)

Profile Applicability:

- Level 1

Description:

The /var/tmp/dpid2.log is the logfile used by dpid2 daemon, and contains SNMP information.

Rationale:

The /var/tmp/dpid2.log logfile is used by the dpid2 daemon and can contain sensitive SNMP information. This file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of /var/tmp/dpid2.log:

```
ls -l /var/tmp/dpid2.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/dpid2.log
```

Remediation:







Remove world read and write from /var/tmp/dpid2.log:

```
chmod o-rw /var/tmp/dpid2.log
```

Default Value:

644

CIS Controls:

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

4.7.2.17 /var/tmp/hostmibd.log (Automated)

Profile Applicability:

- Level 1

Description:

The /var/tmp/hostmibd.log is the logfile used by hostmibd daemon, and contains network and machine related information.

Rationale:

The /var/tmp/hostmibd.log log file can contain network and machine related statistics logged by the daemon. This file must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of /var/tmp/hostmibd.log:

```
ls -l /var/tmp/hostmibd.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/hostmibd.log
```

Remediation:







Remove world read and write from /var/tmp/hostmibd.log:

```
chmod o-rw /var/tmp/hostmibd.log
```

Default Value:

644

CIS Controls:

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

4.7.2.18 /var/tmp/snmpd.log (Automated)

Profile Applicability:

- Level 1

Description:

The /var/tmp/snmpd.log is the logfile used by snmpd daemon, and contains network and machine related information.

Rationale:

The /var/tmp/snmpd.log logfile contains sensitive information through which an attacker can find out about the SNMP deployment architecture in your network. This log file must be secured from unauthorized access.

Audit:

Validate the permissions of /var/tmp/snmpd.log:

```
ls -l /var/tmp/snmpd.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/snmpd.log
```

Remediation:







Remove world read and write from /var/tmp/snmpd.log:

```
chmod o-rw /var/tmp/snmpd.log
```

Default Value:

644

CIS Controls:

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

4.8 Trusted Execution (TE)

This is a further development of the Trusted Computing Base (TCB) packaged with previous versions of AIX. Unlike TCB, Trusted Execution is not an install time only option and it can be enabled on previously installed systems. Its primary purpose is to protect from Trojan horse style attacks, by only allowing the execution of certain executables and kernel extensions.

TE has two modes of operation, online and offline. The online mode provides the most comprehensive security, as a check is made every time a file is loaded into memory. If the integrity checks fail, the file will not be loaded into memory. The offline mode checks file integrity at a specified time, via either the command line or via `crontab`.

4.8.1 TE - implementation (Automated)

Profile Applicability:

- Level 2

Description:

The recommendation is to implement TE to protect the system from Trojan horse style attacks. TE provides a robust system integrity checking process.

Rationale:

One of the common ways a hacker infiltrates a system is through file tampering or the use of a Trojan horse. The implementation of TE can provide a number of integrity checks prior to loading a program into memory, any deviations can also be highlighted when programs and files are validated offline. This ensures that the programs executed are those which are intended to be and not malicious code masquerading as a true program.

When a discrepancy is identified it is classified as either minor or major. A minor discrepancy is automatically reset to the value defined in the TSD. In the event of a major discrepancy the file access permissions are changed to make the file inaccessible.

There is a pre-requisite requirement to install CLiC and SSL software.

Audit:

Ensure that TE is enabled:

```
trustchk -p TE
```

The above command should yield the following output:

```
TE=ON
```

Ensure that TEP is enabled:

```
trustchk -p TEP
```

The above command should yield the following output:

```
TEP=ON
```


Remediation:

It is recommended that TE is configured in online mode. This provides real time protection against Trojan horse attacks.

The `tsd.dat` file contains the important security attributes relating to all of the managed files:

```
cat /etc/security/tsd/tsd.dat
```

NOTE: The `trustchk` command is used to manage the entries in this file.

To enable TE, firstly enable online checking of executables and shell scripts:

```
trustchk -p CHKEEXEC=ON
trustchk -p CHKSCRIPT=ON
```

Stop the execution or loading of binaries and files into memory when the integrity checks fail:

```
trustchk -p STOP_ON_CHKFAIL=ON
```

Enable online TE based on the policy selections above:

```
trustchk -p TE=ON
```

To set a Trusted Execution Path or TEP:

```
trustchk -p TEP=<PATH variable>
```

Enable the TEP:

```
trustchk -p TEP=ON
```

NOTE: Commands will not be executed if they reside outside of the TEP.

Further details regarding planning and implementation of TE can be found within the IBM AIX 7.1 Infocentre:

<https://www.ibm.com/docs/en/aix/7.1?topic=configuration-trusted-execution>

NOTE: The configuration of TE is dependant on the unique requirements of a given environment.

Default Value:

Not enabled

References:

1. <https://www.ibm.com/docs/en/aix/7.1?topic=configuration-trusted-execution>

Additional Information:

Reversion:

Disable TE:

```
trustchk -p TE=off
```

Disable TEP:

```
trustchk -p TEP=off
```

4.9 Ensure root access is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Restricts access to root via `su` to members of a specific group. Direct login via console and/or remote login via `telnet` is blocked.

Rationale:

- For accountability, no direct access to root is allowed.
- The attributes here control access to root for programs other than OpenSSH.
- Setting the `sugroups` attribute to `SUADMIN` ensures that only members of the this group are able to `su` root. This makes it more difficult for an attacker to use a stolen root password as the attacker first has to get access to a system user ID.
- Access via a *console* (e.g., `/dev/vty0` or `/dev/tty0`) is only permitted when there are external controls managing accountability of access to the console. For example, HMC access must not be via the account `hscroot`; a physical console is accessible only after a hard-copy log has been entered and verified before physical access is granted to the (data center) console terminal.
- The group `system` is not recommended as it is not uncommon for other accounts to be included in this OS-provided group (`gid==0`).

Impact:

- In this recommendation we specify the group `SAADMIN`. This is same group name applied during installation of the *security profile* known as `BAS - Base AIX Security`.
- When scoring - the attribute `login` may be true as long as access to the HMC is not via the account name `hscroot`.
- In any case, `sugroups` should not equal `ALL`.

Audit:

- From the command prompt, execute the following commands:

```
#!/usr/bin/ksh -e
lsuser -a login rlogin su sugroups root | tr '=' ' ' | read user a1 login a2
rlogin a3 su a4 sugroups
[[ ${su} != "false" && ${sugroups} == "ALL" ]] && print $0 failed :
${a3}==${su}, ${a4}==${sugroups}
[[ ${login} == "true" || ${rlogin} == "true" ]] && print $0 failed :
${a1}==${login}, ${a2}==${rlogin}

- The command should **NOT** output:
```

Remediation:

In `/etc/security/user`, set the root stanza `sugroups` attribute to `SUADMIN` and ensure the `login` and `rlogin` attributes are set to *false*:















```
lsgroup SUADMIN >/dev/null || mkgroup -a SUADMIN
chuser login=false rlogin=false sugroups=SUADMIN
```

- **NOTE:** For the remediation the setting of `su` is irrelevant.

Default Value:

root login=true rlogin=true sugroups=ALL su=true

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.			
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	<u>4.1 Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			
v7	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.10 Disable core dumps (Automated)

Profile Applicability:

- Level 1

Description:

This change disables core dumps in the default user stanza of `/etc/security/limits` and also ensures the `fullcore` kernel parameter is set to false.

Rationale:

The creation of core dumps can reveal pertinent system information, potentially even passwords, within the core file. The ability to create a core dump is also a vulnerability to be exploited by a hacker.

The commands below disable core dumps by default, but they may be specifically enabled for a particular user in `/etc/security/limits`.

Audit:

From the command prompt, execute the following command to validate the `/etc/security/limits` changes:

```
lssec -f /etc/security/limits -s default -a core -a core_hard
```

The above command should yield the following output:

```
default core=0 core_hard=0
```

Ensure that the `fullcore` kernel parameter has been set to false:

```
lsattr -El sys0 -a fullcore
```

The above command should yield the following output:

```
fullcore false Enable full CORE dump True
```

Remediation:







Change the default user stanza attributes `core` and `core_hard` in `/etc/security/limits` and then set the `fullcore` kernel parameter to false:

```
chsec -f /etc/security/limits -s default -a core=0 -a core_hard=0  
chdev -l sys0 -a fullcore=false
```

Default Value:

Core dumps enabled

CIS Controls:

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

4.11 Remove current working directory from default /etc/environment PATH (Automated)

Profile Applicability:

- Level 1

Description:

This change removes any "." or "::" entries from /etc/environment. If a "." or "::" is present the current working directory is included in the default search path.

Rationale:

Any "." and "::" will be removed from /etc/environment. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Examine PATH in /etc/environment to see if it contains any "." or "::" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine PATH in /etc/environment to see if it contains any "." or "::" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```







If the command above yields output, remove the "." and "::" entries from:

```
vi /etc/environment
```

Default Value:

Dot present

CIS Controls:

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

4.12 Lock historical users (Automated)

Profile Applicability:

- Level 1

Description:

Lock OS administrative accounts to further enhance security.

Rationale:

Lock administrative user accounts. Generic OS administrative user accounts are targeted by hackers in an attempt to gain unauthorized access to a server.

Audit:

Ensure that the user accounts have been locked:

```
ACCOUNTS=daemon,bin,sys,adm,uucp,nobody,lpd,lp,invscout,ipsec,nuucp,sshd  
lsuser -a account_locked ${ACCOUNTS} | grep -v account_locked=true
```

The command should not have any output.

Remediation:










Lock standard accounts using chuser:

```
ACCOUNTS=daemon,bin,sys,adm,uucp,nobody,lpd,lp,invscout,ipsec,nuucp,sshd  
lsuser -a account_locked ${ACCOUNTS} | grep -v account_locked=true | while  
read account attributes; do  
    chuser account_locked=true ${account}  
done
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			
v7	<u>16.8 Disable Any Unassociated Accounts</u> Disable any account that cannot be associated with a business process or business owner.			
v7	<u>16.9 Disable Dormant Accounts</u> Automatically disable dormant accounts after a set period of inactivity.			

4.13 Remove current working directory from root's PATH (Automated)

Profile Applicability:

- Level 1

Description:

This change removes any "." or "::" entries from the root PATH. If a "." or "::" is present the current working directory is included in the search path.

Rationale:

Any "." and "::" will be removed from the root PATH. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Ensure that root's PATH does not contain any "." or "::" entries:

```
su - root -c "echo ${PATH}" |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine root's PATH to see if it contains any "." or "::" entries:

```
su - root -c "echo ${PATH}" |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```







If the command above yields output, remove the "." and "::" entries from the relevant initialization files. The files to examine are dependant on the root users shell definition in /etc/passwd. Once the file or files have been identified remove the "." and "::" from the PATH variable

```
vi <filename>
```

Default Value:

Dot not present

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>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.14 Configuration: */etc/motd* (Automated)

Profile Applicability:

- Level 1

Description:

Create a `/etc/motd` file which displays, post initial logon, a statutory warning message.

Rationale:

The creation of a `/etc/motd` file which contains a statutory warning message could aid in the prosecution of offenders guilty of unauthorized system access. The `/etc/motd` is displayed after successful logins from the console, SSH and other system access protocols.

Audit:

Log back into the system via SSH:

```
ssh localhost
```

NOTE: The `/etc/motd` file will now be displayed
Validate that `/etc/motd` is not writable by group or other

```
ls -l /etc/motd
```

Remediation:

Create a `/etc/motd` file:

```
touch /etc/motd
chmod u=rw,go=r /etc/motd
chown bin:bin /etc/motd
```

Below is a sample banner:







```
*****
NOTICE TO USERS
This computer system is the private property of its owner, whether
individual, corporate or government. It is for authorized use only. Users
(authorized or unauthorized) have no explicit or implicit expectation of
privacy. Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and disclosed
to your employer, to authorized site, government, and law enforcement
personnel, as well as authorized officials of government agencies, both
domestic and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection, and
disclosure at the discretion of such personnel or officials. Unauthorized or
improper use of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to use
this system you indicate your awareness of and consent to these terms and
conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this warning.
*****
```

NOTE: Replace "its owner" with the relevant company name

Default Value:

N/A

CIS Controls:

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

5 Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

See [CIS Controls v8: Section 5: Account Management](#)

Implementation Group 1 Recommendations (IG1)

The relevant CIS Controls are:

5.1 Establish and Maintain an Inventory of Accounts (Function: Identify)
5.2 Use Unique Passwords (Function: Protect)
5.3 Disable Dormant Accounts (Function: Respond)
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts (Function: Protect)
5.5 Establish and Maintain an Inventory of Service Accounts (IG1, Function Identify)

Implementation Group 2 Recommendations (IG2)

The remainder of this section focuses on possible changes to the above recommendations that may be needed when multi-user access is 5.5 Establish and Maintain an Inventory of Service Accounts (IG2, Function Identify) 5.6 Centralize Account Management (Function: Protect)

IG1 and AIX Recommendations

The recommendations included in first sub-sections of the chapter are organized following the sub-sections of CIS (v8) Control 5: Account Management.

These recommendation address controls that manage **local** accounts, not accounts managed by an external service (e.g., LDAP).

Note: The **root** account (euid == 0) should never be managed by an external instance.

What is a System Account?

We define OS standard accounts (e.g., bin, daemon, sshd) as system accounts and these should be managed (and locked/disabled) via local controls. The other characteristic that is used to identify an account as *system* account is a) attribute `admin` is set to true; b) both attributes `login` and `rlogin` are set to false. System administrators are expected to have the attribute `login` set to true so that they could, if needed, login to the AIX console.

Basically, *system* accounts should be managed locally - and, with some exceptions - be (b)locked from command line access.

What is a *Regular* Account?

Classically, a *regular* account is any account that does not own application or service data and login to a command-line shell or menu application is expected. Userid (Account Name) and Password are the principle Security Identification and Authentication mechanisms used to validate and grant access to the system. In this sense a system administrator account is seen as a *regular* account. Also, on a multi-user system - any account not an application (data) owner nor a system administrator should be a regular account.

Regular accounts may, perhaps should, be managed by an external service. Ideally, this external service is also aware of the AIX user and group extended attributes.

5.1 Establish and Maintain an Inventory of Accounts

This sub-section has recommendations for managing local accounts: focus here is controls that manage local accounts.

CIS Control Description

- 5.1 Establish and Maintain an Inventory of Accounts

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule, at a minimum quarterly, or more frequently.

Rationale

The recommendations here are focused on a system level rather than *enterprise*.

The controls mention both *user* and *administrator* accounts. For the purpose of this benchmark, an account is *administrator* when the AIX user attribute *admin* is *true*.

Additionally, the benchmark looks also at an inventory of *administrative* groups. Groups are defined as *administrator* when the AIX group attribute *admin* is *true*.

Note also, the general recommendation to review *all* accounts every 13 weeks (or more frequently).

Including *password controls* (see sub-section for Unique Passwords) AIX has approximately 65 user attributes. These attributes include `ulimits`, `umask`, `rlogin` and more.

The recommendations in this section focus on the password related parameters specified in the `default:` user stanza in the file `/etc/security/user`. The values set are applicable if specific values are not defined in a `username:` stanza.

The recommended procedure for user or account management is to not set any of these attributes explicitly (i.e., in a user stanza in `/etc/security/user` unless there is a specific requirement to override setting in `default:` stanza. The exception is the account *root*. For the *root:* stanza specific recommendations will be made regarding the root (aka superuser) account.

The root account should always be locally managed.

User Management and External Services

When `user access credentials` are managed using an external service many, if not all, of the password related parameters may be managed by the external service. As to other attributes, when the external service does not support other AIX user attributes (e.g., LDAP and scheme `rfc2307` (or better, not `rfc2307aix`) other user attributes **not** managed by the LDAP server will be assigned from the default: *stanza* of the following files: `/etc/security/envIRON`, `/etc/security/limits`, `/etc/security/roles`, `/etc/security/user`, `/etc/security/user.roles`.

For local users (e.g., root) these attributes retain their importance. Remember, generally, only a small subset of the attributes are superseded by external authentication services.

5.1.1 Maintain Account Passwords

Maintaining an account implies maintaining current passwords.

Stale passwords might imply a dormant account (see section later in document).

5.1.1.1 histexpire (Automated)

Profile Applicability:

- Level 1

Description:

Defines the period of time in weeks that a user will not be able to reuse a password.

Rationale:

In setting the `histexpire` attribute, it ensures that a user cannot reuse a password within a set period of time.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a histexpire
```

The above command should yield the following output:

```
default histexpire=52
```

Remediation:

In `/etc/security/user`, set the default user stanza `histexpire` attribute to be greater than or equal to 26:




```
chsec -f /etc/security/user -s default -a histexpire=52
```

This means that a user will not be able to reuse any password set in the last 52 weeks (one year).

Default Value:

Disabled

CIS Controls:

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

5.1.1.2 *histsize* (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of previous passwords that a user may not reuse.

Rationale:

In setting the `histsize` attribute, it enforces a minimum number of previous passwords a user cannot reuse.

Impact:

The recommendation is to not use this attribute. This attribute was traditionally used together with *minage* to prevent rapid reuse of old passwords. Instead "Unique Passwords" relies solely on the time-based *histexpire* attribute.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a histsize
```

The above command should yield the following output:

```
default histsize=0
```

Remediation:

In `/etc/security/user`, set the default user stanza `histsize` attribute to be 0:




```
chsec -f /etc/security/user -s default -a histsize=0
```

This means that this setting is not being used for password management.

Default Value:

Disabled

CIS Controls:

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

5.1.1.3 minage (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of weeks before a password can be changed.

Rationale:

The `minage` attribute prohibits users changing their password until a set number of weeks have passed.

Impact:

The AIX community prefers to rely on the AIX attribute `histexpire` rather than a historical `minage` value.

Historically, the `minage` attribute has been used to prevent a user from write a script to spool through `histsize` passwords, and then return to the same password as before. The attribute `histexpire` overrides `histsize`. Therefore, there is no need to force a user to request assistance from system administrators in order to reset a poorly chosen password, or in the case of special accounts that policy states passwords are meant for "one time use".

Again, since AIX has a different way to prevent scripted password re-cycling, the need for `minage` is not longer warranted.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minage
```

The above command should yield the following output:

```
default minage=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minage` attribute to 1:




```
chsec -f /etc/security/user -s default -a minage=1
```

This means that a user can only change their password after one week.

Default Value:

```
minage=0
```


CIS Controls:

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

5.1.2 All accounts must have a hashed password (Automated)

Profile Applicability:

- Level 1

Description:

All (unlocked) accounts on the server must have a password.

For this recommendation we look at the so-called **files** registry - as we cannot reliably review the entries kept in a centralized authentication system such as **LDAP** or

Kerberos.

Rationale:

An account password is a secret code word that must be entered to gain access to the account. If an account exists that has a blank password, multiple users may access the account without authentication and leave a weak audit trail. An attacker may gain unauthorized system access or perform malicious actions, which then cannot be attributed to any specific individual.

Impact:

If no password hash is available and a locked account gets unlocked then the account is available without any verification aka authentication.

Audit:

Run the command:

```
/usr/bin/egrep -p "password = +$" /etc/security/passwd | grep ":" | awk -F: '{ print $1 } ' | \
while read user rest; do
    print "Locking account ${user} due to blank password"
    /usr/bin/chuser account_locked='true' expires=0101000070 ${user}
done
```

- The command should not yield output.
- Note: this is a partial remediation - setting the attribute `account_locked` - as it is too serious to leave unattended.

Remediation:




Check for accounts with an empty password field. If any, lock the account and assign an *impossible password hash*, as well as flag admin change (**ADMCHG**) to the password record.

```
set $(/usr/bin/egrep -c -p "password = +$" /etc/security/passwd)
if [[ $1 != "0" ]]; then
    # get seconds since epoch
    now=$(date +%s)
    # copy everything except entries without password
    /usr/bin/egrep -v -p "password = +$" /etc/security/passwd >
/etc/security/passwd.cis
    # create new entries with an impossible password hash and append to
password.cis
    /usr/bin/egrep -p "password = +$" /etc/security/passwd | grep ":" | awk -F:
'{ print $1 } ' | \
    while read user; do
        print "Locking and giving account ${user} impossible password hash"
        /usr/bin/chuser account_locked='true' expires=0101000070 ${user}
        printf "%s:\n\tpassword = *\n" ${user} >>
/etc/security/passwd.cis
        printf "\tflags = ADMCHG\n\tlastupdate=%s\n\n" ${now} >>
/etc/security/passwd.cis
    done
    cat /etc/security/passwd.cis > /etc/security/passwd
    rm /etc/security/passwd.cis
fi
```

Default Value:

N/A

CIS Controls:

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

5.1.3 All usernames and UIDs must be unique (Automated)

Profile Applicability:

- Level 1

Description:

All users should have a unique UID. In particular the only user on the system to have a UID of 0 should be the root user. Likewise, usernames need to be verified as unique.

Rationale:

The only user with a UID of 0 on the system must be the **root** account. Any account (username) with a UID of 0 has super user privileges on the system and becomes root at login.

Access to the root account should be via `su`, `sudo` or PKI fingerprint. Logging must include sufficient information such that each action taken with root authority can be accounted to a specific account.

All accounts (or users) must have a unique UID to ensure that file and directory security is not compromised.

Impact:

Identification is the basis of Access Control. What you can access is determined by who you are (uid), OR by a group you belong to (resource GID and your group list) OR access is permitted to all (i.e., your UID and group list) do not match the resource UID and GID values.

Audit:

Run the commands:

```
cut -d: -f 3 /etc/passwd | sort -n | uniq -d  
cut -d: -f 1 /etc/passwd | sort      | uniq -d
```

The commands should not yield output

Remediation:

- Examine the user IDs of all configured accounts:

```
cut -d: -f 3 /etc/passwd | sort -n | uniq -d
```

If a number, or numbers are returned from the command above, these are UID values which are not unique within the `/etc/passwd` file. Determine the effected accounts/s:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d | while read UID; do
  cut -f "1 3" -d : /etc/passwd | grep ":{UID}"
done
```

- Examine the usernames IDs of all configured accounts:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d
```

If a username, or usernames are returned from the command above, these are username values which are not unique within the `/etc/passwd` file. Determine the effected accounts/s:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d | while read username; do
  cut -f "1 3" -d : /etc/passwd | grep "${username}:"
done
```

NOTE: Any account names returned should either be deleted or have the UID changed
To remove:

```
rmuser <username>
```






To change the UID:

```
chuser id=<id> <username>
```

Default Value:

N/A

CIS Controls:

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

5.1.4 All group names and GIDs must be unique (Automated)

Profile Applicability:

- Level 1

Description:

All groups should have a unique GID on the system.

Rationale:

All groups should have an individual and unique GID. If GID numbers are shared this could lead to undesirable file and directory access.

Audit:

Run the commands:

```
cut -d: -f 3 /etc/group | sort -n | uniq -d  
cut -d: -f 1 /etc/group | sort      | uniq -d
```

The commands should not yield output

Remediation:

- Examine the *group IDs* (GID) of all locally configured accounts:

```
cut -d: -f 3 /etc/group | sort -n | uniq -d
```

If the command has output there is at least one duplicate GID number. Determine any duplicates within the `/etc/group` file:

```
cut -d: -f 1 /etc/group | sort -n | uniq -d | while read GID; do
  cut -f "1 3 4" -d : /etc/group | /usr/bin/sort -t: -k2n | grep ":{GID}:"
done
```

- Examine the *names* of all locally configured groups:

```
cut -d: -f 1 /etc/group | sort -n | uniq -d
```

If the command has output there is at least one duplicate group name. Determine any duplicates within the `/etc/group` file:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d | while read groupname; do
  cut -f "1 3 4" -d : /etc/group | /usr/bin/sort -t: -k2n | grep
"${groupname}:"
done
```

NOTE: Any duplicates returned should either be deleted or have the GID changed. Be careful. We recommend you examine any accounts assigned to a duplicate and ensure the account is neither losing nor gaining authorized group access through any remedial action.

To remove:

```
rmgroup <groupname>
```






To change the UID:

```
chgroup id=<id> <groupname>
```

Default Value:

N/A

CIS Controls:

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

5.1.5 Establish and Maintain an Inventory of Administrator accounts (Manual)

Profile Applicability:

- Level 1

Description:

AIX defines *Administrator* accounts with the attribute *admin*. When *true* the account is **Administrator** and when *false* the account is considered **User**.

Rationale:

An inventory of accounts with the attribute "*admin=true*" allows verification that all accounts considered *administrative* are so labeled by the system.

Impact:

The impact of '*admin=true*' is two-fold. a) a label for identifying accounts considered related to system administration b) providing additional controls for account management. On AIX, an account with the attribute '*admin=true*' requires a security role of *Senior Security Admin* to make modifications to the account attributes.

Audit:

Verify that there is, off system, an inventory of Administrative accounts and that the date is not more 13 weeks old.








Remediation:

A printable report can be prepared using the following example:

```
cnt=0
printf "%4s%68s\n" "AIX" "Administator Accounts"

lsuser -R files -a admin ALL | while read usr adm; do
if [[ ${adm} = "admin=true" ]] ; then
    printf "%12s" ${usr}
    let cnt=cnt+1
    [[ $(expr ${cnt} % 6) == 0 ]] && print
fi
done
[[ $(expr ${cnt} % 6) != 0 ]] && print
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.			

5.1.6 Establish and Maintain an Inventory of User Accounts (Manual)

Profile Applicability:

- Level 1

Description:

AIX defines *Administrator* accounts with the attribute *admin*. When *true* the account is **Administrator** and when *false* the account is considered **User**.

Rationale:

An inventory of accounts with the attribute "*admin=true*" allows verification that all accounts considered *administrative* are so labeled by the system.

Impact:

The impact of '*admin=true*' is two-fold. a) a label for identifying accounts considered related to system administration b) providing additional controls for account management. On AIX, an account with the attribute '*admin=true*' requires a security role of *Senior Security Admin* to make modifications to the account attributes.

Audit:

Verify that there is, off system, an inventory of User (not Administrative) accounts and that the date is not more 13 weeks old.




Remediation:

A printable report can be prepared using the following example:

```
cnt=0
printf "%4s%68s\n" "AIX" "User Accounts"

lsuser -R files -a admin ALL | while read usr adm; do
if [[ ${adm} = "admin=false" ]] ; then
    printf "%12s" ${usr}
    let cnt=cnt+1
    [[ $(expr ${cnt} % 6) == 0 ]] && print
fi
done
[[ $(expr ${cnt} % 6) != 0 ]] && print
```

CIS Controls:

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

5.2 Use Unique Passwords

This section provides guidance on the configuration of the user attributes that affect password policy and password creation. (See CIS Control 5.2: Use Unique Passwords)

Password policy attributes for password uniqueness include minimum length, reuse, and complexity.

How many recommendations?

AIX has nine individual *password attributes* that can be *tuned*. For each attribute a recommendation is expected. Nine (9) sounds like a lot of unique recommendations but you could also see the attributes as are 5 core attributes - and of these five, four have a min/max setting.

Defining policy based on nine recommendations, even with passwords of 14 characters, can complicate defining sufficient, yet usable password requirements. In other words define statements that provide sufficient protection from abuse yet give users some freedom of choice in creating strong, yet rememberable, passwords.

Remember: password attributes are not policy statements. They are the *knobs* that can be turned to implement a policy specification.

The challenge faced: which combination of attributes will satisfy a set of minimum requirements: *password length*, *number of different characters (including/excluding case)* each per characteristic: alpha, numeric, and other (so-called special).

Historically the core requirements has been based on setting minimums, e.g.,: *minlen*, *mindiff*, *maxrepeats*, *minalpha*, and *minother*. More recently additional *knobs* have been added to add further specification the characters *alpha* and *other*: *mindigit*, *minloweralpha*, *minupperalpha* and *minspecialchar*. This expansion was added in AIX 7.1 TL0 (and AIX 6.1 TL8). Remember: Historical recommendations are for the *core* attributes: **minlen**, **mindiff**, **maxrepeats**, **minalpha**, **minother**.

The four new attributes, according to the on-line manual - depend on, read modify, the historical attributes when certain conditions are met.

1. Rules for Alphabetic Characters (*minalpha*)
 - If minloweralpha > minalpha then minloweralpha=minalpha
 - If minupperalpha > minalpha then minupperalpha=minalpha
 - If minloweralpha + minupperalpha > minalpha; then
 - minupperalpha=minalpha – minloweralpha
2. Rules for Non-Alphabetic Characters (*minother*)
 - If mindigit > minother then mindigit=minother
 - If minspecialchar > minother then minspecialchar=minother
 - If minspecialchar + mindigit > minother then
 - minspecialchar = minother – mindigit

In effect this means *minalpha* and *minother* are still the leading attributes - but can be *fine-tuned*. **IMPORTANT:** to get your desired effect ensure *minalpha* \geq *minloweralpha* + *minupperalpha*, and *minother* \geq *mindigit* + *minspecialchar*.

Are there too many requirements?

No. The number of specific minimums: length, different characters, repeating characters, alphabetical, not-alphabetical has not changed. The introduction of the additional attributes merely allows more fine tuning on how these minimums are satisfied. **Note:** *mindiff* is superseded by *minalpha* + *minother*. In other words, if *mindiff*=4 together while *minalpha* and *minother* both set to 3 *mindiff*. effectively, is 6 (the sum of *minalpha* and *minother*).

The historical recommendations were: *minlen*=8 (now 14), *minalpha*=2, *minother*=2, *mindiff*=4 and *maxrepeats*=4. The recommendations do nothing to change these as the starting point. Whether any of the new attributes are required will depend on how policy is formulated. Perhaps the new attributes min(lower|upper|special|digit) are ignored. Our recommendation is to set *mindigit* to at least '1' (as a super-specification of *minother*).

The new minimum passing configuration includes: *minlen*=14, *mindiff*=6, *maxrepeats*=4, *minalpha*=3, *minother*=3. Further, we recommend that *minother* > *mindigit* \geq 1. The other super specifications: *minloweralpha*, *minupperalpha* and *minspecial* needs to have a value of 1 (the published recommendations have them all at 1). These settings ensure password uniqueness while leaving the selection of the *fine-tuning* character type to local preferences.

5.2.1 Ensure new passwords are controlled by password attributes (disable NOCHECK) (Automated)

Profile Applicability:

- Level 1

Description:

Ensure new passwords are *required* to pass password attribute controls.

Rationale:

Impact:

When exceptions to the defaults are required - rather than disable all password checking - an account needs to have the attribute redefined *per account*.

SHA512 password encryption is recommended as the most secure.

Audit:

Execute the following command:

```
grep NOCHECK /etc/security/passwd
```

The exit status should be 1 and there should not be any output.






Remediation:

In the file `/etc/security/passwd` clear the NOCHECK attribute from all users:

```
#!/usr/bin/ksh -e
# Copyright AIXTools, 2022

/usr/bin/grep -p NOCHECK /etc/security/passwd | /usr/bin/egrep ":$" | sed -e
's/:://' | while read USER; do
    /usr/bin/pwdadm -c $USER
done
```

CIS Controls:

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

5.2.2 *pwd_algorithm (Automated)*

Profile Applicability:

- Level 1

Description:

Defines the loadable password algorithm used when storing user passwords.

Rationale:

A development since AIX 5.1 was the ability to use different password algorithms as defined in `/etc/security/pwddalg.cfg`. The traditional UNIX password algorithm is `crypt`, which is a one-way hash function supporting only 8 character passwords. The use of brute force password guessing attacks means that `crypt` no longer provides an appropriate level of security and so other encryption mechanisms are recommended.

The recommendation of this benchmark is to set the password algorithm to `ssha512`. This algorithm supports long passwords, up to 255 characters in length and allows passphrases including the use of the extended ASCII table and the space character. Any passwords already set using `crypt` will be recognized. When the password is reset the new password hash algorithm will be used to encrypt the password.

Impact:

A password algorithm other than `crypt` is required to support a password *minlen* greater than 8 (eight) characters.

SHA512 password encryption is recommended as the most secure.

Audit:

Execute the following command:

```
#!/usr/bin/ksh -e
# chk_algorithm:5.2.1
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

EXPECT="usw pwd algorithm=ssha512"
CMD="lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm"

TST=${${CMD}}
[[ ${TST} == ${EXPECT} ]] && exit 0
print "%0: password hash algorithm is not ssha512"
exit 1
```

Remediation:

In the file `/etc/security/login.cfg` set the `usw` stanza attribute `pwd_algorithm` to `ssha512`:

```
#!/usr/bin/ksh -e
# chk_algorithm:5.2.1
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

EXPECT="usw pwd_algorithm=ssha512"
CMD="lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm"

TST=$(( ${CMD} ))
[[ ${TST} == ${EXPECT} ]] && exit 0

chsec -f /etc/security/login.cfg -s usw -a pwd_algorithm=ssha512
exit $?
```








Default Value:

`crypt`

Additional Information:

- Consider looking for passwords encrypted using `crypt` and set the `ADMCHG` flag to initiate a password change at next login.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.			

5.2.3 Ensure passwords are not hashed using 'crypt' (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to change the default password hash algorithm to `ssha512` (see paragraph 5.2.1). However, changing the default algorithm away from `crypt` is not enough. The user must supply a new password before a new hashed version of the password is stored in the *shadow* password file `/etc/security/passwd`.

Rationale:

The hash algorithm `crypt` is known by all *nix versions - so it has provided portability. And in the '70's processor power was weak enough that the mere 56 bits protection against brute-force attacks was reasonable to sufficient. Fifty (50) years later - this is not the case.

Impact:

The audit looks for hashed passwords that are 14 (fourteen) characters long. That is the length of the `crypt` hash. The remediation neither changes the password nor locks the account. However, it does clear (if present) and password flags (notably **NOCHECK** needs to be removed) and sets the flag **ADMCHG** so that the account will be required to reset their password during the next login.

Audit:

Use the following to find passwords using `crypt` hash method:

```
#!/usr/bin/ksh -e
# hash:5.2.2
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

grep 'password[[:blank:]]= .....$' /etc/security/passwd | \
while read pass equals cryptedhash; do
    user=$(grep -p $cryptedhash /etc/security/passwd | egrep '[a-zA-z0-9]+:$' |
sed -e s/:$//)
    print ${user}: needs to update passwd
done
```








Remediation:

Execute the following command to enable an administrative requirement to update password on next login - when current password is still *hashed* using the `crypt` algorithm.

```
#!/usr/bin/ksh -e
# hash_chk:5.2.12
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

#SystemAccounts are skipped, root is treated a regular account
#pconsole is no longer a system account - being deprecated/removed
SACTS1="(adm|bin|daemon|invscout|ipsec|lp|lpd|nobody|nuucp|sshd|sys|uucp)"
SACTS2="(esa|srvproxy|imnadm|anonymou|ftp)"
grep 'password[[:blank:]]*= .....$' /etc/security/passwd | \
while read pass equals cryptedhash; do
    user=$(/usr/bin/grep -p $cryptedhash /etc/security/passwd | \
        /usr/bin/egrep -vp "${SACTS1}:$" | \
        /usr/bin/egrep -vp "${SACTS2}:$" | \
        /usr/bin/egrep '[a-zA-z0-9]+:.$' | sed -e s/:$/ /)
    print ${user}: needs to update passwd
    set -x
    /usr/bin/pwdadm -c ${user}
    /usr/bin/pwdadm -f ADMCHG ${user}
    set +x
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.			

5.2.4 Ensure password policy is enforced for all users (Automated)

Profile Applicability:

- Level 1

Description:

If the `NOCHECK` flag is set on a user account it bypasses the password restrictions for that user.

Rationale:

If password restrictions are not enforced for some accounts, those accounts represent a much greater risk of being compromised by an attacker as they may have weaker passwords vulnerable to brute force attack or provide an indefinite window of opportunity for the use of already compromised credentials if the same password has been used on multiple systems.

Audit:

Execute the following command:

```
grep -p NOCHECK /etc/security/passwd
```

It should return no output

Remediation:

Obtain a list of any affected users:

```
grep -p NOCHECK /etc/security/passwd
```






Clear the `NOCHECK` flag from any account returned by executing the following command

```
pwdadm -c <USERNAME>
```

Set the `ADMCHG` flag from any account returned to force the user to change their password on next login

```
pwdadm -f ADMCHG <USERNAME>
```

CIS Controls:

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

5.2.5 minlen (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum length of a password.

Rationale:

In setting the `minlen` attribute, it ensures that passwords meet the required length criteria.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minlen
```

The above command should yield the following output:

```
default minlen=14
```

Remediation:

In `/etc/security/user`, set the default user stanza `minlen` attribute to be greater than or equal to 14:

```
chsec -f /etc/security/user -s default -a minlen=14
```






This means that all user passwords must be at least 14 characters in length.

NOTE: To support a password length greater than 8 characters the default algorithm must be changed. If the command above returns an error (3004-692 Error changing "minlen" to "14" : Value is invalid.) the recommendation [3.1.15 /etc/security/login.cfg - pwd algorithm](#) needs to be completed first.

Default Value:

default minlen=0

CIS Controls:

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

5.2.6 mindiff (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of characters that are required in a new password which were not in the old password.

Rationale:

The `mindiff` attribute ensures that users are not able to reuse the same or similar passwords.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a mindiff
```

The above command should yield the following output:

```
default mindiff=4
```

Remediation:

In `/etc/security/user`, set the default user stanza `mindiff` attribute to be greater than or equal to 4:






```
chsec -f /etc/security/user -s default -a mindiff=4
```

This means that when a user password is set it needs to comprise of at least 4 characters not present in the previous password.

Default Value:

```
mindiff=0
```

CIS Controls:

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

5.2.7 minalpha (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of alphabetic characters in a password.

Rationale:

In setting the `minalpha` attribute, it ensures that passwords have a minimum number of alphabetic characters.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minalpha
```

The above command should yield the following output:

```
default minalpha=3
```

Remediation:

In `/etc/security/user`, set the default user stanza `minalpha` attribute to be greater than or equal to 3:






```
chsec -f /etc/security/user -s default -a minalpha=3
```

This means that there must be at least 3 alphabetic characters (upper or lowercase) within a password.

Default Value:

`minalpha=0`

CIS Controls:

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

5.2.8 minother (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of characters within a password which must be non-alphabetic.

Rationale:

In setting the `minother` attribute, it increases password complexity by enforcing the use of non-alphabetic characters in every user password.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minother
```

The above command should yield the following output:

```
default minother=3
```

Remediation:

In `/etc/security/user`, set the default user stanza `minother` attribute to be greater than or equal to 3:






```
chsec -f /etc/security/user -s default -a minother=3
```

This means that there must be at least 3 non-alphabetic characters within a password.

Default Value:

default minother=0

CIS Controls:

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

5.2.9 maxrepeats (Automated)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of times a character may appear in a password.

Rationale:

In setting the `maxrepeats` attribute, it enforces a maximum number of character repeats within a password.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxrepeats
```

The above command should yield the following output:

```
default maxrepeats=4
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxrepeats` attribute to 2:

```
chsec -f /etc/security/user -s default -a maxrepeats=4
```






This means that a user may not use the same character more than four (4) times in a password.

This value has been increased from two (2) - in parallel with the increase in `minlen` from eight (8) to fourteen (14).

Default Value:

```
maxrepeats=8
```

CIS Controls:

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

5.2.10 mindigit (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of digits in a password.

Rationale:

In setting the `mindigit` attribute, the password must contain a digit when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a mindigit
```

The above command should yield the following output:

```
default mindigit=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `mindigit` attribute to 1:






```
chsec -f /etc/security/user -s default -a mindigit=1
```

This means that there must be at least 1 digit within a password.

Default Value:

default mindigit=0

CIS Controls:

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

5.2.11 minloweralpha (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of lower case alphabetic characters in a password.

Rationale:

In setting the `minloweralpha` attribute, the password must contain a lower case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minloweralpha
```

The above command should yield the following output:

```
default minloweralpha=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minloweralpha` attribute to 1:






```
chsec -f /etc/security/user -s default -a minloweralpha=1
```

This means that there must be at least 1 lower case alphabetic character within a password.

Default Value:

default minloweralpha=0

CIS Controls:

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

5.2.12 minupperalpha (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of upper case alphabetic characters in a password.

Rationale:

In setting the `minupperalpha` attribute, the password must contain an upper case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minupperalpha
```

The above command should yield the following output:

```
default minupperalpha=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minupperalpha` attribute to 1:






```
chsec -f /etc/security/user -s default -a minupperalpha=1
```

This means that there must be at least 1 upper case alphabetic character within a password.

Default Value:

default minupperalpha=0

CIS Controls:

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

5.2.13 minspecialchar (Automated)

Profile Applicability:

- Level 1

Description:

Defines the minimum number of special characters in a password.

Rationale:

In setting the `minspecialchar` attribute, the password must contain a special character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a minspecialchar
```

The above command should yield the following output:

```
default minspecialchar=1
```

Remediation:

In `/etc/security/user`, set the default user stanza `minspecialchar` attribute to 1:






```
chsec -f /etc/security/user -s default -a minspecialchar=1
```

This means that there must be at least 1 special character within a password.

Default Value:

default minspecialchar=0

CIS Controls:

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

5.3 System Accounts

- This section deals with managing (preferred: disable any command-line activity) the generic system accounts i.e. `daemon`, `bin`, `sys`, `adm`, `uucp`, `nobody` and `lpd`.
- Disable is defined as setting attribute `account_locked=true`, `rlogin=false`, `login=false`, `shell=/bin/false` and `sugroups=bin` (as there are no normal accounts with `bin` as a group).
- These accounts exist to own certain files and/or perform a service as a non-root (less privileged) userid. As such, the accounts are NOT to be removed (and files transferred to `root`).

Motivation:

- There is no reason that these userid's have any access to a shell - whether through a login or `su(do)`.
- There is no need for an encrypted password in the shadow file. Better is to leave the shadow password as the single character `'*`' as that will never resolve to a normal password - effectively blocking `login` and `su` operations.
- Not even `su` as `root` needs to succeed.

Exception:

- There should not be a requirement to log in as any of these users directly. However, if a need does arise access should be regulated via the `sudoers` attribute (document the group creation and assignment) so that the legitimate user may `su` from there own account to ensure traceability and accountability. This also implies that a real encrypted (as sha512) password will exist in the shadow password file.

5.3.1 adm (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `adm` user account.

Rationale:

This change disables direct local and remote login to the `adm` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `adm` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `adm` user:

```
lsuser -a account_locked login rlogin adm
```

The above command should yield the following output:

```
adm account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `adm` user:

```
chuser account_locked=true login=false rlogin=false adm
```

Default Value:

`account_locked=false rlogin=true login=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.2 bin (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `bin` user account.

Rationale:

This change disables direct local and remote login to the `bin` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `bin` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `bin` user:

```
lsuser -a account_locked login rlogin bin
```

The above command should yield the following output:

```
bin account_locked=true login=false rlogin=false
```

Remediation:




Change the login and remote login user flags to disable `bin` user access:

```
chuser account_locked=true login=false rlogin=false bin
```

Default Value:

`account_locked=false rlogin=true login=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.3 daemon (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `daemon` user account.

Rationale:

This change disables direct local and remote login to the `daemon` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `daemon` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `daemon` user:

```
lsuser -a account_locked login rlogin daemon
```

The above command should yield the following output:

```
daemon account_locked=true login=false rlogin=false
```

Remediation:




Change the login and remote login user flags to disable `daemon` user access:

```
chuser account_locked=true login=false rlogin=false daemon
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.4 *guest (Automated)*

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `guest` user account.

Rationale:

This change disables direct local and remote login to the `guest` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `guest` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Impact:

Historically the `guest` user account was to provide access to unknown users, i.e., the user identity was not important.

Today the `guest` account should not be used. The numeric userid is reserved by the OS.

All authorized users should be given specific logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `guest` user:

```
lsuser -a account_locked login rlogin guest
```

The above command should yield the following output:

```
guest account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `guest` user:

```
chuser account_locked=true login=false rlogin=false adm
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.5 lpd (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `lpd` user account.

Rationale:

This change disables direct local and remote login to the `lpd` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `lpd` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the `lpd` user:

```
lsuser -a account_locked login rlogin lpd
```

The above command should yield the following output:

```
lpd account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `lpd` user:

```
chuser account_locked=true login=false rlogin=false lpd
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.6 nobody (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `nobody` user account.

Rationale:

This change disables direct local and remote login to the `nobody` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `nobody` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `nobody` user:

```
lsuser -a account_locked login rlogin nobody
```

The above command should yield the following output:

```
nobody account_locked=true login=false rlogin=false
```

Remediation:




Change the login and remote login user flags to disable `nobody` user access:

```
chuser account_locked=true login=false rlogin=false nobody
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.7 nuucp (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `nuucp` user account.

Rationale:

This change disables direct local and remote login to the `nuucp` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `nuucp` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `nuucp` user:

```
lsuser -a account_locked login rlogin nuucp
```

The above command should yield the following output:

```
nuucp account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `nuucp` user::

```
chuser account_locked=true login=false rlogin=false nuucp
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.8 sys (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `sys` user account.

Rationale:

This change disables direct local and remote login to the `sys` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `sys` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `sys` user:

```
lsuser -a account_locked login rlogin sys
```

The above command should yield the following output:

```
sys account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `sys` user:

```
chuser account_locked=true login=false rlogin=false sys
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.9 uucp (Automated)

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the `uucp` user account.

Rationale:

This change disables direct local and remote login to the `uucp` user account. Do not set a password on this account to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as the `uucp` user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the `uucp` user:

```
lsuser -a account_locked login rlogin uucp
```

The above command should yield the following output:

```
uucp account_locked=true login=false rlogin=false
```

Remediation:




Change the following user attributes to `uucp` user:

```
chuser account_locked=true login=false rlogin=false uucp
```

Default Value:

`account_locked=false login=true rlogin=true`

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.10 Ensure System Accounts cannot access system using ftp. (Automated)

Profile Applicability:

- Level 1

Description:

If ftp is active on the system, the file `/etc/ftpusers` is a deny list used by `ftp` daemon containing a list of users who are not allowed to access the system via `ftp`.

Rationale:

The `/etc/ftpusers` file contains a list of users who are not allowed to access the system via `ftp`. All users with a UID less than 200 should typically be added into the file.

Audit:

If `ftp` is active on the system, review the content of `/etc/ftpusers` and ensure there are no duplicate entries:

```
cat /etc/ftpusers
```

Remediation:

List all users with a UID less than 200 to the `/etc/ftpusers` file:

```
lsuser -c ALL | grep -v ^#name |grep -v root | cut -f1 -d: | while read NAME;
do
if [ `lsuser -f $NAME | grep id | cut -f2 -d= ` -lt 200 ] > /dev/null 2>&1;
then
echo "Would add $NAME to /etc/ftpusers"
fi
done
```

NOTE: Review the list of users

Add all relevant users with a UID of less than 200 to the `/etc/ftpusers` file:

```
lsuser -c ALL | grep -v ^#name |grep -v root | cut -f1 -d: | while read NAME;
do
if [ `lsuser -f $NAME | grep id | cut -f2 -d= ` -lt 200 ] > /dev/null 2>&1;
then
echo $NAME >> /etc/ftpusers
fi
done
```

Default Value:

N/A




Additional Information:

Reversion:

Edit `/etc/ftpusers` and leave only the `root` entry:

```
vi /etc/ftpusers
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.4 User Attributes for Active Processes

Other attributes manage user/application settings for active processes. These attributes include `ulimits`, `umask`. Including password controls - there are approximately 65 user attributes.

The recommendations in this section focus on the parameters of the default user stanza in the file `/etc/security/user`. The values set are only applicable if specific values are not defined during the creation of a user.

The recommended user management is to not set any of these values explicitly - unless there is a specific requirement to override a default.

5.5 Disable Dormant Accounts

Some attributes that previously were associated with *Unique Passwords* are actually attributes to automate disabling dormant accounts.

The attributes do not control the passwords. Instead they require an active account to create a new password, OR - be considered dormant and disabled. These attributes focus on how long a password is valid, when it should be changed, and disables an account when it not changed.

Other settings here, traditionally, have been characterized as "secure configuration of enterprise assets". We believe they fit better under the heading of automated "Disable Dormant Accounts"

5.6 maxage (Automated)

Profile Applicability:

- Level 1

Description:

Defines the maximum number of weeks that a password is valid.

Rationale:

The `maxage` attribute enforces regular password changes. We recommend this to be 13 or less, but not 0 which disables this setting.

Impact:

Historically, this recommendation has been to set `maxage=13`. In recent years several communities (e.g., Windows, DoD) have concluded that too frequent forced password changes leads to both weaker passwords and weaker/bad password discipline.

An initial proposal to increase the maxage to 52 is not unanimous within the AIX community - so the recommendation, for now, remains at 13.

Local Policy may decide to follow the *other* communities and set this value as 52.

Due to this lack of consensus this control is being set at Level 2.

The value chosen by an organization is to maintain overall password quality and secrecy.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxage
```

The above command should yield the following output:

```
default maxage=13
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxage` attribute to a number greater than 0 but less than or equal to 13:




```
chsec -f /etc/security/user -s default -a maxage=13
```

This means that a user password must be changed 13 weeks after being set. If 0 is set then this effectively disables password ageing.

Default Value:

`maxage=0`

CIS Controls:

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

5.7 maxexpired (Automated)

Profile Applicability:

- Level 1

Description:

Defines the number of weeks after `maxage`, that a password can be reset by the user.

Rationale:

The `maxexpired` attribute limits the number of weeks after password expiry that a password may be changed by the user.

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s default -a maxexpired
```

The above command should yield the following output:

```
default maxexpired=4
```

Remediation:

In `/etc/security/user`, set the default user stanza `maxexpired` attribute to 4:




```
chsec -f /etc/security/user -s default -a maxexpired=4
```

This means that a user can reset their password up to 4 weeks after it has expired. After this an administrative user would need to reset the password.

Default Value:

No limit

CIS Controls:

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

6 Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

See [Control v8: Access Control Management](#)

Why Is This Control Critical?

Where CIS Control 5 (Account Management) deals specifically with account identification, authentication and status (active or dormant), CIS Control 6 (Access Control Management) focuses on managing what access these identities have, ensuring identities (processes or users) only have access to the data or enterprise assets appropriate for their role. Identities should only have the minimal authorization, i.e., access, needed for the role.

Defining roles, developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Access Control in AIX environment

Most AIX servers are used in a commercial environment and rely on classic UNIX File System DAC (discretionary access control) mechanisms based on the effective UID and list of GID's a process is associated with. Every object a process accesses using system calls `open()`, `read()`, and `write()` (and others) is determined by the UID/GID of the inode and the mode or permission bits associated with it. If the object UID and the EUID are equal then only the permission bits associated with the UID are relevant. If `UID != EUID` and `GID ==` one of the associated GIDs the the group bits are relevant. If neither are true then either the "other" permissions are valid, or an ACL (access control list) may be valid, or an enhanced RBAC setting may permit access. **Note:** a *deny* ACL supersedes file system DAC and/or enhanced RBAC permissions.

6.1 Legacy RBAC mechanisms

Starting with AIX release 4.2 (anno 1996) the concept of "role-based" accounts was introduced into AIX systems management.

The principles of **legacy** AIX RBAC is: group membership, rolename, and adjustments to programs to verify both group and role membership. While role membership could be considered mandatory, group membership might be a temporary privilege promotion using the standard mechanism of SGID (set Group ID).

A role-based program would require belonging to a specific group to even be executable. Further, during it's initialization it would verify role membership - and if that was passed would either perform it's function without further privilege elevation or it would call another program with SUID (set UID), usually to root, that was able to access nay missing privileges.

Form a baseline

The recommendations here are not scored. Instead, they are here to assist with forming a baseline of programs (executable) that affect privilege escalation.

6.1.1 Create baseline of executables that elevate to a different GUID (Not scored) (Manual)

Profile Applicability:

- Level 2

Description:

Access Control can be managed by a judicious arrangement of file system DAC controls. Legacy AIX Role based management relies on careful assignment of "Other" to group escalation, followed by Group membership to EUID for the remaining privilege requirement - where the object owner (or super-user access) is able to access any resources needed to complete a task or function.

Rationale:

The baseline is to have a point that can be used to verify system integrity - the file system DAC permissions are "as installed" by OEM.

Should you make local changes to OEM, be sure to create a second list to verify the desired settings (and perhaps verify a specific delta).

Impact:

An example:

```
# find / -fstype jfs2 -type f ! -size 0 -perm -g+s ! -perm -u+s -perm -o+x -
ls | awk '{ print $6, $5, $3, $11 }' | sort
adm bin -r-xr-sr-x /usr/bin/timex
cron bin -r-xr-sr-x /usr/bin/atq
printq bin -r-xr-sr-x /usr/bin/splp
printq bin -r-xr-sr-x /usr/lib/lpd/piobe
printq root -r-xr-sr-x /usr/lib/lpd/pio/etc/piomkapqd
security root -r-xr-sr-x /usr/bin/chfn
security root -r-xr-sr-x /usr/bin/chgrpmm
security root -r-xr-sr-x /usr/bin/chsh
security root -r-xr-sr-x /usr/bin/smitacl
security root -r-xr-sr-x /usr/sbin/lsgroup
system bin -r-xr-sr-x /usr/bin/ps
system bin -r-xr-sr-x /usr/sbin/killall
system root -r-xr-sr-x /usr/bin/lssrc
system root -r-xr-sr-x /usr/bin/uptime
system root -r-xr-sr-x /usr/bin/w
```

Audit:

Remediation:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6 <u>Access Control Management</u> Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.			
v7	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

6.1.2 Create baseline of executables that require a specific group for elevation to a different EUID (not scored) (Manual)

Profile Applicability:

- Level 2

Description:

Access Control can be managed by a judicious arrangement of file system DAC controls. Legacy AIX Role based management relies on careful assignment of "Other" to group escalation, followed by Group membership to EUID for the remaining privilege requirement - where the object owner (or super-user access) is able to access any resources needed to complete a task or function.

Rationale:

The baseline is to have a point that can be used to verify system integrity - the file system DAC permissions are "as installed" by OEM.

Should you make local changes to OEM, be sure to create a second list to verify the desired settings (and perhaps verify a specific delta).

Impact:

An example:

```
# find / -fstype jfs2 -type f ! -size 0 ! -perm -o+x -perm -u+s -ls | awk '{
print $6, $5, $3, $11 }' | sort
adm root -r-sr-s--- /usr/bin/acctctl
adm root -r-sr-s--- /usr/bin/accttras
adm root -r-sr-x--- /sbin/helpers/jfs2/diskusg
adm root -r-sr-x--- /usr/lib/sa/sadc
adm root -r-sr-x--- /usr/lpp/bos/inst_root/sbin/helpers/jfs2/diskusg
adm root -r-sr-x--- /usr/sbin/acct/accton
adm root -r-sr-x--- /usr/sbin/diskusg
adm root -r-sr-xr-- /usr/sbin/perf/diag_tool/getschedparms
adm root -r-sr-xr-- /usr/sbin/perf/diag_tool/getvmparms
audit root -r-sr-x--- /usr/sbin/audit
audit root -r-sr-x--- /usr/sbin/auditbin
audit root -r-sr-x--- /usr/sbin/auditcat
audit root -r-sr-x--- /usr/sbin/auditconv
audit root -r-sr-x--- /usr/sbin/auditmerge
audit root -r-sr-x--- /usr/sbin/auditpr
audit root -r-sr-x--- /usr/sbin/auditselect
audit root -r-sr-x--- /usr/sbin/auditstream
audit root -r-sr-x--- /usr/sbin/watch
cron root -r-s--S--- /usr/sbin/cron
printq root -r-sr-s--- /usr/bin/chque
printq root -r-sr-s--- /usr/bin/chquedev
printq root -r-sr-s--- /usr/bin/mkque
printq root -r-sr-s--- /usr/bin/mkquedev
printq root -r-sr-s--- /usr/bin/rmque
printq root -r-sr-s--- /usr/bin/rmquedev
printq root -r-sr-s--- /usr/sbin/lpd
printq root -r-sr-s--- /usr/sbin/qdaemon
printq root -r-sr-x--- /usr/lib/lpd/digest
printq root -r-sr-x--- /usr/lib/lpd/pio/etc/piomkpq
printq root -r-sr-x--- /usr/lib/lpd/rembak
security root -r-sr-x--- /usr/bin/chgroup
security root -r-sr-x--- /usr/bin/chrole
security root -r-sr-x--- /usr/bin/chsec
security root -r-sr-x--- /usr/bin/chuser
security root -r-sr-x--- /usr/bin/lssec
security root -r-sr-x--- /usr/bin/mkgroup
security root -r-sr-x--- /usr/bin/mkrole
security root -r-sr-x--- /usr/bin/mkuser
security root -r-sr-x--- /usr/bin/pwdck
security root -r-sr-x--- /usr/bin/sysck
security root -r-sr-x--- /usr/bin/tcbck
security root -r-sr-x--- /usr/bin/usrck
security root -r-sr-x--- /usr/sbin/chtcb
security root -r-sr-x--- /usr/sbin/grpck
security root -r-sr-x--- /usr/sbin/mkpasswd
security root -r-sr-x--- /usr/sbin/rmgroup
security root -r-sr-x--- /usr/sbin/rmrole
security root -r-sr-x--- /usr/sbin/rmuser
shutdown root -r-sr-x--- /usr/sbin/exec shutdown
shutdown root -r-sr-x--- /usr/sbin/fastboot
shutdown root -r-sr-x--- /usr/sbin/reboot
snapp root -r-sr-x--- /usr/sbin/snappd
system root -r-sr-s--- /usr/lib/semutil
system root -r-sr-s--- /usr/sbin/srcd
system root -r-sr-s--- /usr/sbin/srcmstr
```

```

system root -r-sr-x--- /usr/bin/filemon
system root -r-sr-x--- /usr/bin/fileplace
system root -r-sr-x--- /usr/bin/fileplacej2
system root -r-sr-x--- /usr/bin/netpmon
system root -r-sr-x--- /usr/lpp/diagnostics/bin/Dctrl
system root -r-sr-x--- /usr/lpp/diagnostics/bin/diagTasksWebSM
system root -r-sr-x--- /usr/lpp/diagnostics/bin/diagela_exec
system root -r-sr-x--- /usr/lpp/diagnostics/bin/diaggetrto
system root -r-sr-x--- /usr/lpp/diagnostics/bin/diagrto
system root -r-sr-x--- /usr/lpp/diagnostics/bin/diagsetrto
system root -r-sr-x--- /usr/lpp/diagnostics/bin/uesensor
system root -r-sr-x--- /usr/lpp/diagnostics/bin/update_flash
system root -r-sr-x--- /usr/lpp/diagnostics/bin/update_manage_flash
system root -r-sr-x--- /usr/lpp/diagnostics/bin/uspchrp
system root -r-sr-x--- /usr/lpp/diagnostics/bin/usysfault
system root -r-sr-x--- /usr/lpp/diagnostics/bin/usysident
system root -r-sr-x--- /usr/lpp/diagnostics/bin/utape
system root -r-sr-x--- /usr/sbin/allocp
system root -r-sr-x--- /usr/sbin/cfgmgr
system root -r-sr-x--- /usr/sbin/chcod
system root -r-sr-x--- /usr/sbin/chcons
system root -r-sr-x--- /usr/sbin/chdev
system root -r-sr-x--- /usr/sbin/chpath
system root -r-sr-x--- /usr/sbin/devinstall
system root -r-sr-x--- /usr/sbin/diag_exec
system root -r-sr-x--- /usr/sbin/extendvg
system root -r-sr-x--- /usr/sbin/getlvcb
system root -r-sr-x--- /usr/sbin/getlvname
system root -r-sr-x--- /usr/sbin/getvgname
system root -r-sr-x--- /usr/sbin/gsclvmd
system root -r-sr-x--- /usr/sbin/invscoutd
system root -r-sr-x--- /usr/sbin/ipl_varyon
system root -r-sr-x--- /usr/sbin/lchangelv
system root -r-sr-x--- /usr/sbin/lchangevp
system root -r-sr-x--- /usr/sbin/lchangevg
system root -r-sr-x--- /usr/sbin/lchlvcopy
system root -r-sr-x--- /usr/sbin/lcreatelv
system root -r-sr-x--- /usr/sbin/ldeletelv
system root -r-sr-x--- /usr/sbin/ldeletepv
system root -r-sr-x--- /usr/sbin/lextendlv
system root -r-sr-x--- /usr/sbin/lmigratelv
system root -r-sr-x--- /usr/sbin/lmigratepp
system root -r-sr-x--- /usr/sbin/lreducelv
system root -r-sr-x--- /usr/sbin/lresynclp
system root -r-sr-x--- /usr/sbin/lresynclv
system root -r-sr-x--- /usr/sbin/lvaryoffvg
system root -r-sr-x--- /usr/sbin/lvaryonvg
system root -r-sr-x--- /usr/sbin/lvgenmajor
system root -r-sr-x--- /usr/sbin/lvgenminor
system root -r-sr-x--- /usr/sbin/lvrelmajor
system root -r-sr-x--- /usr/sbin/lvrelminor
system root -r-sr-x--- /usr/sbin/mkdev
system root -r-sr-x--- /usr/sbin/mklvcopy
system root -r-sr-x--- /usr/sbin/mkpath
system root -r-sr-x--- /usr/sbin/mkvg
system root -r-sr-x--- /usr/sbin/pdelay
system root -r-sr-x--- /usr/sbin/pdisable

```

```

system root -r-sr-x--- /usr/sbin/penable
system root -r-sr-x--- /usr/sbin/phold
system root -r-sr-x--- /usr/sbin/pshare
system root -r-sr-x--- /usr/sbin/pstart
system root -r-sr-x--- /usr/sbin/putlvcb
system root -r-sr-x--- /usr/sbin/putlvodm
system root -r-sr-x--- /usr/sbin/redefinevg
system root -r-sr-x--- /usr/sbin/rmdev
system root -r-sr-x--- /usr/sbin/rmpath
system root -r-sr-x--- /usr/sbin/swap
system root -r-sr-x--- /usr/sbin/swapoff
system root -r-sr-x--- /usr/sbin/swapon
system root -r-sr-x--- /usr/sbin/swcons
system root -r-sr-x--- /usr/sbin/switch.prt
system root -r-sr-x--- /usr/sbin/synclvodm
system root -r-sr-x--- /usr/sbin/tellclvmd
system root -r-sr-x--- /usr/sbin/uucpd
system root -r-sr-x--- /usr/sbin/varyonvg
system root -r-sr-xr-- /usr/sbin/inetd
system root -r-sr-xr-- /usr/sbin/krlogind
system root -r-sr-xr-- /usr/sbin/krshd
system root -r-sr-xr-- /usr/sbin/named9
system root -r-sr-xr-- /usr/sbin/route
system root -r-sr-xr-- /usr/sbin/rwhod
system root -r-sr-xr-- /usr/sbin/talkd

```

Audit:

Remediation:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6 <u>Access Control Management</u> Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.			
v7	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

6.1.3 Create baseline of executables that elevate directly to a new EUID (not scored) (Manual)

Profile Applicability:

- Level 2

Description:

Access Control can be managed by a judicious arrangement of file system DAC controls. Legacy AIX Role based management relies on careful assignment of "Other" to group escalation, followed by Group membership to EUID for the remaining privilege requirement - where the object owner (or super-user access) is able to access any resources needed to complete a task or function.

Rationale:

The baseline is to have a point that can be used to verify system integrity - the file system DAC permissions are "as installed" by OEM.

Should you make local changes to OEM, be sure to create a second list to verify the desired settings (and perhaps verify a specific delta).

Impact:

An example:

```
# find / -fstype jfs2 -type f ! -size 0 -perm -u+s -perm -o+x -ls | awk '{
print $6, $5, $3, $11 }' | sort
audit root -r-sr-xr-x /usr/sbin/lsaudit
bin root -r-sr-xr-x /usr/bin/getconf
bin root -r-sr-xr-x /usr/bin/iostat
bin root -r-sr-xr-x /usr/bin/ipcs
bin root -r-sr-xr-x /usr/bin/mesg
bin root -r-sr-xr-x /usr/bin/rdist
bin root -r-sr-xr-x /usr/bin/rexec
bin root -r-sr-xr-x /usr/bin/rlogin
bin root -r-sr-xr-x /usr/bin/vmstat
bin root -r-sr-xr-x /usr/lib/mh/slocal
bin root -r-sr-xr-x /usr/sbin/arp.atm
bin root -r-sr-xr-x /usr/sbin/atmstat
bin root -r-sr-xr-x /usr/sbin/atmstat.batm
bin root -r-sr-xr-x /usr/sbin/atmstat.chrm
bin root -r-sr-xr-x /usr/sbin/atmsvcd
bin root -r-sr-xr-x /usr/sbin/atmvcstat
bin root -r-sr-xr-x /usr/sbin/entstat
bin root -r-sr-xr-x /usr/sbin/entstat.bent
bin root -r-sr-xr-x /usr/sbin/entstat.ethchan
bin root -r-sr-xr-x /usr/sbin/entstat.goent
bin root -r-sr-xr-x /usr/sbin/entstat.gxent
bin root -r-sr-xr-x /usr/sbin/entstat.hea
bin root -r-sr-xr-x /usr/sbin/entstat.kngent
bin root -r-sr-xr-x /usr/sbin/entstat.ment
bin root -r-sr-xr-x /usr/sbin/entstat.phxent
bin root -r-sr-xr-x /usr/sbin/entstat.scent
bin root -r-sr-xr-x /usr/sbin/entstat.vent
bin root -r-sr-xr-x /usr/sbin/entstat.vioent
bin root -r-sr-xr-x /usr/sbin/entstat.vnic
bin root -r-sr-xr-x /usr/sbin/fcstat
bin root -r-sr-xr-x /usr/sbin/hdlcstat
bin root -r-sr-xr-x /usr/sbin/ibstat
bin root -r-sr-xr-x /usr/sbin/muxatmd
bin root -r-sr-xr-x /usr/sbin/netstat
bin root -r-sr-xr-x /usr/sbin/quota
bin root -r-sr-xr-x /usr/sbin/repquota
bin root -r-sr-xr-x /usr/sbin/rmssock
bin root -r-sr-xr-x /usr/sbin/rnicstat
bin root -r-sr-xr-x /usr/sbin/rsct/bin/ctstrtcasd
bin root -r-sr-xr-x /usr/sbin/rsct/bin/nlssrc_c
bin root -r-sr-xr-x /usr/sbin/tokstat
bin root -r-sr-xr-x /usr/sbin/tokstat.cstok
cron root -r-sr-sr-x /usr/bin/at
cron root -r-sr-sr-x /usr/bin/crontab
mail root -r-sr-sr-x /usr/bin/bellmail
printq root -r-sr-sr-x /usr/bin/enq
printq root -r-sr-sr-x /usr/lib/lpd/pio/etc/piodmgrsu
printq root -r-sr-xr-x /usr/lib/lpd/pio/etc/pioout
security root -r-sr-xr-x /usr/bin/chcore
security root -r-sr-xr-x /usr/bin/lscore
security root -r-sr-xr-x /usr/bin/newgrp
security root -r-sr-xr-x /usr/bin/pagdel
security root -r-sr-xr-x /usr/bin/paginit
security root -r-sr-xr-x /usr/bin/paglist
security root -r-sr-xr-x /usr/bin/passwd
```

```
security root -r-sr-xr-x /usr/bin/pwddadm
security root -r-sr-xr-x /usr/bin/setgroups
security root -r-sr-xr-x /usr/bin/setsend
security root -r-sr-xr-x /usr/bin/shell
security root -r-sr-xr-x /usr/bin/su
security root -r-sr-xr-x /usr/bin/yppasswd
security root -r-sr-xr-x /usr/sbin/getty
security root -r-sr-xr-x /usr/sbin/login
security root -r-sr-xr-x /usr/sbin/luser
security root -r-sr-xr-x /usr/sbin/tsm
sys root -r-sr-xr-x /usr/bin/errpt
sys root -r-sr-xr-x /usr/lib/trcload
system root -r-sr-s--x /usr/sbin/mailq
system root -r-sr-s--x /usr/sbin/newaliases
system root -r-sr-s--x /usr/sbin/sendmail
system root -r-sr-s--x /usr/sbin/sendmail_nonssl
system root -r-sr-s--x /usr/sbin/sendmail_ssl
system root -r-sr-sr-x /usr/bin/confsrc
system root -r-sr-sr-x /usr/sbin/lresource
system root -r-sr-xr-x /opt/IBMinvscout/bin/invscoutClient_PartitionID
system root -r-sr-xr-x /opt/IBMinvscout/bin/invscoutClient_VPD_Survey
system root -r-sr-xr-x /sbin/helpers/jfs2/backbyinode
system root -r-sr-xr-x /sbin/helpers/jfs2/restbyinode
system root -r-sr-xr-x /usr/bin/capture
system root -r-sr-xr-x /usr/bin/chkey
system root -r-sr-xr-x /usr/bin/ftp
system root -r-sr-xr-x /usr/bin/logout
system root -r-sr-xr-x /usr/bin/rcp
system root -r-sr-xr-x /usr/bin/remsh
system root -r-sr-xr-x /usr/bin/rm_mlcachefile
system root -r-sr-xr-x /usr/bin/rsh
system root -r-sr-xr-x /usr/bin/ruptime
system root -r-sr-xr-x /usr/bin/rwho
system root -r-sr-xr-x /usr/bin/script
system root -r-sr-xr-x /usr/bin/telnet
system root -r-sr-xr-x /usr/bin/tftp
system root -r-sr-xr-x /usr/bin/tn
system root -r-sr-xr-x /usr/bin/tn3270
system root -r-sr-xr-x /usr/bin/traceroute
system root -r-sr-xr-x /usr/bin/utftp
system root -r-sr-xr-x /usr/lib/boot/tftp
system root -r-sr-xr-x /usr/lpp/X11/bin/msmitpasswd
system root -r-sr-xr-x /usr/lpp/bos/inst_root/sbin/helpers/jfs2/backbyinode
system root -r-sr-xr-x /usr/lpp/bos/inst_root/sbin/helpers/jfs2/restbyinode
system root -r-sr-xr-x /usr/lpp/diagnostics/bin/diagrpt
system root -r-sr-xr-x /usr/sbin/arp
system root -r-sr-xr-x /usr/sbin/arp.ib
system root -r-sr-xr-x /usr/sbin/backbyinode
system root -r-sr-xr-x /usr/sbin/fdformat
system root -r-sr-xr-x /usr/sbin/format
system root -r-sr-xr-x /usr/sbin/frcactrl
system root -r-sr-xr-x /usr/sbin/fuser
system root -r-sr-xr-x /usr/sbin/invscout
system root -r-sr-xr-x /usr/sbin/keyenvoy
system root -r-sr-xr-x /usr/sbin/lparsetres
system root -r-sr-xr-x /usr/sbin/lquerylv
system root -r-sr-xr-x /usr/sbin/lquerypv
```

```

system root -r-sr-xr-x /usr/sbin/lqueryvg
system root -r-sr-xr-x /usr/sbin/lqueryvgs
system root -r-sr-xr-x /usr/sbin/lscfg
system root -r-sr-xr-x /usr/sbin/lscons
system root -r-sr-xr-x /usr/sbin/lslv
system root -r-sr-xr-x /usr/sbin/lsmcode
system root -r-sr-xr-x /usr/sbin/lspath
system root -r-sr-xr-x /usr/sbin/lspv
system root -r-sr-xr-x /usr/sbin/lsrset
system root -r-sr-xr-x /usr/sbin/lsslot
system root -r-sr-xr-x /usr/sbin/lsvg
system root -r-sr-xr-x /usr/sbin/lsvgfs
system root -r-sr-xr-x /usr/sbin/mknod
system root -r-sr-xr-x /usr/sbin/mount
system root -r-sr-xr-x /usr/sbin/mtrace
system root -r-sr-xr-x /usr/sbin/ndp
system root -r-sr-xr-x /usr/sbin/nfsstat
system root -r-sr-xr-x /usr/sbin/ping
system root -r-sr-xr-x /usr/sbin/portmir
system root -r-sr-xr-x /usr/sbin/restbyinode
system root -r-sr-xr-x /usr/sbin/sliplogin
system root -r-sr-xr-x /usr/sbin/timedc
system root -r-sr-xr-x /usr/sbin/umount
system root -r-sr-xr-x /usr/sbin/unmount
system root -rwsr-xr-x /usr/lib/perf/libperfstat_updt_dictionary
system root -rwsr-xr-x /usr/lpp/X11/Xamples/bin/xload
system root -rwsr-xr-x /usr/lpp/X11/bin/aixterm
system root -rwsr-xr-x /usr/lpp/X11/bin/xlock
system root -rwsr-xr-x /usr/lpp/X11/bin/xterm
uucp uucp -r-sr-xr-x /usr/bin/cu
uucp uucp -r-sr-xr-x /usr/bin/uucp
uucp uucp -r-sr-xr-x /usr/bin/uuname
uucp uucp -r-sr-xr-x /usr/bin/uuq
uucp uucp -r-sr-xr-x /usr/bin/uusnap
uucp uucp -r-sr-xr-x /usr/bin/uustat
uucp uucp -r-sr-xr-x /usr/bin/uux
uucp uucp -r-sr-xr-x /usr/sbin/uucp/uucico
uucp uucp -r-sr-xr-x /usr/sbin/uucp/uusched
uucp uucp -r-sr-xr-x /usr/sbin/uucp/uuxqt

```

Audit:

Remediation:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6 <u>Access Control Management</u> Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.			
v7	4 <u>Controlled Use of Administrative Privileges</u> Controlled Use of Administrative Privileges			

6.2 RBAC managed privilege escalation

This section covers AIX enhanced RBAC (hereafter just RBAC, legacy-RBAC will be used, as needed to discuss the RBAC system built into AIX 4.2)

6.2.1 Privilege escalation: enhanced RBAC (Manual)

Profile Applicability:

- Level 2

Description:

The recommendation is to configure RBAC to reflect the privileged command access requirements for all users of the system. RBAC is a default component of AIX 7.1.

Rationale:

Privileged command access should be limited to and defined by a user's individual needs. Access to a root command prompt should be limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

The choice between sudo and enhanced RBAC revolves around whether or not the environment is heterogeneous in nature, running different flavors of UNIX, or perhaps different versions of AIX. It may be that sudo is the standard tool of choice for managing privileged command access across an entire UNIX estate. However, if the environment is AIX 6.1+ only, it is recommended that enhanced RBAC is used as the tool of choice. Some implementations however may benefit from a combined approach, utilizing both sudo and enhanced RBAC.

Audit:

N/A

Remediation:

Enhanced RBAC improves on its legacy implementation by allowing greater flexibility around command lists and authorization definitions, which can be customized. The definitions are also saved to a kernel table rather than in flat files, which improves security.

The implementation of RBAC is role based, allowing users to be specifically granted access to the privileged commands they need to perform their day to day tasks. The tool can be used to replace sudo in many instances, or indeed to work alongside it.

A successful implementation may also allow the root account to be deprecated.

The RBAC definition files:

```
/etc/security/privcmds  
/etc/security/privfiles  
/etc/security/privdevs
```

The command used to list the active RBAC definitions, i.e. those loaded into the kernel:

```
lskst
```

The command used to update RBAC definitions in the kernel table:

```
setkst
```

Further details regarding planning and implementation of RBAC can be found within the IBM AIX 7.1 Infocentre:

<https://www.ibm.com/docs/en/aix/7.1?topic=control-aix-rbac>

NOTE: The configuration of enhanced RBAC is completely dependent on the unique requirements of a given environment.

Default Value:

N/A

References:

1. <https://www.ibm.com/docs/en/aix/7.1?topic=control-aix-rbac>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

6.3 SUDO managed privilege escalation

SUDO is one technology to manage privilege escalation by letting users "RUNAS" (usually RUNAS as root) another userid - basically giving them all the privileges associated by that EUID (effective User ID).

6.3.1 Privilege escalation: sudo (Manual)

Profile Applicability:

- Level 2

Description:

The recommendation is to install and configure `sudo`, to reflect the privileged command access requirements of all users of the system.

Rationale:

Privileged command access should be limited to and defined by a user's individual needs. Access to a root command prompt should be limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

The choice between `sudo` and enhanced RBAC revolves around whether or not the environment is heterogeneous in nature, running different flavors of UNIX, or perhaps different versions of AIX. It may be that `sudo` is the standard tool of choice for managing privileged command access across an entire UNIX estate. However, if the environment is AIX 6.1+ only, it is recommended that enhanced RBAC is used as the tool of choice. Some implementations however may benefit from a combined approach, utilizing both `sudo` and enhanced RBAC.

Audit:

Validate the `sudo` installation:

```
sudo --version
```

The above command should yield similar output:

```
sudo version <version> (<version> should be the latest version for the sudo
distribution installed on your system. This should be version 1.9.5p2 or
later)
```

NOTE: The version reflected above may differ from the one installed.

Remediation:

Install the latest available version for the `sudo` distribution installed on your system. This version should be 1.9.5p2 or later.

Default Value:

Not installed

Additional Information:

Once installed refer to the sudo man page for information regarding the creation of a custom `/etc/sudoers` file. It is recommended that, to reduce rule complexity, privileges are assigned at a group level wherever possible:

<http://www.gratisoft.us/sudo/man/sudo.html>

NOTE: The configuration of sudo is completely dependent on the unique requirements of a given environment.

All editing of the `/etc/sudoers` file must be performed by the following command:

```
visudo
```




Once the `/etc/sudoers` file has been successfully created, validate the syntax of the file:

```
visudo -c
```

Reversion:

De-install the sudo software:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

6.3.2 Ensure sudo logging is active (Manual)

Profile Applicability:

- Level 2

Description:

All commands executed via `sudo` should be logged to either syslog (default) or a dedicated log file

Note: 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 or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Rationale:

Logging of commands executed via `sudo` enables auditing of those commands

Audit:

Verify that `syslog_badpri` and `syslog_goodpri` are not set to `none`

Run the following commands:

```
# grep -Ei '^\s*Defaults\s+syslog_badpri=\S+' /etc/sudoers /etc/sudoers.d/*
# grep -Ei '^\s*Defaults\s+syslog_goodpri=\S+' /etc/sudoers /etc/sudoers.d/*
```

No output should be returned

-OR-

Verify that sudo has a custom log file configured

Run the following command:

```
# grep -Ei '^\s*Defaults\s+logfile=\S+' /etc/sudoers /etc/sudoers.d/*
```


Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo -f <PATH TO FILE>`
Remove the any lines which are found containing

```
syslog_badpri=none
```

or

```
syslog_goodpri=none
```

-OR-

If you do not want to log sudo commands to syslog, to use as sudo specific log file add the following line:

```
Defaults logfile="<PATH TO CUSTOM LOG FILE>"
```




Example:

```
Defaults logfile="/var/log/sudo.log"
```

Default Value:

All options are unset by default

CIS Controls:

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

6.3.3 Ensure sudo commands use pty (Manual)

Profile Applicability:

- Level 2

Description:

sudo can be configured to run only from a pseudo-pty

Note: 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 or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Rationale:

Attackers can run a malicious program using sudo, which would again fork a background process that remains even when the main program has finished executing.

Audit:

Verify that sudo can only run other commands from a pseudo-pty

Run the following command:



```
# grep -Ei '^\\s*Defaults\\s+([\\^#]+,\\s*)?use_pty(,\\s+\\S+\\s*)*(\\s+#.*)?\\$' /etc/sudoers /etc/sudoers.d/*
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `visudo -f <PATH TO FILE>` and add the following line:

```
Defaults use_pty
```

CIS Controls:

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

6.4 Adding authorized users in *at.allow* (Manual)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/at.allow` file defines which users on the system are able to schedule jobs via `at`.

Rationale:

The `/var/adm/cron/at.allow` file defines which users are able to schedule jobs via `at`. Review the current `at` files and add any relevant users to the `/var/adm/cron/at.allow` file.

Audit:

Review the content `/var/adm/cron/at.allow`, ensure that the content reflects the changes made:

```
cat /var/adm/cron/at.allow
```

Remediation:

Review the current `at` files:

```
ls -l /var/spool/cron/atjobs
cat /var/spool/cron/atjobs/*
```

NOTE: Review the list of `at` schedules and remove any files which should not be there, or have no content

Add the recommended system users to the `at.allow` list:

```
echo "adm" >> /var/adm/cron/at.allow
echo "sys" >> /var/adm/cron/at.allow
```

Add any other users who require permissions to use the `at` scheduler:




```
echo <user> >> /var/adm/cron/at.allow
```

NOTE: Where `<user>` is the username.

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

6.5 Services - at access is root only (Automated)

Profile Applicability:

- Level 2

Description:

This change creates an `at.allow` file with a root user entry and removes the `at.deny` file, if it exists.

Rationale:

This ensures that only the root user has the ability to schedule jobs through the `at` command. A hacker may exploit use of `at` to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

Audit:

From the command prompt, execute the following command:

```
ls /var/adm/cron/at.deny
```

The above command should yield the following output:

```
ls: 0653-341 The file /var/adm/cron/at.deny does not exist
```

From the command prompt, execute the following command:

```
cat /var/adm/cron/at.allow
```

The above command should yield the following output:

```
root
```

Remediation:



Create the `/var/adm/cron/at.allow` file and remove `/var/adm/cron/at.deny` (if it exists):

```
echo "root" > /var/adm/cron/at.allow  
rm /var/adm/cron/at.deny
```

Default Value:

N/A

CIS Controls:

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

6.6 Adding authorised users in cron.allow (Automated)

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/cron.allow` file defines which users on the system are able to schedule jobs via `cron`.

Rationale:

The `/var/adm/cron/cron.allow` file defines which users are able to schedule jobs via `cron`. Review the current `cron` files and add any relevant users to the `/var/adm/cron/cron.allow` file.

Audit:

Review the content `/var/adm/cron/cron.allow`, ensure that the content reflects the changes made:

```
cat /var/adm/cron/cron.allow
```

Remediation:

Review the current `cron` files:

```
ls -l /var/spool/cron/crontabs/  
cat /var/spool/cron/crontabs/*
```

NOTE: Review the list of `cron` schedules and remove any files which should not be there, or have no content.

Add the recommended system users to the `cron.allow` list:

```
echo "sys" >> /var/adm/cron/cron.allow  
echo "adm" >> /var/adm/cron/cron.allow
```

Add any other users who require permissions to use the `cron` scheduler:




```
echo <user> >> /var/adm/cron/cron.allow
```

NOTE: Where `<user>` is the username.

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			

6.7 Services - crontab access is root only (Automated)

Profile Applicability:

- Level 2

Description:

This change creates a `cron.allow` file with a root user entry and removes the `cron.deny` file, if it exists.

Rationale:

This ensures that only the root user has the ability to create a crontab. A hacker may exploit use of the crontab to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

Audit:

From the command prompt, execute the following command:

```
ls /var/adm/cron/cron.deny
```

The above command should yield the following output:

```
ls: 0653-341 The file /var/adm/cron/cron.deny does not exist.
```

From the command prompt, execute the following command:

```
cat /var/adm/cron/cron.allow
```

The above command should yield the following output:

```
root
adm
```

Additional users may be present per site policy if they require the use of `cron`

Remediation:

Create the `/var/adm/cron/cron.allow` file and remove `/var/adm/cron/cron.deny` (if it exists):

```
print "root\nadm" > /var/adm/cron/cron.allow
rm /var/adm/cron/cron.deny
```

Default Value:

N/A

CIS Controls:

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

7 Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is this Control critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

7.1 Use FLRT regularly (Manual)

Profile Applicability:

- Level 2

Description:

FLRT (Fix Level Recommendation Tool) provides upgrade recommendations for software and firmware, providing custom reports for each system.

Rationale:

The Fix Level Recommendation Tool (FLRT) provides cross-product compatibility information and fix recommendations for IBM products. Use FLRT to plan upgrades of key components or to **verify the current health of a system**.

Audit:

Remediation:

Default Value:

Not installed

Additional Information:







To take advantage of the FLRT scripting capabilities, use an HTTP retrieval program, such as wget, to query FLRT for the recommended software levels for your machine.

Make sure your machine has network access to
<http://www14.software.ibm.com/webapp/set2/flrt/query>.

Write a script to query FLRT by reading the FLRT scripting documentation listed below. Or, start with one of the sample ksh scripts provided on this page.

The scripts provided are sample scripts only. You must create your own script based on your environment. If you want to use one of the script samples as a starting point, please modify it to suit the needs of your machine. Comment out sections for software that is not running on your machine. Place your script in a directory where execution will have write authority so that it can create temporary files for processing.

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.			

7.2 Use FLRTVC regularly (Automated)

Profile Applicability:

- Level 1

Description:

The Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) provides security and HIPER (High Impact PERvasive) reports based on the inventory of your system.

Rationale:

Audit:

Remediation:

To download, click the download link below and save to a folder. It is packaged as a ZIP file with the FLRTVC.ksh script and LICENSE.txt file.





Download: FLRTVC (v0.8.1)

Note: The script requires ksh93 to use. If you are receiving errors when running the script, you may execute the script using "ksh93 flrtvc.ksh". As of v0.7, only non-fixed vulnerabilities will be shown by default. Use -a to show all.

Default Value:

Not installed

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v7	<u>3.1 Run Automated Vulnerability Scanning Tools</u> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			

8 Audit Log Management

CIS Control

8.1 Syslog

This section will detail the recommendations regarding the configuration of syslog. By default the information sent to `syslogd` is not logged and important and pertinent information, such as failed switch user and login attempts are not recorded. The type of data which can be captured through this mechanism can be used for real-time and retrospective analysis, and is particularly useful for monitoring access to the system.

Logging data, via `syslogd`, may also provide unequivocal evidence against any individual or organization that successfully breach, or attempt to circumvent the security access controls surrounding a system.

Note:

- This section describes standard AIX `syslogd`. There is no *requirement* to use AIX syslog. In other words this section should be read that a `syslogd` is properly configured and minimally covers the recommendations listed. Some known alternative syslogd packages include *syslog-ng*, *rsyslogd* and *corelog*.
- If you use a different syslog it is your responsibility to modify commands used to audit and remediate the recommendation.

8.1.1 Configuring syslog - local logging (Manual)

Profile Applicability:

- Level 1

Description:

This recommendation implements a local `syslog` configuration.

Rationale:

Establishing a logging process via `syslog` provides system and security administrators with pertinent information relating to: login, mail, daemon, user and kernel activity. The recommendation is to enable local `syslog` logging, with a weekly rotation policy in a four weekly cycle. The log rotation isolates historical data which can be reviewed retrospectively if an issue is uncovered at a later date.

Impact:

This recommendation is `manual` because there are likely local requirements that surpass the basic recommendation here.

Audit:

- Ensure that the log entries have been added successfully:

```
/usr/bin/egrep -v "^(^$)|(^#)" /etc/syslog.conf
```

- The above command should yield the output similar to:

```
aso.notice /var/log/aso/aso.log rotate size 1m files 8 compress
aso.info /var/log/aso/aso_process.log rotate size 1m files 8 compress
aso.debug /var/log/aso/aso_debug.log rotate size 32m files 8 compress
*.info;local4.none /var/log/syslog/info.log files 52 rotate time 1w
compress archive /var/log/syslog/archive
auth.info /var/log/syslog/auth.log files 52 rotate time 1w
compress archive /var/log/syslog/archive
```

- Check that the `auth.log` and `info.log` files and `syslog archive` directory exist:

```
ls -ld /var/log/syslog/auth.log /var/log/syslog/info.log
/var/log/syslog/archive
```

The output of the command above should list both files and the directory

Remediation:

Explicitly define a log file for the `auth.info` output in `/etc/syslog.conf`:

```
printf "auth.info\t\t/var/adm/authlog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately
Create the `authlog` file and make it readable by root only:

```
touch /var/adm/authlog
chown root:system /var/adm/authlog
chmod u=rw,go= /var/adm/authlog
```

Create an entry in `/etc/syslog.conf` to capture all other output of level info or higher, excluding authentication information, as this is to be captured within `/var/adm/authlog`:

```
printf "*.info;auth.none\t/var/adm/syslog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

Create the `syslog` file:

```
touch /var/adm/syslog
chmod u=rw,g=r,o= /var/adm/syslog
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

Default Value:

Not configured

Additional Information:

Reversion:

Edit `/etc/syslog.conf` and remove the `authlog` and `syslog` entries:

```
vi /etc/syslog.conf
```

Remove:

```
auth.info          /var/adm/authlog rotate time 1w files 4
*.info;auth.none   /var/adm/syslog rotate time 1w files 4
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

Delete the `authlog` and `syslog` files:

```
rm /var/adm/authlog /var/adm/syslog
```

8.1.2 Configuring syslog - remote logging (Automated)

Profile Applicability:

- Level 2

Description:

This recommendation implements a remote `syslog` configuration.

Rationale:

To further enhance the local `syslog` logging process CIS recommends that `syslog` information, in particular that generated by the `auth` facility, is logged remotely. This recommendation assumes that a remote and secure syslog server is available on the network. If this is not the case, please skip to the next recommendation.

The primary reason for logging remotely is to provide an un-editable audit trail of system access. If a hacker were to access a system and gain super user authority it would be easy to edit local files and remove all traces of access, providing the system administrator with no way of identifying the individual or group responsible. If the log data is sent remotely at the point of access, these remote logs can then be reconciled with local data to identify tampered and altered files. The logs can also be used as evidence in any subsequent prosecution.

Audit:

Ensure that the log entries have been added successfully:

```
tail -2 /etc/syslog.conf
```

The above command should yield the following output:

```
auth.info          @<IP address of remote syslog server>
*.info;auth.none   @<IP address of remote syslog server>
```

Remediation:

Explicitly define a remote host for auth.info data in `/etc/syslog.conf` (enter the remote host IP address in the example below):

```
printf "auth.info\t\t@<IP address of remote syslog server>" >>  
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately
Create a remote host entry in `/etc/syslog.conf` to capture all other output of level info or higher (enter the remote host IP address in the example below):

```
printf "/*.info;auth.none\t@<IP address of remote syslog server>\n" >>  
/etc/syslog.conf
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

Default Value:

Not configured

Additional Information:

IBM POWER Systems can supply an additional security mechanism named `Trusted Logging` in it's PowerSC package.

This product writes logs to storage on a VIOS (Virtual I/O Server) without any need for an active/open IP path.

Since it is an additional product - we consider using `Trusted Logging` as Level 2, IG2 whereas remote syslog may be considered Level 1.

8.1.3 Configuring syslog - remote messages (Automated)

Profile Applicability:

- Level 2

Description:

This recommendation prevents the local `syslogd` daemon from accepting messages from other hosts on the network.

Rationale:

Apart from a central `syslog` server, all other hosts should not accept remote `syslog` messages. By default the `syslogd` daemon accepts all remote `syslog` messages as no authentication is required. This means that a hacker could flood a server with `syslog` messages and potentially fill up the `/var` filesystem.

Audit:

Ensure that daemon is running with the newly updated configuration:

```
ps -ef |grep "syslogd"
```

The above command should yield output similar to the following:

```
root  57758  70094  0 10:22:08  -  0:00 /usr/sbin/syslogd -r
```

NOTE: The `-r` flag should be present at the end out of the output.

Remediation:

If the server does not act as a central `syslog` server, suppress the logging of messages originating from remote servers:

```
chssys -s syslogd -a "-r"
```

Re-cycle `syslogd` to activate the configuration change:

```
stopsrc -s syslogd  
startsrc -s syslogd
```

Default Value:

Not configured

Additional Information:

Reversion:

Remove the suppression of remote `syslog` messages:

```
chssys -s syslogd -a ""
```

Re-cycle `syslogd` to activate the configuration change:

```
stopsrc -s syslogd  
startsrc -s syslogd
```

8.2 AIX Auditing (Manual)

Profile Applicability:

- Level 2

Description:

This recommendation configures AIX auditing in bin mode.

Rationale:

AIX auditing provides a framework within which to capture pertinent system and security related information, such as failed login attempts, cron usage etc. It is recommended that auditing is enabled as part of a group of measures designed to provide enhanced logging of system and security changes. Further information regarding the setup and management of AIX accounting and auditing can be found in the redbook [Accounting and Auditing for AIX 5L](#)

Audit:

- Ensure that the `/audit` filesystem has been created and mounted:

```
lsfs /audit || print "Audit Filesystem is missing"
```

The command should not yield any output:

NOTE: Failed output will look something like this:

```
lsfs: 0506-915 No record matching /audit was found in /etc/filesystems.  
Audit Filesystem is missing
```

- Validate the configuration in the `/etc/security/audit/config` file. This should match the changes made in the remediation section:

```
cat /etc/security/audit/config
```

- Ensure that the `/usr/lib/security/mkuser.default` `auditclasses` entry has been updated:

```
lssec -f /usr/lib/security/mkuser.default -s user -a auditclasses
```

The above command should yield the following output:

```
user auditclasses=general, SRC, cron, tcpip
```

- Ensure that the `cron` audit rotation script has been implemented:

```
crontab -l |grep "cronaudit"
```

The above command should yield the following output:

```
0 * * * * /etc/security/aixpert/bin/cronaudit
```

- Ensure that the audit startup line has been added into `/etc/inittab`:

```
lsitab audit
```

This should return:

```
audit:2:boot:audit start > /dev/console 2>&1 # Start audit
```


Remediation:

Configure AIX auditing in-line with the High Level AIX Security Expert policy.
Create a /audit filesystem, at least 100 MB in size:

```
mklv -y <LV name> -t jfs2 -u 1 -c 1 rootvg 1 hdisk0
crfs -v jfs2 -d auditlv -m /audit -A yes -t no
mount /audit
```

Reflect the following configuration in the /etc/security/audit/config file:

```
vi /etc/security/audit/config
```

Add in:

```
start:
    binmode = on
    streammode = off
bin:
    trail = /audit/trail
    bin1 = /audit/bin1
    bin2 = /audit/bin2
    binsize = 10240
    cmds = /etc/security/audit/bincmds
```

Add the auditing entries for root and all other users below the pre-defined audit classes:

```
users:
    root = general, SRC, mail, cron, tcpip, ipsec, lvm
    <user 1> = general, SRC, cron, tcpip
    <user 2> = general, SRC, cron, tcpip
    etc.
```

Update the /usr/lib/security/mkuser.default auditclasses entry to ensure that auditing is set up for any newly created users:

```
chsec -f /usr/lib/security/mkuser.default -s user -a
auditclasses=general, SRC, cron, tcpip
```

A cron job is implemented to monitor the free space in /audit, running hourly, to ensure that /audit does not fill up. If /audit is greater than 90% used, /audit/trail is moved to /audit/trailOneLevelBack:

```
crontab -e
```

Add in:

```
0 * * * * /etc/security/aixpert/bin/cronaudit
```

NOTE: The implementation of a script to suit internal security policy is recommended to further enhance the log rotation process.

Add the audit startup command into /etc/inittab:

```
mkitab "audit:2:boot:audit start > /dev/console 2>&1 # Start audit"
```

Default Value:

Auditing not enabled

References:

1. Accounting and Auditing for AIX 5L:
<http://www.redbooks.ibm.com/redbooks/pdfs/sg246396.pdf>

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Benchmark Organization		
1.1	Benchmark Principles, Conventions and Assumptions		
1.2	HOWTO use this benchmark		
1.3	AIX - Installation methods		
1.3.1	AIX RTE Installation		
1.3.2	AIX Secure Profile Installation (Basic AIX Security - BAS)		
1.3.3	AIX MKSYSB Installation		
1.4	AIX Patch Management		
1.5	Summary		
2	Inventory and Control of Assets		
2.1	Collect system configuration regularly (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Allowlist Authorized Software and Report Violations (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Allowlist Authorized Libraries and Report Violations (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Allowlist Authorized Scripts and Report Violations (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Enforce Allowlist aka Trusted Execution Checks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.8	Ensure the Trusted Execution Policies cannot be modified (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3	Data Protection		
3.1	Encryption: File System Level (EFS) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Encryption: Logical Volume (ELV) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Application Data with requirement for world writable directories (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure all files and directories are owned by a user (uid) and assigned to a group (gid) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4	Secure Configuration of Enterprise Assets and Software		
4.1	System Boot		
4.1.1	Boot phase: /etc/inittab		
4.1.1.1	Disable writesrv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Disable ntalk/talk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	dt (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	piobe (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	qdaemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.1.6	rc.nfs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	cas_agent (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Boot phase: /etc/rc.tcpip: daemons		
4.1.2.1	inetd - aka Super Daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	aixmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	dhcpcd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	dhcprd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	dhcpsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	dpid2 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	gated (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	hostmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	mrouted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	named (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	portmap (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.12	routed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.13	rwhod (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.14	sendmail (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.15	snmpd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.16	snmpmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.17	timed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Boot phase: IPv6		
4.1.3.1	autoconf6 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.3.2	ndpd-host (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	NFS		
4.1.4.1	NFS - de-install NFS client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.2	NFS - de-install NFS server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.3	NFS - enable both nosuid and nodev options on NFS client mounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.4	NFS - localhost removal (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.5	NFS - restrict NFS access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.6	NFS - no_root_squash option (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.7	NFS - secure NFS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Inetd Services		
4.1.5.1	bootps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.2	chargen (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.3	comsat (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.4	daytime (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.5	discard (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.6	echo (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.7	exec (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.8	finger (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.9	ftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.10	imap2 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.5.11	instsrv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.12	klogin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.13	kshell (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.14	login (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.15	netstat (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.16	ntalk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.17	pcnfsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.18	pop3 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.19	rexed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.20	rquotad (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.21	rstatd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.22	rusersd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.23	rwalld (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.24	shell (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.25	sprayd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.26	xmquery (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.27	talk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.28	telnet (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.29	tftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.30	time (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.31	uucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2	Network Options: '/usr/sbin/no'		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2.1	clean_partial_conns (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	bcastping (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	directed_broadcast (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	icmpaddressmask (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	ipforwarding (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	ipignoreredirects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	ipsendredirects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	ipsrouteforward (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	ipsrouterecv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	ipsrouteseend (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.11	ip6srouteforward (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.12	nfs_use_reserved_ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.13	nonlocsrcroute (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.14	sockthresh (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.15	tcp_pmtu_discover (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.16	tcp_tcpsecure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.17	udp_pmtu_discover (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.18	ip6forwarding (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3	Implement and Manage a Firewall (bos.net.ipsec)		
4.3.1	Ensure that IP Security is available (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure loopback traffic is blocked on external interfaces (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.3	Ensure that IPsec filters are active (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4	Remove or Disable Weak/Defunct Network Services		
4.4.1	NIS		
4.4.1.1	NIS - de-install NIS client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.2	NIS - de-install NIS server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.3	NIS - remove NIS markers from password and group files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.4	NIS - restrict NIS server communication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.2	Remote command lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.3	Removal of entries from /etc/hosts.equiv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.4	Removal of .rhosts and .netrc files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.5	Remote daemon lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5	Standard Services and Applications		
4.5.1	Common Desktop Environment (CDE)		
4.5.1.1	CDE - de-installing CDE (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.2	/etc/inetd.conf - cmsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.3	CDE - disabling dtlogin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.4	/etc/inetd.conf - dtspc (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.5	CDE - sgid/suid binary lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.6	CDE - remote GUI login disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.7	CDE - screensaver lock (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.8	CDE - login screen hostname masking (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.1.9	CDE - /etc/dt/config/Xconfig permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.10	CDE - /etc/dt/config/Xservers permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.11	CDE - /etc/dt/config/*/Xresources permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2	FTPD		
4.5.2.1	FTPD: Disable root access to ftpd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.2	FTPD: Display acceptable usage policy during login (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.3	FTPD: Prevent world access and group write to files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3	OpenSSH		
4.5.3.1	OpenSSH: Minimum version is 8.1 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.2	OpenSSH: Remove /etc/shosts.equiv and /etc/rhosts.equiv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.3	OpenSSH: Remove .shosts files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -l INFO' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s). (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4	Sendmail Configuration		
4.5.4.1	/etc/mail/sendmail.cf - Hide sendmail version information (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.2	/etc/mail/sendmail.cf - PrivacyOptions (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.3	/etc/mail/sendmail.cf - DaemonPortOptions (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.4	/etc/mail/sendmail.cf - access control (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.5	/var/spool/clientmqueue - access control (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.6	/var/spool/mqueue - access control (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5	SNMP Configuration		
4.5.5.1	SNMP - disable private community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.5.2	SNMP - disable system community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.3	SNMP - disable public community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.4	SNMP - disable Readwrite community access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.5	SNMP - restrict community access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.6	Uninstall snmp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.7	Uninstall/Disable sendmail (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6	Login Controls		
4.6.1	/etc/security/login.cfg - logintimeout (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.2	/etc/security/login.cfg - logindelay (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.3	herald (logon message) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.4	loginretries (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7	Trusted Files and Directories		
4.7.1	Trusted Directories		
4.7.1.1	Home directory must exist (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.7.1.6	/var/adm/ras (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2	Trusted Files		
4.7.2.1	New configuration file for sendmail /etc/mail/submit.cf (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.3	crontab entries - owned by userid (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.12	/var/adm/cron/at.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.7.2.13	/var/adm/cron/cron.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.8	Trusted Execution (TE)		
4.8.1	TE - implementation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5	Account Management		
5.1	Establish and Maintain an Inventory of Accounts		
5.1.1	Maintain Account Passwords		
5.1.1.1	histexpire (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.2	histsize (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.3	minage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	All accounts must have a hashed password (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.3	All usernames and UIDs must be unique (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Establish and Maintain an Inventory of User Accounts (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	Use Unique Passwords		
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	minloweralpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3	System Accounts		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3.1	adm (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	bin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	guest (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	lpd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	nobody (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	nuucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	sys (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	uucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.3.10	Ensure System Accounts cannot access system using ftp. (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	User Attributes for Active Processes		
5.5	Disable Dormant Accounts		
5.6	maxage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.7	maxexpired (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6	Access Control Management		
6.1	Legacy RBAC mechanisms		
6.1.1	Create baseline of executables that elevate to a different GUID (Not scored) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.2	Create baseline of executables that require a specific group for elevation to a different EUID (not scored) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.1.3	Create baseline of executables that elevate directly to a new EUID (not scored) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2	RBAC managed privilege escalation		
6.2.1	Privilege escalation: enhanced RBAC (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	SUDO managed privilege escalation		
6.3.1	Privilege escalation: sudo (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure sudo logging is active (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure sudo commands use pty (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Adding authorized users in at.allow (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Services - at access is root only (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Adding authorised users in cron.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Services - crontab access is root only (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7	Continuous Vulnerability Management		
7.1	Use FLRT regularly (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Use FLRTVC regularly (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8	Audit Log Management		
8.1	Syslog		
8.1.1	Configuring syslog - local logging (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
8.1.2	Configuring syslog - remote logging (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	Configuring syslog - remote messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.2	AIX Auditing (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.1	CDE - de-installing CDE	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist)	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Disable writesrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Disable ntalk/talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	dt	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	piobe	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	qdaemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.6	rc.nfs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	cas_agent	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	inetd - aka Super Daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	aixmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	dhcpcd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	dhcprd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	dhcpsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	dpid2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	gated	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	hostmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	mrouted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	named	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.2.11	portmap	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.12	routed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.13	rwhod	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.14	sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.15	snmpd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.16	snmpmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.17	timed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.1	autoconf6	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.2	ndpd-host	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.1	bootps	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.2	chargen	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.3	comsat	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.1	CDE - de-installing CDE	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.1	OpenSSH: Minimum version is 8.1	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed"	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -l INFO'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s).	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.1	New configuration file for sendmail /etc/mail/submit.cf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	All usernames and UIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt'	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	minloweralpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Use FLRTVC regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Allowlist Authorized Software and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Allowlist Authorized Libraries and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Allowlist Authorized Scripts and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Enforce Allowlist aka Trusted Execution Checks	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Encryption: File System Level (EFS)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Encryption: Logical Volume (ELV)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Disable writesrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Disable ntalk/talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	dt	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	piobe	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	qdaemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.6	rc.nfs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	cas_agent	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	inetd - aka Super Daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	aixmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	dhcpcd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	dhcprd	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.2.5	dhcpcsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	dpid2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	gated	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	hostmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	mrouted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	named	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	portmap	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.12	routed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.13	rwhod	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.14	sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.15	snmpd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.16	snmpmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.17	timed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.1	autoconf6	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.2	ndpd-host	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.1	bootps	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.2	chargen	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.3	comsat	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.1	CDE - de-installing CDE	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.1	OpenSSH: Minimum version is 8.1	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed"	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -I INFO'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s).	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.1	New configuration file for sendmail /etc/mail/submit.cf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	All usernames and UIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt'	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2.11	minloweralpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Use FLRTVC regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.8	Ensure the Trusted Execution Policies cannot be modified	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Application Data with requirement for world writable directories	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure all files and directories are owned by a user (uid) and assigned to a group (gid)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.1	NFS - de-install NFS client	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.2	NFS - de-install NFS server	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.3	NFS - enable both nosuid and nodev options on NFS client mounts	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.4	NFS - localhost removal	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.5	NFS - restrict NFS access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.6	NFS - no_root_squash option	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.7	NFS - secure NFS	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.4	daytime	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.5	discard	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.6	echo	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.7	exec	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.8	finger	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.9	ftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.10	imap2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.11	instsrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.12	klogin	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.13	kshell	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.14	login	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.15	netstat	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.16	ntalk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.17	pcnfsd	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.5.18	pop3	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.19	rexed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.20	rquotad	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.21	rstatd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.22	rusersd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.23	rwalld	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.24	shell	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.25	sprayd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.26	xmquery	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.27	talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.28	telnet	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.29	tftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.30	time	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.31	uucp	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	clean_partial_conns	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	bcastping	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	directed_broadcast	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	icmpaddressmask	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	ipforwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	ipignoreredirects	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	ipsendredirects	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	ipsrouteforward	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	ipsrouterecv	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	ipsrouteseed	<input type="checkbox"/>	<input type="checkbox"/>
4.2.11	ip6srouteforward	<input type="checkbox"/>	<input type="checkbox"/>
4.2.12	nfs_use_reserved_ports	<input type="checkbox"/>	<input type="checkbox"/>
4.2.13	nonlocsrcroute	<input type="checkbox"/>	<input type="checkbox"/>
4.2.14	sockthresh	<input type="checkbox"/>	<input type="checkbox"/>
4.2.15	tcp_pmtu_discover	<input type="checkbox"/>	<input type="checkbox"/>
4.2.16	tcp_tcpsecure	<input type="checkbox"/>	<input type="checkbox"/>
4.2.17	udp_pmtu_discover	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.2.18	ip6forwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	Ensure that IP Security is available	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure loopback traffic is blocked on external interfaces	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3	Ensure that IPsec filters are active	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.1	NIS - de-install NIS client	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.2	NIS - de-install NIS server	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.3	NIS - remove NIS markers from password and group files	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.4	NIS - restrict NIS server communication	<input type="checkbox"/>	<input type="checkbox"/>
4.4.2	Remote command lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.4.3	Removal of entries from /etc/hosts.equiv	<input type="checkbox"/>	<input type="checkbox"/>
4.4.4	Removal of .rhosts and .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
4.4.5	Remote daemon lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.2	/etc/inetd.conf - cmsd	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.3	CDE - disabling dtlogin	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.4	/etc/inetd.conf - dtspc	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.5	CDE - sgid/suid binary lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.6	CDE - remote GUI login disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.7	CDE - screensaver lock	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.8	CDE - login screen hostname masking	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.9	CDE - /etc/dt/config/Xconfig permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.10	CDE - /etc/dt/config/Xservers permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.11	CDE - /etc/dt/config/*/Xresources permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.1	FTPD: Disable root access to ftpd	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.2	FTPD: Display acceptable usage policy during login	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.3	FTPD: Prevent world access and group write to files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.2	OpenSSH: Remove /etc/shosts.equiv and /etc/rhosts.equiv	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.3	OpenSSH: Remove .shosts files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.1	/etc/mail/sendmail.cf - Hide sendmail version information	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.2	/etc/mail/sendmail.cf - PrivacyOptions	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.3	/etc/mail/sendmail.cf - DaemonPortOptions	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.4.4	/etc/mail/sendmail.cf - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.5	/var/spool/clientmqueue - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.6	/var/spool/mqueue - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.1	SNMP - disable private community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.2	SNMP - disable system community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.3	SNMP - disable public community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.4	SNMP - disable Readwrite community access	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.5	SNMP - restrict community access	<input type="checkbox"/>	<input type="checkbox"/>
4.5.6	Uninstall snmp	<input type="checkbox"/>	<input type="checkbox"/>
4.5.7	Uninstall/Disable sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.6.1	/etc/security/login.cfg - logintimeout	<input type="checkbox"/>	<input type="checkbox"/>
4.6.2	/etc/security/login.cfg - logindelay	<input type="checkbox"/>	<input type="checkbox"/>
4.6.3	herald (logon message)	<input type="checkbox"/>	<input type="checkbox"/>
4.6.4	loginretries	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.12	/var/adm/cron/at.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.8.1	TE - implementation	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.1	histexpire	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.2	histsize	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.3	minage	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	All accounts must have a hashed password	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Establish and Maintain an Inventory of User Accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	adm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	bin	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	daemon	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	guest	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	lpd	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	nobody	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	nuucp	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	sys	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	uucp	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.10	Ensure System Accounts cannot access system using ftp.	<input type="checkbox"/>	<input type="checkbox"/>
5.6	maxage	<input type="checkbox"/>	<input type="checkbox"/>
5.7	maxexpired	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Privilege escalation: enhanced RBAC	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Privilege escalation: sudo	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure sudo logging is active	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Adding authorized users in at.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Services - at access is root only	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Adding authorised users in cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Services - crontab access is root only	<input type="checkbox"/>	<input type="checkbox"/>
8.1.1	Configuring syslog - local logging	<input type="checkbox"/>	<input type="checkbox"/>
8.1.2	Configuring syslog - remote logging	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	Configuring syslog - remote messages	<input type="checkbox"/>	<input type="checkbox"/>
8.2	AIX Auditing	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Application Data with requirement for world writable directories	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure all files and directories are owned by a user (uid) and assigned to a group (gid)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.1	autoconf6	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.2	ndpd-host	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router	<input type="checkbox"/>	<input type="checkbox"/>
4.2.18	ip6forwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	Ensure that IP Security is available	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure loopback traffic is blocked on external interfaces	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3	Ensure that IPsec filters are active	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.7	CDE - screensaver lock	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.1	FTPD: Disable root access to ftpd	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.2	FTPD: Display acceptable usage policy during login	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.3	FTPD: Prevent world access and group write to files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.1	OpenSSH: Minimum version is 8.1	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed"	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -I INFO'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s).	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.1	histexpire	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.2	histsize	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.3	minage	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	All accounts must have a hashed password	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	All usernames and UIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Establish and Maintain an Inventory of User Accounts	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt'	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	minloweralpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	adm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	bin	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	daemon	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	guest	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	lpd	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	nobody	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	nuucp	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	sys	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	uucp	<input type="checkbox"/>	<input type="checkbox"/>
5.3.10	Ensure System Accounts cannot access system using ftp.	<input type="checkbox"/>	<input type="checkbox"/>
5.6	maxage	<input type="checkbox"/>	<input type="checkbox"/>
5.7	maxexpired	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Privilege escalation: sudo	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure sudo logging is active	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Adding authorized users in at.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Adding authorised users in cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Allowlist Authorized Software and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Allowlist Authorized Libraries and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Enforce Allowlist aka Trusted Execution Checks	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Encryption: File System Level (EFS)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Encryption: Logical Volume (ELV)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Application Data with requirement for world writable directories	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure all files and directories are owned by a user (uid) and assigned to a group (gid)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Disable writesrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Disable ntalk/talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	dt	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	piobe	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	qdaemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.6	rc.nfs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	cas_agent	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	inetd - aka Super Daemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.2	aixmibd	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.2.3	dhcpcd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	dhcprd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	dhcpsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	dpid2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	gated	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	hostmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	mrouted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	named	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	portmap	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.12	routed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.13	rwhod	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.14	sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.15	snmpd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.16	snmpmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.17	timed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.1	autoconf6	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.2	ndpd-host	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.1	bootps	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.2	chargen	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.3	comsat	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.4	daytime	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.5	discard	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.6	echo	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.7	exec	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.8	finger	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.9	ftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.10	imap2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.11	instsrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.12	klogin	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.13	kshell	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.5.14	login	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.15	netstat	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.16	ntalk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.17	pcnfsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.18	pop3	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.19	rexed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.20	rquotad	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.21	rstatd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.22	rusersd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.23	rwalld	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.24	shell	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.25	sprayd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.26	xmquery	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.27	talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.28	telnet	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.29	tftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.30	time	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.31	uucp	<input type="checkbox"/>	<input type="checkbox"/>
4.2.18	ip6forwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	Ensure that IP Security is available	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure loopback traffic is blocked on external interfaces	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3	Ensure that IPsec filters are active	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.1	NIS - de-install NIS client	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.2	NIS - de-install NIS server	<input type="checkbox"/>	<input type="checkbox"/>
4.4.5	Remote daemon lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.1	CDE - de-installing CDE	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.3	CDE - disabling dtlogin	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.4	/etc/inetd.conf - dtspc	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.6	CDE - remote GUI login disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.7	CDE - screensaver lock	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.1	FTPD: Disable root access to ftpd	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.2.2	FTPD: Display acceptable usage policy during login	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.3	FTPD: Prevent world access and group write to files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.1	OpenSSH: Minimum version is 8.1	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed"	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -l INFO'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s).	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit	<input type="checkbox"/>	<input type="checkbox"/>
4.6.4	loginretries	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.1	New configuration file for sendmail /etc/mail/submit.cf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.1	histexpire	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.1.2	histsize	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.3	minage	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	All accounts must have a hashed password	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	All usernames and UIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Establish and Maintain an Inventory of User Accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt'	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	minloweralpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	adm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	bin	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	daemon	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	guest	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	lpd	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	nobody	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	nuucp	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	sys	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	uucp	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.10	Ensure System Accounts cannot access system using ftp.	<input type="checkbox"/>	<input type="checkbox"/>
5.6	maxage	<input type="checkbox"/>	<input type="checkbox"/>
5.7	maxexpired	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Privilege escalation: sudo	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure sudo logging is active	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Adding authorized users in at.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Services - at access is root only	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Adding authorised users in cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Services - crontab access is root only	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Use FLRTVC regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1	Collect system configuration regularly	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Scan for TROJAN aka Untrusted/Unauthorized Applications (Implement Allowlist)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Allowlist Authorized Software and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Allowlist Authorized Libraries and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.5	Allowlist Authorized Scripts and Report Violations	<input type="checkbox"/>	<input type="checkbox"/>
2.6	Enforce Allowlist aka Trusted Execution Checks	<input type="checkbox"/>	<input type="checkbox"/>
2.7	Remove Unused Symbolic Links	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Encryption: File System Level (EFS)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Encryption: Logical Volume (ELV)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure default user umask is 027 or more restrictive	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Remove group write permission from default groups - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Application Data with requirement for world writable directories	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure there are no world writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure there are no 'staff' writable files - exceptions must be in TSD and audit	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure all files and directories are owned by a user (uid) and assigned to a group (gid)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.1	Disable writesrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.2	Disable ntalk/talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.3	dt	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.4	piobe	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.5	qdaemon	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.6	rc.nfs	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1.7	cas_agent	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.1	inetd - aka Super Daemon	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.2.2	aixmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.3	dhcpcd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.4	dhcprd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.5	dhcpsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.6	dpid2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.7	gated	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.8	hostmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.9	mrouted	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.10	named	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.11	portmap	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.12	routed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.13	rwhod	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.14	sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.15	snmpd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.16	snmpmibd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2.17	timed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.1	autoconf6	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.2	ndpd-host	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3.3	ndpd-router	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.1	bootps	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.2	chargen	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.3	comsat	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.4	daytime	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.5	discard	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.6	echo	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.7	exec	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.8	finger	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.9	ftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.10	imap2	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.11	instsrv	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.12	klogin	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.5.13	kshell	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.14	login	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.15	netstat	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.16	ntalk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.17	pcnfsd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.18	pop3	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.19	rexed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.20	rquotad	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.21	rstatd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.22	rusersd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.23	rwalld	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.24	shell	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.25	sprayd	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.26	xmquery	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.27	talk	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.28	telnet	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.29	tftp	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.30	time	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5.31	uucp	<input type="checkbox"/>	<input type="checkbox"/>
4.2.18	ip6forwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.3.1	Ensure that IP Security is available	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure loopback traffic is blocked on external interfaces	<input type="checkbox"/>	<input type="checkbox"/>
4.3.3	Ensure that IPsec filters are active	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.1	NIS - de-install NIS client	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.2	NIS - de-install NIS server	<input type="checkbox"/>	<input type="checkbox"/>
4.4.5	Remote daemon lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.1	CDE - de-installing CDE	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.3	CDE - disabling dtlogin	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.4	/etc/inetd.conf - dtspc	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.6	CDE - remote GUI login disabled	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.7	CDE - screensaver lock	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.5.2.1	FTPD: Disable root access to ftpd	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.2	FTPD: Display acceptable usage policy during login	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2.3	FTPD: Prevent world access and group write to files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.1	OpenSSH: Minimum version is 8.1	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.4	sshd_config: Restrict users and groups allowed access via OpenSSH	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.5	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.6	sshd_config: Banner exists and message contains "Only authorized users allowed"	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.7	sshd_config: HostbasedAuthentication is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.8	sshd_config: IgnoreRhosts is 'yes' or 'shosts-only'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.9	sshd_config: PermitEmptyPasswords is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.10	sshd_config: LogLevel is 'INFO' or 'VERBOSE'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.11	sshd_config: sftp-server arguments include '-u 027 -f AUTH -l INFO'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.12	sshd_config: MaxAuthTries is '4'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.13	sshd_config: PermitUserEnvironment is 'no'	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.14	sshd_config: Use Conditional exception(s).	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.15	sshd_config, ssh_config: KexAlgorithms	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.16	sshd_config, ssh_config: Ciphers	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.17	sshd_config, ssh_config: MACs - Message Authentication Codes	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.18	sshd_config, ssh_config: ReKeyLimit	<input type="checkbox"/>	<input type="checkbox"/>
4.6.4	loginretries	<input type="checkbox"/>	<input type="checkbox"/>
4.6.5	Unattended terminal session timeout is 900 seconds (or less)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.1	Home directory must exist	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.2	Home directory must be owned by account, or special account	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.3	Home directory: write access restricted to 'owner'	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.4	AUDIT subsystem: /audit and /etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.5	SECURITY Subsystems: /etc/security	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.7.1.6	/var/adm/ras	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.7	/var/adm/sa	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.8	/var/spool/cron/crontabs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.9	Ensure all directories in root PATH deny write access to all	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.10	Ensure root user has a dedicated home directory	<input type="checkbox"/>	<input type="checkbox"/>
4.7.1.11	/etc/security/audit	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.1	New configuration file for sendmail /etc/mail/submit.cf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.2	Verify Trust of suid, sgid, acl, and trusted-bit files and programs	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.3	crontab entries - owned by userid	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.4	Home directory configuration files	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.5	/smit.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.6	/etc/group	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.7	/etc/inetd.conf	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.8	/etc/motd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.9	/etc/passwd	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.10	/etc/ssh/ssh_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.11	/etc/ssh/sshd_config	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.13	/var/adm/cron/cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.14	/var/ct/RMstart.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.15	/var/adm/cron/log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.16	/var/tmp/dpid2.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.17	/var/tmp/hostmibd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.18	/var/tmp/snmpd.log	<input type="checkbox"/>	<input type="checkbox"/>
4.9	Ensure root access is controlled	<input type="checkbox"/>	<input type="checkbox"/>
4.10	Disable core dumps	<input type="checkbox"/>	<input type="checkbox"/>
4.11	Remove current working directory from default /etc/environment PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.12	Lock historical users	<input type="checkbox"/>	<input type="checkbox"/>
4.13	Remove current working directory from root's PATH	<input type="checkbox"/>	<input type="checkbox"/>
4.14	Configuration: /etc/motd	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.1.1	histexpire	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.2	histsize	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1.3	minage	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	All accounts must have a hashed password	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	All usernames and UIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	All group names and GIDs must be unique	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Establish and Maintain an Inventory of Administrator accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Establish and Maintain an Inventory of User Accounts	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure new passwords are controlled by password attributes (disable NOCHECK)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	pwd_algorithm	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure passwords are not hashed using 'crypt'	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure password policy is enforced for all users	<input type="checkbox"/>	<input type="checkbox"/>
5.2.5	minlen	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	mindiff	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	minalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	minother	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	maxrepeats	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	mindigit	<input type="checkbox"/>	<input type="checkbox"/>
5.2.11	minloweralpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.12	minupperalpha	<input type="checkbox"/>	<input type="checkbox"/>
5.2.13	minspecialchar	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	adm	<input type="checkbox"/>	<input type="checkbox"/>
5.3.2	bin	<input type="checkbox"/>	<input type="checkbox"/>
5.3.3	daemon	<input type="checkbox"/>	<input type="checkbox"/>
5.3.4	guest	<input type="checkbox"/>	<input type="checkbox"/>
5.3.5	lpd	<input type="checkbox"/>	<input type="checkbox"/>
5.3.6	nobody	<input type="checkbox"/>	<input type="checkbox"/>
5.3.7	nuucp	<input type="checkbox"/>	<input type="checkbox"/>
5.3.8	sys	<input type="checkbox"/>	<input type="checkbox"/>
5.3.9	uucp	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.3.10	Ensure System Accounts cannot access system using ftp.	<input type="checkbox"/>	<input type="checkbox"/>
5.6	maxage	<input type="checkbox"/>	<input type="checkbox"/>
5.7	maxexpired	<input type="checkbox"/>	<input type="checkbox"/>
6.2.1	Privilege escalation: enhanced RBAC	<input type="checkbox"/>	<input type="checkbox"/>
6.3.1	Privilege escalation: sudo	<input type="checkbox"/>	<input type="checkbox"/>
6.3.2	Ensure sudo logging is active	<input type="checkbox"/>	<input type="checkbox"/>
6.3.3	Ensure sudo commands use pty	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Adding authorized users in at.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.5	Services - at access is root only	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Adding authorised users in cron.allow	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Services - crontab access is root only	<input type="checkbox"/>	<input type="checkbox"/>
7.1	Use FLRT regularly	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Use FLRTVC regularly	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.8	Ensure the Trusted Execution Policies cannot be modified	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.1	NFS - de-install NFS client	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.2	NFS - de-install NFS server	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.3	NFS - enable both nosuid and nodev options on NFS client mounts	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.4	NFS - localhost removal	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.5	NFS - restrict NFS access	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.6	NFS - no_root_squash option	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4.7	NFS - secure NFS	<input type="checkbox"/>	<input type="checkbox"/>
4.2.1	clean_partial_conns	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	bcastping	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	directed_broadcast	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	icmpaddressmask	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	ipforwarding	<input type="checkbox"/>	<input type="checkbox"/>
4.2.6	ipignoreredirects	<input type="checkbox"/>	<input type="checkbox"/>
4.2.7	ipsendredirects	<input type="checkbox"/>	<input type="checkbox"/>
4.2.8	ipsrcrouteforward	<input type="checkbox"/>	<input type="checkbox"/>
4.2.9	ipsrcrouterecv	<input type="checkbox"/>	<input type="checkbox"/>
4.2.10	ipsrcroutesend	<input type="checkbox"/>	<input type="checkbox"/>
4.2.11	ip6srcrouteforward	<input type="checkbox"/>	<input type="checkbox"/>
4.2.12	nfs_use_reserved_ports	<input type="checkbox"/>	<input type="checkbox"/>
4.2.13	nonlocsrcroute	<input type="checkbox"/>	<input type="checkbox"/>
4.2.14	sockthresh	<input type="checkbox"/>	<input type="checkbox"/>
4.2.15	tcp_pmtu_discover	<input type="checkbox"/>	<input type="checkbox"/>
4.2.16	tcp_tcpsecure	<input type="checkbox"/>	<input type="checkbox"/>
4.2.17	udp_pmtu_discover	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.4.1.3	NIS - remove NIS markers from password and group files	<input type="checkbox"/>	<input type="checkbox"/>
4.4.1.4	NIS - restrict NIS server communication	<input type="checkbox"/>	<input type="checkbox"/>
4.4.2	Remote command lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.4.3	Removal of entries from /etc/hosts.equiv	<input type="checkbox"/>	<input type="checkbox"/>
4.4.4	Removal of .rhosts and .netrc files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.2	/etc/inetd.conf - cmsd	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.5	CDE - sgid/suid binary lockdown	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.8	CDE - login screen hostname masking	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.9	CDE - /etc/dt/config/Xconfig permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.10	CDE - /etc/dt/config/Xservers permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.1.11	CDE - /etc/dt/config/*/Xresources permissions and ownership	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.2	OpenSSH: Remove /etc/shosts.equiv and /etc/rhosts.equiv	<input type="checkbox"/>	<input type="checkbox"/>
4.5.3.3	OpenSSH: Remove .shosts files	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.1	/etc/mail/sendmail.cf - Hide sendmail version information	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.2	/etc/mail/sendmail.cf - PrivacyOptions	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.3	/etc/mail/sendmail.cf - DaemonPortOptions	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.4	/etc/mail/sendmail.cf - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.5	/var/spool/clientmqueue - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.4.6	/var/spool/mqueue - access control	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.1	SNMP - disable private community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.2	SNMP - disable system community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.3	SNMP - disable public community string	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.4	SNMP - disable Readwrite community access	<input type="checkbox"/>	<input type="checkbox"/>
4.5.5.5	SNMP - restrict community access	<input type="checkbox"/>	<input type="checkbox"/>
4.5.6	Uninstall snmp	<input type="checkbox"/>	<input type="checkbox"/>
4.5.7	Uninstall/Disable sendmail	<input type="checkbox"/>	<input type="checkbox"/>
4.6.1	/etc/security/login.cfg - logintimeout	<input type="checkbox"/>	<input type="checkbox"/>
4.6.2	/etc/security/login.cfg - logindelay	<input type="checkbox"/>	<input type="checkbox"/>
4.6.3	herald (logon message)	<input type="checkbox"/>	<input type="checkbox"/>
4.7.2.12	/var/adm/cron/at.allow	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.8.1	TE - implementation	<input type="checkbox"/>	<input type="checkbox"/>
8.1.1	Configuring syslog - local logging	<input type="checkbox"/>	<input type="checkbox"/>
8.1.2	Configuring syslog - remote logging	<input type="checkbox"/>	<input type="checkbox"/>
8.1.3	Configuring syslog - remote messages	<input type="checkbox"/>	<input type="checkbox"/>
8.2	AIX Auditing	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
September 30, 2022	1.0.0	Published