

CIS IBM AIX 7.1 Benchmark

v2.0.0 - 10-04-2021

Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

Table of Contents

Terms of Use	1
Overview	11
Intended Audience	11
Consensus Guidance.....	11
Assessment Status.....	12
Profile Definitions	13
Acknowledgements	14
Recommendations	15
1 Using this Benchmark.....	15
1.1 Benchmark Scenarios	19
1.2 Using the Build Kit	21
1.3 AIX Installation.....	22
1.4 AIX Maintenance Cadence and Security Management.....	25
1.5 Summary.....	27
2 AIX Security Expert - Technology.....	29
2.1 AIXPERT: Basic usage	30
2.2 AIXPERT: Standard policies	31
2.3 AIXPERT: Custom Policies	33
2.4 Role of AIXPERT in the CIS AIX benchmark.....	34
2.5 Applying the CIS Policy	35
3 AIX Recommendations	37
3.1 Account Management.....	39
3.1.1 Local Identification Management.....	40
3.1.1.1 All accounts must have a hashed password (Automated).....	41
3.1.1.2 All user id's must be unique (Automated).....	45
3.1.1.3 All group id's must be unique (Automated).....	47
3.1.2 Password Controls - Local Registry.....	49
3.1.2.1 histexpire (Automated).....	50
3.1.2.2 histsize (Automated).....	52

3.1.2.3 loginretries (Automated)	54
3.1.2.4 maxage (Automated).....	56
3.1.2.5 maxexpired (Automated)	58
3.1.2.6 maxrepeats (Automated)	60
3.1.2.7 minage (Automated)	62
3.1.2.8 minalpha (Automated).....	64
3.1.2.9 mindiff (Automated)	66
3.1.2.10 mindigit (Automated)	68
3.1.2.11 minlen (Automated)	70
3.1.2.12 minloweralpha (Automated)	72
3.1.2.13 minother (Automated)	74
3.1.2.14 minspecialchar (Automated)	76
3.1.2.15 minuppervalpha (Automated)	78
3.1.3 System Accounts	80
3.1.3.1 adm (Automated)	81
3.1.3.2 bin (Automated).....	83
3.1.3.3 daemon (Automated).....	85
3.1.3.4 guest (Automated)	87
3.1.3.5 lpd (Automated).....	89
3.1.3.6 nobody (Automated).....	91
3.1.3.7 nuucp (Automated)	93
3.1.3.8 sys (Automated).....	95
3.1.3.9 uucp (Automated)	97
3.1.3.10 Ensure System Accounts cannot access system using ftp. (Automated)..	99
3.1.4 User Attributes for Active Processes.....	101
3.2 Access Control Management.....	102
3.2.1 RBAC managed privilege escalation	103
3.2.1.1 Privilege escalation: enhanced RBAC (Manual)	104
3.2.2 SUDO managed privilege escalation.....	107
3.2.2.1 Privilege escalation: sudo (Manual)	108

3.2.2.2 Ensure sudo log file is active (Manual)	110
3.2.2.3 Ensure sudo commands use pty (Manual)	112
3.2.3 Special Permissions Management - suid, sgid, acl, and trusted-bit files and programs (Manual)	114
3.2.4 Adding authorized users in at.allow (Manual)	117
3.2.5 Services - at access is root only (Automated)	119
3.2.6 Adding authorised users in cron.allow (Automated).....	121
3.2.7 Services - crontab access is root only (Automated)	123
3.3 Network Infrastructure Management.....	125
3.3.1 Boot phase: /etc/inittab.....	126
3.3.1.1 Disable writesrv (Automated).....	127
3.3.1.2 dt (Automated).....	129
3.3.1.3 piobe (Automated).....	131
3.3.1.4 qdaemon (Automated)	133
3.3.1.5 rcnfs (Automated)	135
3.3.1.6 cas_agent (Automated).....	137
3.3.2 Boot phase: /etc/rc.tcpip: daemons	139
3.3.2.1 Disable ntalk/talk/write (Automated)	140
3.3.2.2 aixmibd (Automated).....	142
3.3.2.3 dhcpcd (Automated)	144
3.3.2.4 dhcprd (Automated)	146
3.3.2.5 dhcpsd (Automated)	148
3.3.2.6 dpid2 (Automated)	150
3.3.2.7 gated (Automated).....	152
3.3.2.8 hostmibd (Automated).....	154
3.3.2.9 inetd - aka Super Daemon (Automated).....	156
3.3.2.10 mrouted (Automated)	158
3.3.2.11 named (Automated).....	160
3.3.2.12 portmap (Automated).....	162
3.3.2.13 routed (Automated).....	164
3.3.2.14 rwhod (Automated).....	166

3.3.2.15 sendmail (Automated).....	168
3.3.2.16 snmpd (Automated).....	170
3.3.2.17 snmpmibd (Automated).....	172
3.3.2.18 timed (Automated).....	174
3.3.3 Boot phase: IPv6.....	176
3.3.3.1 autoconf6 (Automated).....	177
3.3.3.2 ndpd-host (Automated)	179
3.3.3.3 ndpd-router (Automated).....	183
3.3.4 inetd services.....	185
3.3.4.1 bootps (Automated)	186
3.3.4.2 chargen (Automated).....	188
3.3.4.3 comsat (Automated).....	190
3.3.4.4 daytime (Automated).....	192
3.3.4.5 discard (Automated)	194
3.3.4.6 echo (Automated)	196
3.3.4.7 exec (Automated)	198
3.3.4.8 finger (Automated)	200
3.3.4.9 ftp (Automated)	202
3.3.4.10 imap2 (Automated).....	204
3.3.4.11 instsrv (Automated)	206
3.3.4.12 klogin (Automated).....	208
3.3.4.13 kshell (Automated)	210
3.3.4.14 login (Automated)	212
3.3.4.15 netstat (Automated)	214
3.3.4.16 ntalk (Automated)	216
3.3.4.17 pcnfsd (Automated).....	218
3.3.4.18 pop3 (Automated)	220
3.3.4.19 rexd (Automated)	222
3.3.4.20 rquotad (Automated).....	224
3.3.4.21 rstatd (Automated)	226

3.3.4.22 rusersd (Automated)	228
3.3.4.23 rwalld (Automated)	230
3.3.4.24 shell (Automated)	232
3.3.4.25 sprayd (Automated)	234
3.3.4.26 xmquery (Automated)	236
3.3.4.27 talk (Automated)	238
3.3.4.28 telnet (Automated)	240
3.3.4.29 tftp (Automated)	242
3.3.4.30 time (Automated)	244
3.3.4.31 uucp (Automated)	246
3.3.5 NFS	248
3.3.5.1 NFS - de-install NFS server (Automated)	249
3.3.5.2 NFS - enable both nosuid and nodev options on NFS client mounts (Automated)	251
3.3.5.3 NFS - localhost removal (Automated)	253
3.3.5.4 NFS - restrict NFS access (Automated)	255
3.3.5.5 NFS - no root access via NFS exports (Automated)	257
3.3.5.6 NFS - secure NFS (Automated)	259
3.4 Network Monitoring and Defense	261
3.4.1 bcastping (Automated)	262
3.4.2 clean_partial_conns (Automated)	263
3.4.3 directed_broadcast (Automated)	264
3.4.4 icmpaddressmask (Automated)	265
3.4.5 ipforwarding (Automated)	266
3.4.6 ipignoreredirects (Automated)	267
3.4.7 ipsendredirects (Automated)	268
3.4.8 ipsrouteforward (Automated)	269
3.4.9 ipsrouterecv (Automated)	270
3.4.10 ipsroutesev (Automated)	271
3.4.11 ip6srouteforward (Automated)	272
3.4.12 nfs_use_reserved_ports (Automated)	273

3.4.13 nonlocsrcroute (Automated)	274
3.4.14 sockthresh (Automated).....	275
3.4.15 tcp_pmtu_discover (Automated)	276
3.4.16 tcp_tcpsecure (Automated)	277
3.4.17 udp_pmtu_discover (Automated)	278
3.5 Data Protection	279
3.5.1 Encrypted Filesystems (EFS)	280
3.5.1.1 EFS - implementation (Automated)	281
3.5.2 Ensure default user umask is 027 or more restrictive (Automated).....	284
3.5.3 General Permissions Management - world writable directories (Manual).286	
3.5.4 General Permissions Management - world writable files (Manual)	288
3.5.5 Ensure no unowned files or directories exist (Automated)	290
3.6 Secure Configuration of Enterprise Assets and Software.....	293
3.6.1 Common Desktop Environment (CDE)	294
3.6.1.1 CDE - de-installing CDE (Automated).....	295
3.6.1.2 /etc/inetd.conf - cmsd (Automated).....	297
3.6.1.3 CDE - disabling dtlogin (Automated)	299
3.6.1.4 /etc/inetd.conf - dtspc (Automated)	301
3.6.1.5 CDE - sgid/suid binary lockdown (Automated)	303
3.6.1.6 CDE - remote GUI login disabled (Automated)	305
3.6.1.7 CDE - screensaver lock (Automated)	308
3.6.1.8 CDE - login screen hostname masking (Automated).....	310
3.6.1.9 CDE - /etc/dt/config/Xconfig permissions and ownership (Automated)312	
3.6.1.10 CDE - /etc/dt/config/Xservers permissions and ownership (Automated)	314
3.6.1.11 CDE - /etc/dt/config/*/Xresources permissions and ownership (Automated).....	316
3.6.2 OpenSSH.....	318
3.6.2.1 OpenSSH - Installation (Automated)	319
3.6.2.2 OpenSSH - PermitRootLogin (Automated).....	321
3.6.2.3 OpenSSH - Banner (Automated).....	326

3.6.2.4 Ensure SSH IgnoreRhosts is enabled (Automated)	328
3.6.2.5 Ensure SSH PermitEmptyPasswords is disabled (Automated)	330
3.6.2.6 Configuring SSH - disallow host based authentication (Automated)	332
3.6.2.7 Configuring SSH - removal of .shosts files (Automated)	335
3.6.2.8 Configuring SSH - removal of /etc/shosts.equiv (Automated)	337
3.6.2.9 Configuring SSH - set LogLevel to INFO or VERBOSE (Automated)	339
3.6.2.10 OpenSSH - configure sftp-server (Automated)	341
3.6.2.11 OpenSSH: Ensure MaxAuthTries is set to 4 or less (Automated)	343
3.6.2.12 OpenSSH: Ensure only strong ciphers are used (Automated)	344
3.6.2.13 Ignore user-provided environment variables (Automated)	346
3.6.2.14 OpenSSH: Regulate access to server (Manual)	347
3.6.3 Sendmail Configuration	349
3.6.3.1 /etc/mail/sendmail.cf - SmtgreetingMessage (Automated)	350
3.6.3.2 /etc/mail/sendmail.cf - permissions and ownership (Automated)	352
3.6.3.3 /var/spool/mqueue - permissions and ownership (Automated)	354
3.6.4 Login Controls: /etc/security/login.cfg	356
3.6.4.1 /etc/security/login.cfg - logintimeout (Automated)	357
3.6.4.2 /etc/security/login.cfg - logindelay (Automated)	359
3.6.4.3 herald (logon message) (Automated)	360
3.6.4.4 /etc/security/login.cfg - pwd_algorithm (Automated)	361
3.6.5 Remove or Disable Weak/Defunct Network Services	363
3.6.5.1.1 NIS - de-install NIS client (Automated)	365
3.6.5.1.2 NIS - de-install NIS server (Automated)	367
3.6.5.1.3 NIS - remove NIS markers from password and group files (Automated)	369
3.6.5.1.4 NIS - restrict NIS server communication (Automated)	371
3.6.5.2.1 SNMP - disable private community string (Automated)	375
3.6.5.2.2 SNMP - disable system community string (Automated)	377
3.6.5.2.3 SNMP - disable public community string (Automated)	379
3.6.5.2.4 SNMP - disable Readwrite community access (Automated)	381
3.6.5.2.5 SNMP - restrict community access (Automated)	383

3.6.5.3 Remote command lockdown (Automated)	385
3.6.5.4 Removal of entries from /etc/hosts.equiv (Automated)	387
3.6.5.5 Removal of .rhosts and .netrc files (Automated).....	388
3.6.5.6 Remote daemon lockdown (Automated)	389
3.6.6 Service Accounts	391
3.6.6.1 FTP: Prevent world access and group write to files (Automated)	392
3.6.6.2 FTP: Display acceptable usage policy during login (Automated)	394
3.6.6.3 FTP: Disable root access to ftp (Automated)	396
3.6.7 Trusted Execution (TE)	398
3.6.7.1 TE - implementation (Automated)	399
3.6.8 Trusted Files and Directories.....	402
3.6.8.1.1 Ensure all directories in root PATH deny write access to all (Automated)	404
3.6.8.1.2 Home directory must deny write to all except owner (Manual)	407
3.6.8.1.3 /audit (Automated).....	411
3.6.8.1.4 /etc/security (Automated)	413
3.6.8.1.5 /etc/security/audit (Automated).....	415
3.6.8.1.6 /var/adm/ras (Automated).....	417
3.6.8.1.7 /var/adm/sa (Automated)	419
3.6.8.1.8 /var/spool/cron/crontabs (Automated)	421
3.6.8.2.1 crontab entries - owned by userid (Automated)	424
3.6.8.2.2 Home directory configuration files (Automated).....	427
3.6.8.2.3 /smit.log (Automated)	429
3.6.8.2.4 /etc/group (Automated).....	431
3.6.8.2.5 /etc/inetd.conf (Automated).....	433
3.6.8.2.6 /etc/motd (Automated)	435
3.6.8.2.7 /etc/passwd (Automated)	437
3.6.8.2.8 /etc/ssh/ssh_config (Automated)	439
3.6.8.2.9 /etc/ssh/sshd_config (Automated)	441
3.6.8.2.10 /var/adm/cron/at.allow (Automated).....	444
3.6.8.2.11 /var/adm/cron/cron.allow (Automated)	446

3.6.8.2.12 /var/ct/RMstart.log (Automated)	448
3.6.8.2.13 /var/adm/cron/log (Automated)	450
3.6.8.2.14 /var/tmp/dpid2.log (Automated)	452
3.6.8.2.15 /var/tmp/hostmibd.log (Automated)	454
3.6.8.2.16 /var/tmp/snmpd.log (Automated)	456
3.6.9 Ensure root access is controlled (Automated)	458
3.6.10 Disable core dumps (Automated)	460
3.6.11 Remove current working directory from default /etc/environment PATH (Automated)	462
3.6.12 Remove current working directory from root's PATH (Automated)	463
3.6.13 Lock historical users (Automated)	464
3.6.14 Configuration: /etc/motd (Automated)	466
3.6.15 Unattended terminal session timeout is 900 seconds (or less) (Manual)	468
3.7 Audit Log Management	471
3.7.1 Syslog	472
3.7.1.1 Configuring syslog - local logging (Manual)	473
3.7.1.2 Configuring syslog - remote logging (Automated)	476
3.7.1.3 Configuring syslog - remote messages (Automated)	478
3.7.2 AIX Auditing (Manual)	480
Appendix: AIXPERT Table	484
Appendix: Recommendation Summary Table	503
Appendix: Change History	510

Overview

This document, Security Configuration Benchmark for AIX 7.1, provides prescriptive guidance for establishing a secure configuration posture for AIX version 7.1 running on the Power Systems platform. This guide was tested against AIX 7.1 (TL3, TL4 and TL5) installed from IBM base installation media.

The guidance within requires that operations are being performed as the root user. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. It is advisable to verify root users path integrity and the integrity of any programs being run prior to execution of commands and scripts included in this benchmark.

To obtain the latest version of this guide, please visit

<https://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 7.1 on the Power Systems platform. A working knowledge of `vi` is assumed in order to implement some of the configuration changes.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Assessment Status

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

Automated

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

Manual

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

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:

- extends the "Level 1" profile
- contains more stringent configurations than "Level 1"
- accepts that security requirements may prevail over availability
- may negatively inhibit the utility or performance of the technology
- acts as defense in depth

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

Recommendations

1 Using this Benchmark

This benchmark provides security configuration guidance for use during the configuration of the AIX 7.1 Operating System. The scope of the guide is applicable to AIX 7.1 TL-03 SP1 and above. The recommendations in this guide have been explicitly tested on AIX 7.1 TL-03, TL04 and TL05.

CIS Critical Controls are leading

This new version is a major re-write of the previous version (from 2013). The key difference is that recommendations are no longer organized in terms of `aixpert` groups. Instead, the document recommendation sections are ordered according to CIS Critical Controls (v8).

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

CIS Controls Version 8 Design Principles

When we begin the work of a new version we sit down first to establish “design principles” that will be used to guide the process. These serve as a decision “touchstone” to remind us of what is really important, and of the goals of the CIS Controls. While these have been fairly consistent since the earliest versions of the Controls, we’ve been refining our thinking over the last couple of versions to focus on the role that the Controls play in the total picture of enterprise security.

- 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 Controls and Implementation Profiles

- 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.

The role of AIXPERT

AIXPERT is a very useful tool to enable system configuration and verify configuration using profiles. In this benchmark the role of aixpert is to apply and verify CIS recommendations (as much as possible). CIS Members have access to an AIX build-kit that includes an XML file to apply the recommendations. But `aixpert` no longer drives the organization of the benchmark.

The task of running the benchmark

As stated above, as much as possible the benchmark document is organized following CIS Controls, and within sub-sections the recommendation titles are organized, wherever possible, alphabetically. As such, do not expect an `audit run` based on the document order to succeed. Explicitly, there are recommendations in section 3.6 (aka Secure Configuration of ...) that will need to be resolved before recommendations elsewhere (e.g., sub-sections of Section 3.1, Account Management) will be able to succeed. (The assumption is that will be other (sub-) section dependencies. This is a complex activity and you may need to re-run and remedy multiple times before the task is completed).

1.1 Benchmark Scenarios

This 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.

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 have been 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.

Another assumption is that AIX administrators do not have physical access to the POWER frame or managed system. The expectation is that physical access is managed by physical room controls and/or is exclusive to service providers (e.g., IAAS) or data center (server room) controls.

Fresh Installation - better for first-time users

While the intent is that this benchmark is suitable for both scenario we also expect that for first-time users working from a fresh install of AIX (insecure using default installation selections) and working through the recommendations is the better *Initial Approach* to 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.

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.

Working with existing systems (and CIS Secure Suite advantages)

CIS SecureSuite Membership entitles you (as we shall mention a few times in the document text) to a "Build Kit" that can be used, initially, to check an existing system for compliance. This file needs `aixpert`. Together - `aixpert` and the XML file from the build-kit - are all that are needed to enter a single command and get a good idea of how far on or off the target your system(s) is(are).

For example:

```
# aixpert -c -P ./cis-7.1.xml
Processedrules=117      Passedrules=64   Failedrules=53   Level=CIS
Input file=./cis-7.1.xml
```

Your needs are paramount

Depending on your needs and resource availability - one of the two scenarios will be your preferred scenario. Our goal is to provide the information you will need - regardless of your preference.

1.2 Using the Build Kit

CIS SecureSuite Members and existing systems

CIS SecureSuite Membership entitles you (as we shall mention a few times in the document text) to a "Build Kit" that can be used, initially, to check an existing system for compliance. This file needs `aixpert`. Together - `aixpert` and the XML file from the Build Kit - are all that are needed to enter a single command and get a good idea of how far on or off the target your system(s) is(are).

For example:

```
# aixpert -c -P ./cis-7.1.xml  
  
Processedrules=117      Passedrules=64   Failedrules=53   Level=CIS  
  
Input file=./cis-7.1.xml
```

1.3 AIX Installation

Below shows the steps used to install a generic, not-secured, system with AIX - using a NIM server. The same steps can be used from DVD media or images.

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.

1.4 AIX Maintenance Cadence and Security Management

Before beginning with the benchmark recommendation section we advise setting up a policy for OS (AIX) updates. AIX updates are either an update within a Technology Level (no AIX features are changed), an update to a new Technology Level (and its current Service Pack).

- This benchmark does not address AIX migration updates, e.g., from AIX 6.1 to AIX 7.1, or AIX 7.1 to AIX 7.2.

IBM AIX Maintenance Strategy

The current IBM software maintenance strategy revolves around the release of Technology Levels (TL) and Service Packs (SP). Previously Technology Levels were released twice per year, one in the spring and the other in fall. Currently, if at all, TLs are released annually (in the fall). A Technology introduces support for new hardware, new functionality, and new features and contain cumulative fixes since the release of the previous TL. Historically, the minimum fix support window for a given TL is two years from its release date. IBM is considering (or has already done so) extending this minimum period to three years.

Information on the current support window for a given TL can be found on

<https://www.ibm.com/support/pages/aix-support-lifecycle-information>.

Service Packs are released throughout the lifecycle of the TL and address security vulnerabilities and other critical fixes. For AIX 5.3 and AIX 6.1 they were typically released every 12 weeks; obviously this timeframe is dependent on the number and criticality of the issues found. For AIX 7.1 more than one SP per year is uncommon.

Setting a Maintenance Cadence

AIX Service Pack (SP) updates should be applied regularly. As updates are infrequent (sometimes only once per year) a prior policy of being with N-2 updates could keep your organization at nearly two years behind recent updates. We advise to apply a SP within 90 days of it's release. Recall, the normal release dates are April (if any) and October. There are no hard dates - this estimation is based on observation.

For an example see:

<https://www14.software.ibm.com/webapp/set2/sas/f/genunix3/AIXcurrent.jpg>

- We recommend starting application testing for a new TL at least a year before the end of (normal) support for the current TL. Frequently your organization may skip an intermediary TL (e.g., from AIX 7.1 TL3 to AIX 7.1 TL5).
- We recommend that full TL's or TL/SP's are applied rather than individual fixes. AIX TL/SP releases go through a rigorous testing process. The large and complex matrix of possible fix combinations are not subjected to the same degree of testing and therefore installing individual fixes is not recommended.

Interim Fixes, Third Party updates

A security fix will be initially released as an interim fix. These packages are installed and maintained via the `emgr` framework. Extremely critical security issues should be applied asap. For others you may consider to wait and apply the fix as part of a full SP release. Read the documentation, consider the impact - and do not forget to consider the potential time before the next TL/SP release. When in doubt open a ticket with IBM support and ask when the new SP (for the current TL) is expected.

Further, between SP releases IBM may produce interim Security fixes and/or there are so-called Third-Party updates (notably OpenSSL, OpenSSH and Java updates) that are managed separate from SP releases.

1.5 Summary

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.
- Do not apply interim fixes or individual fixes unless there is an requirement to do so. If time and priorities permit wait and apply full TL/SP's.
- Repeat system verification after an update. (e.g., file mode changes might be reverted by the update).
- Frequent backups of rootvg using `mksysb`. In particular, both *before* and *after* applying security updates.

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 AIX Security Expert - Technology

This section describes the AIX Security Expert framework. The tool, `aixpert` was added to base AIX to simplify and standardize the security hardening process in AIX. The technology manages over 300 settings within its scope.

The command `aixpert` and XML input (aka profiles/levels) can replace in-house security scripts and procedures.

The CIS AIX buildkit - freely available to CIS members - includes an XML file based on the recommendations in the benchmark. This XML file, applied using `aixpert` can be used to "implement the CIS benchmark for AIX".

This section is not meant to be an exhaustive coverage of AIX Security Expert. For a complete description of `aixpert` refer to [AIX Security pdf.pdf](#) and read the section entitled AIX Security Expert.

2.1 AIXPERT: Basic usage

The file `/etc/security/aixpert/core/aixpertall.xml` includes four (4) different security profiles (aka levels) that we discuss here: default (DLS, insecure), low (LLS), medium (MLS), and high (HLS).

One of these profiles can be applied, (e.g., medium) using the following command:

```
# aixpert -l medium
```

And the compliance with the medium level (policy!) is obtained using:

```
# aixpert -c -l medium
```

The output is a summary of rules checked, passed, and failed. Details are available in `/etc/security/aixpert/check_report.txt`.

2.2 AIXPERT: Standard policies

From its first release in AIX 5.2 `aixpert` has included multiple policies (the tool calls them levels) in the file `/etc/security/aixpert/core/aixpertall.xml`. The first three policies aka levels were: `low`, `medium`, and `high`.

As an added feature the ability to create a `custom` policy using the depreciated technology `websm` was added shortly after the initial release.

To round off the `aixpertall.xml` file an additional profiles (level) was added: `default`. The `default` profile can be used to initiate `aixpert` (i.e., create `/etc/security/aixpert/core/appliedaixpert.xml`) so that the command `aixpert -c` can be run successfully. Note: it might undo any previous manual configuration. More common is to use the command to compare the current (manual) settings with the `default` unhardened settings.

Default Level Security (DLS)

This policy can be used to reset AIX to its default (unsecured) settings.

While not secure - this provides a simple mechanism to restore AIX to a known, though unhardened, configuration. This can be needed to determine if a security setting is blocking a desired application or service availability.

Low Level Security (LLS)

This policy implements common non-disruptive security enhancements.

Typically this is suited to servers residing in an internal and secure local network environment. It provides a basic security lockdown, from a minimal default level.

Medium Level Security (MLS)

This policy implements more advanced hardening parameters than the Low Level. These include: port scan protection and an enhanced password management policy. This security level does allow clear text password protocol access, e.g. `ftp`, `rlogin`, and `telnet`.

Typically, this is suited to servers residing in a corporate network protected by a firewall.

High Level Security (HLS)

This policy implements the highest possible security hardening standards. These include: port scan protection and no access for any clear text password protocols. It assumes that the local network is not trusted and is potentially unsafe.

Typically, this is suited to servers residing in an unsafe network. For example, those which are internet facing.

Within modern IT infrastructure, internal firewalls are typically implemented to separate the internal network from any corporate or internet environments and external firewalls to further protect these environments from the outside world. These firewall devices are typically only configured to allow access to the systems on the required core application or database ports. Therefore, port shunning and scan protection are typically something implemented by a firewall, rather than at the operating system level.

AIXPERTALL.XML

The following table shows the **Function**, **Description**, **Command** and the command **arguments** for each of the default security levels (aka policies) included in the file

`/etc/security/aixpert/core/aixpertall.xml`.

- See: appendix aixpert table

2.3 AIXPERT: Custom Policies

The base `AIX Security Expert` provides multiple policies in a single file. One of these base policies is selected using the argument `-l` and a policy name or abbreviation (e.g., 'm' or 'h' for 'medium' or 'high', respectively).

Originally, `custom` was a level that was created using an XML selector widget built-in to the `websm` interface that was standard in AIX 4.3 through AIX 5.3. Now `custom` refers to an external file created by any means following the XML description used in the file `/etc/security/aixpert/core/aixpertall.xml` except that this customized file contains only one level.

while `aixpert` had an option (`-f`) to apply a custom profile it did not have a simple way to compare an existing system with a custom profile. **Starting with AIX 7.1 TL3** `aixpert` added the flag `-P` to compare an current AIX configuration with a profile, e.g.,

```
# aixpert -c -P myCustomPolicy.xml
```

CIS Policy

This benchmark is the basis for the 'CIS' level benchmark. That is, in the XML file, each rule contains this attribute:

```
<AIXPertRuleType type="CIS"/>
```

The starting point of this file is the `HLS` policy - as defined by AIX Security Development. Some of these settings are adjusted according to a consensus model from many benchmarks and especially by comments made on this benchmark during its `DRAFT` and `pre-Published` stages.

In other words, the approach is to implement a hybrid policy containing a combination of recommended settings from Medium and High Level default policies and/or from recommendations following other (generic) benchmarks (e.g., Passwords, OpenSSH).

A customized XML file provides the ultimate flexibility in terms of being able to choose whether or not to implement every recommended controlled setting in this benchmark. An XML file can be copied and modified to satisfy local security and/or environmental requirements.

This flexibility is not present within the default Low, Medium and High Level policies which provide a pre-defined rigid level of security hardening standards.

2.4 Role of AIXPERT in the CIS AIX benchmark

As mentioned in this sections overview - AIXPERT is a core technology for hardening AIX. To this end IBM AIX provides several default profile levels.

A starting point for the early AIX benchmarks was the so-called `high` level profile. Besides the benchmark, published as a PDF and made available to any interested party, CIS also provides so-called `build-kits`. The AIX build-kit is implemented, as much as possible, as a custom XML file that can be applied using `aixpert`.

The benchmark recommendations include `CLI` (command-line interface) commands that can be used to guide an implementation of this benchmark *without* using `aixpert`.

The remainder of this section is a table showing functions that are common to both the CIS and HLS (IBM AIX High Level Security) profiles as well as functions unique to either CIS or IBM AIX.

Unlike the previous AIX benchmarks the default values of the traditional IBM provided profiles will no longer be listed under the heading *Additional Information*. That information is provided via the following table.

2.5 Applying the CIS Policy

Prior to implementing the AIX Security Expert customized settings, please review the benchmark recommendations. If there are any settings that need to be altered from a CIS recommended value, e.g., based on environmental requirements, edit the XML file using a text editor such as the `vi` command.

As much as possible the guide has been automated based on the AIX Security Expert HLS policy. Some of these settings have been altered from an IBM guideline to a CIS (consensus) value. Further, recommendations normally outside the scope of the HLS policy have been added. These instances either use the standard `aixpert` commands or a special `aixpert` script (`execcmds`) for executing commands otherwise unavailable to `aixpert` allowing (nearly) all the recommendations to be applied using `aixpert`.

- CIS Members can use the XML file provided in the build-kit to automatically apply (nearly) all of the AIX Security Expert managed settings from this benchmark.
- Non-CIS Members can get an approximate starting point by executing the following command to extract the high profile. Thereafter the profile will need to be edited using your favorite editor (if not `vi`).

NOTE: The use of the supplied AIX Security Expert Customized XML file is purely optional, as there is remediation guidance provided with each recommendation in this benchmark.

Installing the build-kit

- this will become an installp package with VRMF numbering, what follows, for now, are the old instructions

The absolute path tar file can be extracted via the following command:

```
tar -xvf <PATH to tar file>/CIS_IBM_AIX_7.1_Benchmark_v1.0.0_AIXPERT_7.1.tar
```

This will place the customized XML file into its default location:

```
/etc/security/aixpert/custom/custom_7.1.xml.
```

Review recommendation before applying the settings

Once the recommendations have been reviewed the profile can be applied as follows:

```
# aixpert -f /etc/security/aixpert/custom/custom_7.1.xml
```

Checking system against applied settings

The collective applied settings, regardless of source are kept in the following file:

`/etc/security/aixpert/core/appliedaixpert.xml`.

At any time the current settings of the system can be validated against what `aixpert` believes are the applied settings using:

```
# aixpert -c
```

This command (no additional arguments) compares the settings, defined in the `appliedaixpert.xml` file, to those currently set on the system. Any deviation from these standards i.e. a setting has been changed, it will be reported in the following log file:

`/etc/security/aixpert/check_report.txt`. A summary of the results is provided to `stdout`.

- Any deviations can be corrected manually, or the AIX Security Expert Customized XML file can be re-applied.

3 AIX Recommendations

This section provides details of the recommended settings.

CIS Members can use the AIX `build-kit` that includes an XML file that can be applied using the `aixpert` command to both apply (with the `-f` argument) or verify (using the `-c -p` arguments).

Align with CIS Controls v8

This benchmark reorganizes the recommendations into sections based on CIS Controls v8. Prior AIX benchmarks were closely aligned with the way `aixpert` grouped it's recommendations. Simply put, the organization of the recommendations is "Control"->"Tool|Command" (aka top-down) rather than "Tool command"->recommendation (aka bottom-up) driven.

Excerpts from CIS Controls v8

CIS Controls® started as a simple grassroots activity to identify the most common and important real-world cyber-attacks that affect enterprises every day, translate that knowledge and experience into positive, constructive action for defenders, and then share that information with a wider audience.

The CIS Controls reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.), who have banded together to create, adopt, and support the CIS Controls.

Guiding principles

CIS Controls v8 used a number of design principles. These served as to remind the community of what is really important and of the goals of the CIS Controls. Several of these design principles were copied or borrowed to help reshape 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

3.1 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: Account Management](#)

3.1.1 Local Identification Management

This sub-section has recommendations for managing local accounts: focus here is controls that manage local accounts.

The relevant CIS Controls are:

- 5.1 Establish and Maintain an Inventory of Accounts
- 5.3 Disable Dormant Accounts
- 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts
- 5.5 Establish and Maintain an Inventory of Service Accounts (IG2)

3.1.1.1 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:

```
PID=$$
now=$(date -u +"%s")
umask 077
/usr/bin/egrep -p "password = +$" /etc/security/passwd | grep ":" | awk -F:
'{ print $1 } ' >/var/tmp/nopd.${PID}
/usr/bin/egrep "(:|:|^!|:)[[:digit:]]+:[[:digit:]]+:" /etc/passwd | awk -F:
'{ print $1 } ' >>/var/tmp/nopd.${PID}
test -z /var/tmp/nopd.${PID}
if [[ -s /var/tmp/nopd.${PID} ]]; then
    sort -u /var/tmp/nopd.${PID} | while read user rest; do
        print "Account '${user}' is missing an adequate password."
        # While command below is remediation, you may want to activate it,
        # especially for blank passwords.
        # /usr/bin/chuser account_locked='true' ${user}
    done
    print "## cut/paste commands for 'after the audit' remediation, note
    addition of expires as of ${now}"
    sort -u /var/tmp/nopd.${PID} | while read user rest; do
        print "/usr/bin/chuser account_locked='true' expires=${now} ${user}"
    done
    print "## End of cut/paste commands for 'after the audit' remediation"
fi
rm -f /var/tmp/nopd.${PID}
```

- The command should not yield output.
- Note: If there is output, it also contains a list of chuser commands that can be executed asap, to lock and expire associated accounts.

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.
- Check for accounts with an incorrect password field in `/etc/passwd`. If any, lock and expire those accounts.

```
umask 077
PID=$$
# get seconds since epoch
now=$(date +%s")
set $(/usr/bin/egrep -c -p "password = +" /etc/security/passwd)
if [[ $1 != "0" ]]; then
    # copy everything except entries without password
    /usr/bin/egrep -v -p "password = +" /etc/security/passwd >
/etc/security/passwd.cis.${PID}
    # 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' ${user}
        printf "%s:\n\tpassword = *\n" ${user} >>
/etc/security/passwd.cis
        printf "\tflags = ADMCHG\n\tlastupdate=%s\n\n" ${now} >>
/etc/security/passwd.cis
    done
    cat /etc/security/passwd.cis.${PID} > /etc/security/passwd
    rm /etc/security/passwd.cis.${PID}
fi
/usr/bin/egrep "(:|:|^!|:)[[:digit:]]+:[[:digit:]]+:" /etc/passwd | awk -F:
'{ print $1 } ' | \
while read user; do
    print "Locking account '${user}' due to incorrect password field in
/etc/passwd."
    /usr/bin/chuser account_locked='true' expires=${now} ${user}
done
```

Default Value:

N/A

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.			

3.1.1.2 All user id's 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.

Rationale:

The only user with a UID of 0 on the system must be the root user. Any account with a UID of 0 has super user privileges on the system and is effectively root. All access to the root account should be via `su` or `sudo` to provide an audit trail. All other users must also have a unique UID to ensure that file and directory security is not compromised.

Audit:

Re-run the command:

```
cut -d: -f 3 /etc/passwd |sort -n |uniq -d
```

The command above should not yield output

Remediation:

Examine the user IDs of all configured users:

```
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 username/s:

```
cut -f "1 3" -d : /etc/passwd |grep ":<UID>$"
```

NOTE: Any user 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 <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.			

3.1.1.3 All group id's 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:

Re-run the command:

```
cut -d: -f 3 /etc/group |sort -n |uniq -d
```

The command above should not yield output

Remediation:

Ensure that all group IDs are unique:

```
cut -d: -f 3 /etc/group |sort -n | uniq -d
```

If a number, or numbers are returned from the command above, these are GID which are not unique within the `/etc/group` file. Determine the effected group names:

```
cut -f "1 3" -d : /etc/group |grep ":<GID>$"
```

NOTE: Any group names returned should either be deleted or have the UID changed
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.			

3.1.2 Password Controls - Local Registry

This section provides guidance on the configuration of the user attributes that affect password policy. (See CIS Control 5.2: Use Unique Passwords)

Password policy attributes includes recommended length, complexity, reuse and expiration.

Other User attributes

Other attributes manage user/application values *after* a successful login. These attributes include `ulimits`, `umask`, `rlogin` and more. Including password controls - there are approximately 65 user attributes.

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 user management is to not set any of these values explicitly - unless there is a specific requirement to override a default.

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.

3.1.2.1 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=26
```

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=26
```

This means that a user will not be able to reuse any password set in the last 26 weeks.

Default Value:

Not set

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.			

3.1.2.2 *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.

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=20
```

Remediation:

In `/etc/security/user`, set the default user stanza `histsize` attribute to be (greater than or) equal to 20:






```
chsec -f /etc/security/user -s default -a histsize=20
```

This means that a user may not reuse any of the previous 20 passwords.

Default Value:

No limit

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.			

3.1.2.3 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	4.10 <u>Enforce Automatic Device Lockout on Portable End-User Devices</u> 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.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

3.1.2.4 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 <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.			

3.1.2.5 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.			
v7	16.9 <u>Disable Dormant Accounts</u> Automatically disable dormant accounts after a set period of inactivity.			

3.1.2.6 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.			

3.1.2.7 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=0
```

Remediation:

In `/etc/security/user`, set the default user stanza `minage` attribute to 1:






```
chsec -f /etc/security/user -s default -a minage=0
```

This means that a user can change their password at any time.

Default Value:

`minage=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.			

3.1.2.8 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=2
```

Remediation:

In `/etc/security/user`, set the default user stanza `minalpha` attribute to be greater than or equal to 2:






```
chsec -f /etc/security/user -s default -a minalpha=2
```

This means that there must be at least 2 alphabetic characters within a password.

Default Value:

`minalpha=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.			

3.1.2.9 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.			

3.1.2.10 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 <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.			

3.1.2.11 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.			

3.1.2.12 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 <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.			

3.1.2.13 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=2
```

Remediation:

In `/etc/security/user`, set the default user stanza `minother` attribute to be greater than or equal to 2:






```
chsec -f /etc/security/user -s default -a minother=2
```

This means that there must be at least 2 non-alphabetic characters within a password.

Default Value:

```
default minother=2
```

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.			

3.1.2.14 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 <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.			

3.1.2.15 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=1
```

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.			

3.1.3 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.

3.1.3.1 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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.2 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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.3 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>4.6 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>4.7 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.			

3.1.3.4 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.			
v7	<u>4.6 Use of Dedicated Machines For All Administrative Tasks</u> Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			

3.1.3.5 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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.6 *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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.7 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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.8 *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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.9 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	<p><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></p> <p>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.</p>			
v7	<p><u>4.6 Use of Dedicated Machines For All Administrative Tasks</u></p> <p>Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.</p>			

3.1.3.10 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.			
v7	<u>4.6 Use of Dedicated Machines For All Administrative Tasks</u> Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			

3.1.4 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.

3.2 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 [CIS Controls v8: Access Control Management](#)

3.2.1 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)

3.2.1.1 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	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.			

3.2.2 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).

3.2.2.1 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	5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v7	4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

3.2.2.2 Ensure sudo log file is active (Manual)

Profile Applicability:

- Level 2

Description:

sudo can use a custom 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:

A sudo log file simplifies auditing of sudo commands

Audit:

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` and add the following line: and add the following line:

```
Defaults logfile="<PATH TO CUSTOM LOG FILE>"
```

Example:

```
Defaults logfile="/var/log/sudo.log"
```

CIS Controls:

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

3.2.2.3 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` 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™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

3.2.3 Special Permissions Management - suid, sgid, acl, and trusted-bit files and programs (Manual)

Profile Applicability:

- Level 2

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	<u>3.3 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	<u>14.6 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.			

3.2.4 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.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

3.2.5 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 <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™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

3.2.6 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.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

3.2.7 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 <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™.			
v7	8.3 <u>Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies</u> Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.			

3.3 Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

See [CIS Controls v8: Network Infrastructure Management](#)

The sub-sections below are divided into `boot` related (or Initial Program Load - IPL):

- `inittab` (called by `rc.boot` phase 3) and is comparable to **SYSV** `sysctl` like mechanisms (there is an entry in `inittab` that calls `/etc/rc.d/rc2.d/S*` scripts)
- `rc.tcpip` (called by `inittab`) and manages the activation of most of the `src` (System Resource Controller) managed services and daemons.
- IPv6 is a separate section (called, if used, by `rc.tcpip`) as most locations do not yet use IPv6. Make sure it is not activated if you are not pursuing IPv6 in your environment.
- `inetd.conf`: this section is not boot (IPL) related - other than the `inetd` service is initiated via `rc.tcpip`. There is a good chance that none of these services are needed. If they are needed, `inetd` provides the service on-demand
- NFS: These are recommendations that may be relevant if you are running an NFS server. The script `/etc/rc.nfs` (called via `/etc/inittab`) activates the NFS services that these recommendations cover. **NOTE:** On AIX, even if all these supporting programs are stopped the kernel still supports NFS client activity. If all NFS activity must be stopped you will need a host-based firewall to block the related port(s).

3.3.1 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).

Additional Information

- During the review three additional daemons have been identified: `pconsole`, `naudio`, and `naudio2`.
- The sound related daemons are installed if you install all drivers. Our instructions or example installation (which will be re-written as a recommendation in the AIX 7.2 benchmark) included the comment to *NOT* install all drivers.
- A separate recommendation will be added in the next release to de-install `pconsole`.

3.3.1.1 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.			

3.3.1.2 dt (Automated)

Profile Applicability:

- Level 2

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	<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.			

3.3.1.3 piobe (Automated)

Profile Applicability:

- Level 2

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	<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.			

3.3.1.4 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.			

3.3.1.5 rcnfs (Automated)

Profile Applicability:

- Level 2

Description:

The `rcnfs` entry starts the NFS daemons during system boot.

Rationale:

NFS is a service with numerous historical vulnerabilities and should not be enabled unless there is no alternative. If NFS serving is required, then read-only exports are recommended and no filesystem or directory should be exported with root access. Unless otherwise required the NFS daemons will be disabled.

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
```

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.			

3.3.1.6 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:

```
(lsllpp -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):

```
lsllpp -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.			

3.3.2 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](#).

3.3.2.1 Disable *ntalk*/*talk*/*write* (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to block `talk` and `write`. This allows connected users to chat within terminal sessions.

Rationale:

The recommendation is to block attempts to use the `write` or `talk` commands. This improves the security of the `tty` device.

However, there are two exceptions:

1. The super user can write to anyone
2. If you are logged in as the same user who has turned the messages off, you can write to the super user

Audit:

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

```
lssrc -s inetd -l | grep -c talk
lssrc -s writesrv | grep -c active
```

NOTE: Both commands should return the string 0

Remediation:





Disable `talk` and `write`.

```
rmitab writesrv
/usr/sbin/chsubserver -r inetd -C /etc/inetd.conf -d -v 'ntalk' -p 'udp'
/usr/sbin/chsubserver -r inetd -C /etc/inetd.conf -d -v 'talk' -p 'udp'
for daemon in /usr/sbin/talkd /usr/sbin/writesrv; do
  chmod a-rwx ${daemon}
  trustchk -u ${daemon} mode
done
```

Default Value:

`ntalk` and `writesrv` are 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.			

3.3.2.2 aixmibd (Automated)

Profile Applicability:

- Level 2

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. If `snmpd` is not required, it is recommended that it is disabled.

The `aixmibd` 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=aixmibd-daemon>

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d aixmibd
```

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.			

3.3.2.3 *dhcpcd* (Automated)

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d dhcpcd
```

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.			

3.3.2.4 *dhcprd* (Automated)

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d dhcprd
```

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.			

3.3.2.5 *dhcpcsd* (Automated)

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d dhcpcsd
```

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.			

3.3.2.6 dpid2 (Automated)

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





In `/etc/rc.tcpip`, comment out the `dpid2` entry:

```
chrctcp -d dpid2
```

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.			

3.3.2.7 *gated* (Automated)

Profile Applicability:

- Level 2

Description:

This entry starts the `gated` daemon 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 communicating 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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d gated
```

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.			

3.3.2.8 *hostmibd* (Automated)

Profile Applicability:

- Level 2

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:

```
lssrc -g tcpip | grep hostmibd | grep active | wc -l
```

The above command should yield the following output:

```
0
```

Remediation:





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

```
chrc tcp -d hostmibd
stopsrc -s hostmibd
```

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.			

3.3.2.9 *inetd* - aka Super Daemon (Automated)

Profile Applicability:

- Level 1

Description:

When none of 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 `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	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.			

3.3.2.10 *mrouted* (Automated)

Profile Applicability:

- Level 2

Description:

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

Rationale:

The `mrouted` daemon is an implementation of the multicast routing protocol. It is recommended that this daemon is disabled, unless the server is functioning as a multicast router.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d mrouted
```

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.			

3.3.2.11 *named (Automated)*

Profile Applicability:

- Level 2

Description:

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.

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d named
```

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.			

3.3.2.12 portmap (Automated)

Profile Applicability:

- Level 2

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` is inactive:

```
set $(lssrc -s portmap | tail -1)

if [ $# -eq 4 ] ; then
print $1 is $4 with PID $3
print Active RPC programs needing portmap are:
rpcinfo -p localhost
fi
```

The above command should not have any output.

Remediation:

- Review any active RPC services:

```
rpcinfo -p localhost
```

NOTE: If there are active RPC services and the services are required, do not disable portmap.

- Disable portmap if there are no active or required RPC services:

```
chrctcp -d portmap  
stopsrc -s portmap
```

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	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.			

3.3.2.13 *routed* (Automated)

Profile Applicability:

- Level 2

Description:

This entry starts the `routed` daemon at 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.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d routed
```

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.			

3.3.2.14 rwhod (Automated)

Profile Applicability:

- Level 2

Description:

This entry starts the `rwhod` daemon at 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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d rwhod
```

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.			

3.3.2.15 *sendmail (Automated)*

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d sendmail
```

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.			

3.3.2.16 *snmpd (Automated)*

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d 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.			

3.3.2.17 snmpmibd (Automated)

Profile Applicability:

- Level 2

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
```

The above command should yield the following output:

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

Remediation:

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

```
chrctcp -d snmpmibd
```





Default Value:

Uncommented

References:

1. <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.			

3.3.2.18 *timed* (Automated)

Profile Applicability:

- Level 1

Description:

This entry starts the `timed` daemon at system startup. This is the old, read 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
```

The above command should yield the following output:

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

Remediation:





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

```
chrctcp -d 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.			

3.3.3 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`

3.3.3.1 *autoconf6 (Automated)*

Profile Applicability:

- Level 2

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>4.8 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.			

3.3.3.2 *ndpd-host (Automated)*

Profile Applicability:

- Level 2

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:deed:beef:fef7:6204	105190883		0	49267729		
1	0							
en0	1492	fe80::deed: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	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.			

3.3.3.3 *ndpd-router (Automated)*

Profile Applicability:

- Level 2

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	<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.			

3.3.4 *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., `inetd` services) 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.

3.3.4.1 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.			

3.3.4.2 *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	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.			

3.3.4.3 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	<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>			

3.3.4.4 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	<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.			

3.3.4.5 *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	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.			

3.3.4.6 *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.			
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.			

3.3.4.7 *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	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.			

3.3.4.8 *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.			
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.			

3.3.4.9 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.			
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.			

3.3.4.10 *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.			
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.			

3.3.4.11 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	<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.			

3.3.4.12 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	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.			

3.3.4.13 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.			
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.			

3.3.4.14 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	<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.			

3.3.4.15 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 telnet is disabled. This service can be performed securely using OpenSSH.

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 `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.			
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.			

3.3.4.16 *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.			
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.			

3.3.4.17 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	<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>			

3.3.4.18 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	<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>			

3.3.4.19 *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.			
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.			

3.3.4.20 *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.			
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.			

3.3.4.21 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	<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>			

3.3.4.22 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	<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>			

3.3.4.23 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	<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.			

3.3.4.24 *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	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.			

3.3.4.25 *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	<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.			

3.3.4.26 *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	<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.			

3.3.4.27 *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.			
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.			

3.3.4.28 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.			
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.			

3.3.4.29 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.			
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.			

3.3.4.30 *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.			
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.			

3.3.4.31 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	<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>			

3.3.5 NFS

During the implementation of the default customized aixpert XML file, NFS services will have been disabled as the `/etc/rc.nfs` startup file will have been removed from `/etc/inittab`.

The first recommendation in this section is to de-install NFS to complete the lockdown of this service. However, if the server acts as either an NFS server or NFS client there are further security recommendations to implement.

3.3.5.1 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:

```
lsrpm -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

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.			

3.3.5.2 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
```







NOTES:

- The NFS mount needs is re-mounted automatically by chnfsmnt.
- The second loop might not do anything as both loops set both `nosuid (-y)` and `nodev (-z)`

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.			
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.			

3.3.5.3 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

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.			

3.3.5.4 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.

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

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.			

3.3.5.5 NFS - no root access via NFS exports (Automated)

Profile Applicability:

- Level 1

Description:

The `superuser` (`euclid==0`) should not be able to modify file system objects as a client of an NFS server. Thus, 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 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.

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.			

3.3.5.6 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
```

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.			

3.4 Network Monitoring and Defense

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.

See [CIS Controls v8: Network Monitoring and Defense](#)

Why Is This Control Critical?

We cannot rely on network defenses 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 currently limited to the hardening of standard TCP/IP tuning parameters using the command `no` (network options). These settings can help mitigate risks such as SYN, source routing and smurf attacks. As the control implies - this is meant to be a second line defense as we expect that firewalls will also be configured to safeguard against these types of attack.

3.4.1 *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

3.4.2 *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

3.4.3 *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

3.4.4 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

3.4.5 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

3.4.6 *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

3.4.7 *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

3.4.8 *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

3.4.9 ipsrouterecv (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsrouterecv` parameter determines whether the system accepts source routed packets.

Rationale:

The `ipsrouterecv` 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 "ipsrouterecv[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrouterecv = 0
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrouterecv` entry:

```
no -p -o ipsrouterecv=0
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

3.4.10 *ipsroutese*nd (Automated)

Profile Applicability:

- Level 1

Description:

The `ipsroutese`nd parameter determines whether or not the system can send source-routed packets.

Rationale:

The `ipsroutese`nd 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 "ipsroutese
```

The above command should yield the following output:

```
ipsroutese
```

Remediation:

In `/etc/tunables/nextboot`, add the `ipsroutese`nd entry:

```
no -p -o ipsroutese
```

This makes the change permanent by adding the entry into `/etc/tunables/nextboot`

Default Value:

1

3.4.11 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

3.4.12 *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

3.4.13 *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

3.4.14 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

3.4.15 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

3.4.16 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`

3.4.17 *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

3.5 Data Protection

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

See: [CIS Controls v8: Data Protection](#)

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 multinational 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.

3.5.1 Encrypted Filesystems (EFS)

Another enhancement of AIX 6.1 is the introduction of Encrypted Filesystems. This enables an individual user, via keystore files, to encrypt their own data within a `jfs2` filesystem. After creating EFS enabled filesystems, individual files can be encrypted or inheritance can be set at the filesystem or directory level. The standard AIX data and user management commands have been modified to work with encryption.

There are a number of reasons for encrypting data in this manner, perhaps to send backups of data off site, or to encrypt sensitive or confidential information such as payroll details.

3.5.1.1 EFS - implementation (Automated)

Profile Applicability:

- Level 2

Description:

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

Rationale:

The use of EFS further 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:

```
lslpp -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/instl/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 files:

```
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.			

3.5.2 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.			

3.5.3 General Permissions Management - world writable directories (Manual)

Profile Applicability:

- Level 1

Description:

The system is audited for world writable directories.

Rationale:

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.			
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.			

3.5.4 General Permissions Management - world writable files (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. Files should only be world writable when absolutely necessary.

Audit:

Re-execute the appropriate `find` command.

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

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

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:

Reversion:

To reinstate world writable permission:

```
chmod o+w <dir or file>
```

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.			

3.5.5 Ensure no unowned files or directories exist (Automated)

Profile Applicability:

- Level 1

Description:

Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups.

Rationale:

A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Audit:

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
```

If all non-local filesystems have been un-mounted:

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

The `find` command should not yield output

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 command 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
```

If all non-local filesystems have been un-mounted:

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

NOTE: An un-owned file or directory is referred to via the GID or UID as it cannot be translated to a user or group name in `/etc/group` or `/etc/passwd`. This is typically caused by removing users or groups from the system.







Remediate the un-owned file and directory list:

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

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.			
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.			

3.6 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 <https://workbench.cisecurity.org/benchmarks/6480/sections/698296>

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.

3.6.1 Common Desktop Environment (CDE)

During the implementation of the default customized aixpert XML file, CDE will have been disabled as the `/etc/rc.dt` startup file will have been removed from `/etc/inittab`.

CDE has a history of security problems and should remain disabled. However, if the server has a graphics adapter and CDE is used then the recommendations in this section should be followed to enhance security. If CDE is not required and the filesets are installed, is recommended that the filesets are de-installed to avoid exposure to potential security vulnerabilities.

3.6.1.1 CDE - de-installing CDE (Automated)

Profile Applicability:

- Level 2

Description:

The recommendation is to de-install CDE 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:

```
lsbpc -L |grep -i CDE
```

The above command should yield no output.

Remediation:

Identify if CDE is already installed:

```
lsbpc -L |grep -i CDE
```

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 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>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.			

3.6.1.2 /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

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>			
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>			

3.6.1.3 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.			
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.			

3.6.1.4 /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	<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.			

3.6.1.5 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

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.			

3.6.1.6 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.			
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.			

3.6.1.7 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.			
v8	<u>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</u> 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.			

3.6.1.8 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

3.6.1.9 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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 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	<u>14.6 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.			

3.6.1.10 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

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.			

3.6.1.11 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

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.			

3.6.2 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 of the benchmark will focus on the installation and configuration of SSH. Some of the parameters specified in this section are default values, but explicit declaration is preferred, to ensure that these recommendations remain constant over time.

3.6.2.1 OpenSSH - Installation (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) -gt 8 && 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	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	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.			

3.6.2.2 OpenSSH - PermitRootLogin (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 (using password) was enabled by default with prior versions of OpenSSH. To be absolutely certain direct login using a password is disabled *the recommendation is to set this variable specifically* rather than rely on a new, changeable, default. In other words, never rely on default values!!!

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.

Accountability can be achieved using PKI keys and sufficient log information to syslog.

Impact:

One setting would be to block all root access (by assigning the value `no` to *PermitRootLogin*). 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.

Considering the recommendation **3.2.6.9 - Configuring SSH - set LogLevel to INFO** specifies a `LOG_LEVEL` of `INFO` or `DEBUG` a setting of `prohibit-password` is acceptable. In short, unless `no` is required by local corporate policy the preferred setting is to disable root login using a password and verify that OpenSSH logging is at least at level `INFO`.

See Additional Info for an example of how root login can be accounted.

Note: only public keys in the file `~root/.ssh/authorized_keys` will be able to connect.

Audit:

- This audit procedure verifies that the setting for `PermitRootLogin` is not dependent upon a default that might be acceptable today, but not later. That is, our recommendation requires an explicit setting.
- 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
```

- Consider *no output* as a configuration failure

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).
- Man Page extract







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.

- To resolve *accountability* for who is logging in as `root` using `publickey` authentication 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
```

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.			
v7	<u>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

3.6.2.3 OpenSSH - Banner (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

3.6.2.4 Ensure SSH IgnoreRhosts is enabled (Automated)

Profile Applicability:

- Level 1

Description:

The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files will not 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 is fundamentally insecure as the local system can 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 have been known and exploited for a long time. Since this authentication method is not secure, it must be disabled.

Audit:

Ensure that the `IgnoreRhosts` parameter has been changed:

```
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	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.			

3.6.2.5 Ensure SSH PermitEmptyPasswords is disabled (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	6.5 <u>Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	16.3 <u>Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

3.6.2.6 Configuring SSH - disallow host based authentication (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that host-based authentication is disallowed.

Rationale:

Using host-based authentication, any user on a trusted host can log into another host on which this feature is enabled. Since this feature depends only on system authentication and not on user authentication, it must be disabled.

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>6.5 Require MFA for Administrative Access</u> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			
v7	<u>16.3 Require Multi-factor Authentication</u> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.			

3.6.2.7 Configuring SSH - removal of .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.

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.			

3.6.2.8 Configuring SSH - removal of `/etc/shosts.equiv` (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to remove the `/etc/shosts.equiv` file.

Rationale:

The existence of a `/etc/shosts.equiv` file, 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 `/etc/shosts.equiv` file has been successfully removed:

```
ls /etc/shosts.equiv
```

The above command should yield no output.

Remediation:

Review the content of the `/etc/shosts.equiv` file:

```
cat /etc/shosts.equiv
```

If the file exists:

```
rm /etc/shosts.equiv
```

Default Value:





N/A

Additional Information:

Reversion:

The `/etc/shosts.equiv` file would need to be restored from a backup.

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>			
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>			

3.6.2.9 Configuring SSH - set LogLevel to INFO or VERBOSE (Automated)

Profile Applicability:

- Level 1

Description:

The `INFO` parameter specifies that record login and logout activity will be logged.

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.

Audit:

Ensure that the `LogLevel` parameter is set to `INFO`:

```
grep "^LogLevel[[:blank:]]" /etc/ssh/sshd_config
```

The above command should yield one of the following output:

```
LogLevel INFO
LogLevel VERBOSE
```

Remediation:

- Edit the `/etc/ssh/sshd_config`:

```
vi /etc/ssh/sshd_config
```

- Set:

```
LogLevel INFO
```

or

```
LogLevel VERBOSE
```

- Re-cycle the `sshd` daemon to pick up the configuration changes:







```
stopsrc -s sshd
sleep 5
startsrc -s sshd
```

Additional Information:

- To resolve *accountability* for who is logging in as `root` using `publickey` authentication together with **LogLevel INFO** remember that AIX syslog must also be configured to provide `.info` level for the facility chosen (default is `auth`).
- For example: `auth.info /var/log/syslog/auth.log rotate size 1m files 4`
- Properly configured provides the following `syslog` information showing the fingerprint of the key used to access an account:

```
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
```

CIS Controls:

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

3.6.2.10 OpenSSH - configure sftp-server (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 VERBOSE
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	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.			

3.6.2.11 OpenSSH: Ensure MaxAuthTries is set to 4 or less (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
```


3.6.2.12 OpenSSH: Ensure only strong ciphers are used (Automated)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Based on research conducted at various institutions, it was 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.

Audit:

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

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

Weak Ciphers:

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

Remediation:

Edit the `/etc/ssh/sshd_config` file 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:

```
stopsrv -s sshd  
startsrv -s sshd
```

Default Value:

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

References:





1. For more information on the Counter mode algorithms, read RFC4344 at <http://www.ietf.org/rfc/rfc4344.txt>.

Additional Information:

German (language) regulations on configuring OpenSSH:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-4.pdf?__blob=publicationFile&v=2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

3.6.2.13 Ignore user-provided environment variables (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)

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:

```
stopsrc -s sshd  
startsrc -s sshd
```

3.6.2.14 OpenSSH: Regulate access to server (Manual)

Profile Applicability:

- Level 1

Description:

There are several options available to regulate access to a server via OpenSSH. At least of the following options needs to be leveraged:

- **AllowUsers:** The `AllowUsers` variable specifies which users may `ssh` into the system. The list is `user names` separated by spaces. *Numeric userIDs* are not recognized with this variable. Access can be narrowed to restrict user access from a specific host using the form `user@host`.
- **AllowGroups:** The `AllowGroups` variable specifies groups of users who are permitted to `ssh` into the system. The list is `group names` separated by spaces. *Numeric groupIDs* are not recognized with this variable.
- **DenyUsers:** The `DenyUsers` variable specifies specific users who may not `ssh` into the system. The list is `user names` separated by spaces. *Numeric userIDs* are not recognized with this variable. Access can be narrowed to restrict user access from a specific host using the form `user@host`.
- **DenyGroups:** The `DenyGroups` variable specifies groups of users who are not permitted to `ssh` into the system. The list is `group names` separated by spaces. *Numeric groupIDs* are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

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 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:

```
stopsrv -s sshd
startsrc -s sshd
```

Default Value:

All users from any host are permitted.

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.			

3.6.3 Sendmail Configuration

During the implementation of the default customized aixpert XML file the `sendmail` daemon will have been disabled. However, if the `sendmail` service is active and required in the environment, the recommendations in this section should be applied.

3.6.3.1 /etc/mail/sendmail.cf - SmtpgreetingMessage (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to change the default `sendmail` greeting string to not display the `sendmail` version and other related information.

Rationale:

The `sendmail` daemon has a history of security vulnerabilities. The recommendation is to change the default `sendmail` greeting string so as not to display the `sendmail` version and other related information, which can be used by an attacker for fingerprinting purposes.

Audit:

Validate the installation of the software:

```
grep "SmtpgreetingMessage=mailerready" /etc/mail/sendmail.cf
```

The above command should yield the following output:

```
O SmtpgreetingMessage=mailerready
```

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 SmtpgreetingMessage=$j Sendmail $b
```

With:

```
O SmtpgreetingMessage=mailerready
```

Default Value:

SmtpGreetingMessage=\$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
```

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.			

3.6.3.2 /etc/mail/sendmail.cf - permissions and ownership (Automated)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership 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 /etc/mail/sendmail.cf
```

Default Value:

```
-rw-r--r-- root system sendmail.cf
```

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.			

3.6.3.3 /var/spool/mqueue - permissions and ownership (Automated)

Profile Applicability:

- Level 1

Description:

The recommended permissions and ownership for the `/var/spool/mqueue` directory are applied.

Rationale:

The `sendmail` daemon generally 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.

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
```

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.			

3.6.4 Login Controls: /etc/security/login.cfg

The file `/etc/security/login.cfg` manages several settings for managing the login process.

3.6.4.1 /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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>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.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

3.6.4.2 /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

3.6.4.3 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

3.6.4.4 /etc/security/login.cfg - 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:

Ensure that all running applications support SHA512 password encryption

Audit:

From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm
```

The above command should yield the following output:

```
usw pwd_algorithm=ssha512
```

Remediation:

In the file `/etc/security/login.cfg` set the `usw` stanza attribute `pwd_algorithm` to `ssha512`:

```
chsec -f /etc/security/login.cfg -s usw -a pwd_algorithm=ssha512
```





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	3.11 <u>Encrypt Sensitive Data at Rest</u> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.			

3.6.5 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.

3.6.5.1 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](#)

3.6.5.1.1 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 should 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	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.			

3.6.5.1.2 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 should 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.			
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.			

3.6.5.1.3 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<u>4.8 Log and Alert on Changes to Administrative Group Membership</u> Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.			
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.			

3.6.5.1.4 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
```

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.			

3.6.5.2 SNMP

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.

3.6.5.2.1 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
```

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.			

3.6.5.2.2 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
```

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.			

3.6.5.2.3 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
```

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.			

3.6.5.2.4 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
```

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.			

3.6.5.2.5 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
```

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.			

3.6.5.3 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

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.			

3.6.5.4 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

3.6.5.5 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

3.6.5.6 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	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.			

3.6.6 Service Accounts

This (sub)-section focuses on CIS Control:

- Establish and Maintain an Inventory of Service Accounts

Note: Currently this section is limited to the *service* `ftpd`. Additional services will be added in following releases. Additional candidates for recommendations include: `sshd`, `srvproxy`, `esaadmin`, `ipsec`, and `nuucp` - even those these accounts are also locked (for login/command-line access).

This is to distinguish between services that run under a non-root userid (i.e, *service account* and services that run as `root` (*services*).

Note: `ftp` can be either a **service** - as some locations run `ftpd` as `root`, while others have `ftp` as a **service account** and create a separate `ftp` account name and put this in a `chroot` environment.

3.6.6.1 FTP: Prevent world access and group write to files (Automated)

Profile Applicability:

- Level 1

Description:

The umask of the `ftp` 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 `ftp` 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	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.			

3.6.6.2 FTP: Display acceptable usage policy during login (Automated)

Profile Applicability:

- Level 1

Description:

Set an `ftp` 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 `ftp` 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:

```
dspscat -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.

Additional Information:

- Another way to install a banner is to create `/etc/ftpaccess.ctl` with the following contents:

herald: /etc/ftp_banner

Then create the file `/etc/ftp_banner` and write something to it. The banner appears before authentication:

```
print "Authorized uses only. All activity may be monitored and reported."
>/etc/ftp_banner

chmod a-wx /etc/ftp_banner
```

ftp localhost

Connected to loopback. 220-Authorized uses only. All activity may be monitored and reported. 220 aix71tl5sp3 FTP server (Version 4.2 Fri Apr 6 19:34:30 CDT 2018) ready.
Name (localhost:root):

3.6.6.3 FTP: Disable root access to ftp (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>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>4.3 Ensure the Use of Dedicated Administrative Accounts</u> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

3.6.7 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`.

3.6.7.1 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
```

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

3.6.8 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.

3.6.8.1 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.

3.6.8.1.1 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	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.			

3.6.8.1.2 Home directory must deny write to all except owner (Manual)

Profile Applicability:

- Level 1

Description:

All user home directories must not have group write or world writable access.

Rationale:

Group or world-writable user home directories may enable malicious users to steal or modify data, or to gain other user's system privileges. Disabling read and execute access for users, who are not members of the same group, allows for appropriate use of discretionary access control by each user.

Impact:

Should have minimal impact as the default already excludes group and other (world) write access. If many different groups are used (i.e., more than 'staff') there may be some impact if users in different groups are used to sharing files via their home directories.

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; locking account named [%s]\n"
            ${home} ${name}
            chuser -R files account_locked=true $name
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            /usr/bin/perl -e '$f=$ARGV[0]; $m=((stat $f)[2] & 0022); \
            printf("%s has group or world write mode::", $f) if $m; exit($m)'
            ${home} \
            || ls -led ${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. Also, if the **HOME** directory has already been defined to something *special* (here, `/dev/null`) no audit is performed.

Remediation:

Change any home directories which have group or world writable access:

```
#!/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; locking account named [%s]\n"
            ${home} ${name}
            chuser -R files account_locked=true $name
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            /usr/bin/perl -e '$f=$ARGV[0]; $m=((stat $f)[2] & 0022); exit($m)'
            ${home} \
                || chmod og-w ${home}
        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	<u>3.3 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	<u>14.6 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.			

3.6.8.1.3 /audit (Automated)

Profile Applicability:

- Level 1

Description:

The `/audit` directory holds the output produced from the audit subsystem.

Rationale:

The `/audit` directory stores the audit output files. This directory must have adequate access controls to prevent unauthorized access.

Audit:

Validate the permissions of `/audit`:

```
ls -ld /audit | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---  root  audit  /audit
```

Remediation:







Ensure correct ownership and permissions are in place for `/audit`:

```
chown root:audit /audit
chmod u=rwx,g=rx,o= /audit
chmod -R u=rw,g=r,o= /audit/*
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>3.3 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	<u>14.6 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.			

3.6.8.1.4 /etc/security (Automated)

Profile Applicability:

- Level 1

Description:

This `/etc/security` directory contains the user and group configuration files and the encrypted passwords.

Rationale:

The `/etc/security` directory contains sensitive files such as `/etc/security/passwd`, `/etc/security/group`. It must be secured from unauthorized access and modifications.

Audit:

Validate the permissions of `/etc/security`:

```
ls -ld /etc/security | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxr-x---  root  security  /etc/security
```

Remediation:







Remove world read, write and execute access and group write access from `/etc/security`:

```
chown -R root:security /etc/security
chmod u=rwx,g=rx,o= /etc/security
chmod -R go-w,o-rx /etc/security
```

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.			
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.			

3.6.8.1.5 /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	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.			

3.6.8.1.6 /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	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.			

3.6.8.1.7 /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	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.			

3.6.8.1.8 /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	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.			

3.6.8.2 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
```


3.6.8.2.1 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>3.3 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	<u>14.6 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.			

3.6.8.2.2 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	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.			

3.6.8.2.3 /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	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.			

3.6.8.2.4 /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	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.			

3.6.8.2.5 /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	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.			

3.6.8.2.6 /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	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.			

3.6.8.2.7 /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	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.			

3.6.8.2.8 /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	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.			

3.6.8.2.9 */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	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.			

3.6.8.2.10 /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

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.			

3.6.8.2.11 /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	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.			

3.6.8.2.12 /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	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.			

3.6.8.2.13 /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:







Remove world read and write access to `/var/adm/cron/log`:

```
chmod o-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	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.			

3.6.8.2.14 /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	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.			

3.6.8.2.15 /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	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.			

3.6.8.2.16 /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	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.			

3.6.9 Ensure root access is controlled (Automated)

Profile Applicability:

- Level 1

Description:

Restricts access to root via `su` to members of a specific group.

Rationale:

Setting the `sugroups` attribute to `system` ensures that only members of the `system` 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.

Impact:

- In this recommendation we specify the group `system` in order to leave this recommendation as a Level 1, IG1 recommendation.
- Further, as IG1 recommendation - we permit the attribute `login` to be true, to permit direct root login using an HMC.
- A higher level of security would create a new group - specific for `su` to root and that group name would be used in the specification.
- Thus, the *Remediation* procedure below specifies `system` as the correct group name. This is merely an initial solution.
- In any case, `sugroups` should not equal `ALL`.

Audit:

- From the command prompt, execute the following commands:

```
lsuser -a login rlogin su root
```

- The command should yield the following output:

```
root login=true rlogin=false su=true
```

```
lsuser -a sugroups root
```

- The command should **NOT** yield the following output:

```
root sugroups=ALL
```

Remediation:







In `/etc/security/user`, set the root stanza `sugroups` attribute to `system`:

```
chuser login=true rlogin=false su=true sugroups=system root
```

Default Value:

`root login=true rlogin=true sugroups=ALL su=true`

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.			

3.6.10 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

3.6.11 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

3.6.12 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

3.6.13 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.			

3.6.14 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

3.6.15 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 <u>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.			
v7	16.11 <u>Lock Workstation Sessions After Inactivity</u> Automatically lock workstation sessions after a standard period of inactivity.			

3.7 Audit Log Management

3.7.1 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.

3.7.1.1 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\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
```

CIS Controls:

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

3.7.1.2 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

3.7.1.3 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
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.			
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.			

3.7.2 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>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

Appendix: AIXPERT Table

Function	Description	Command	HLS	MLS	LLS	DLS
prereqbinaudit	Prereq rule for binaudit: Checks whether auditing is running or not	/etc/security/aixpert/bin/prereqbinaudit	N/A	N/A	N/A	N/A
prereqcde	Prereq rule for CDE: Checks whether CDE entry exists or not in /etc/inittab.	/etc/security/aixpert/bin/prereqcde	N/A	N/A	N/A	N/A
prereqnocde	Prereq rule for CDE: Checks whether CDE entry exists or not in /etc/inittab.	/etc/security/aixpert/bin/prereqcde	N/A	N/A	N/A	N/A
prereqgated	Prereq rule for gated: Checks whether the system is configured to be a router or not	/etc/security/aixpert/bin/prereqgated	N/A	N/A	N/A	N/A
prereqipsec	Prereq rule for IPsec: Checks whether IPsec is enabled or not	/etc/security/aixpert/bin/prereqipsec	N/A	N/A	N/A	N/A
prereqlft	Prereq rule for LFT: Checks whether LFT is configured or not	/etc/security/aixpert/bin/prereqlft	N/A	N/A	N/A	N/A
prereqnolft	Prereq rule for LFT: Checks whether LFT is configured or not	/etc/security/aixpert/bin/prereqlft	N/A	N/A	N/A	N/A
prereqlh	Prereq rule for loginherald: Checks the herald value is set or not	/etc/security/aixpert/bin/prereqlh	N/A	N/A	N/A	N/A
prereqnosyn	Prereq rule for NoSyn: Checks whether IPsec is enabled or not if its not then enable it	/etc/security/aixpert/bin/prereqnosyn	N/A	N/A	N/A	N/A
prereqrl	Prereq rule for root login: Checks whether any non root user exists who has login privileges	/etc/security/aixpert/bin/prereqrl	N/A	N/A	N/A	N/A
prereqrll	Prereq rule for remote root login: Checks whether any non root user exists with privileges to login remotely	/etc/security/aixpert/bin/prereqrll	N/A	N/A	N/A	N/A
prereqtcb	Prereq rule for TCB: Checks whether TCB is enabled or not	/etc/security/aixpert/bin/prereqtcb	N/A	N/A	N/A	N/A
prereqsed	Prereq rule for SED: Checks whether the	/etc/security/aixpert/bin/prereqsed	N/A	N/A	N/A	N/A

	machine has 64 bit kernel support or not					
prereqnon tcb	Prereq rule for non-TCB: Checks whether the system is non TCB or not	/etc/security/aixpert/bin/prereqnon tcb	N/A	N/A	N/A	N/A
prereqRSSF ull	Prereq rule for RealSecure Server Sensor Full: This option is for the full version and has to be purchased. Please visit www.iss.net to get more details.	/etc/security/aixpert/bin/prereqRSSF ull	N/A	N/A	N/A	N/A
prereqRSSLi te	Prereq rule for RealSecure Server Sensor Lite: To use this option please install ServerSensor.pkg from the AIX Expansion Pack.	/etc/security/aixpert/bin/prereqRSSLi te	N/A	N/A	N/A	N/A
minage	Minimum age for password: Specifies the minimum number of weeks to 1 week before a password can be changed	/etc/security/aixpert/bin/chusrattr	minage=1 ALL hls_minage	minage=4 ALL mls_minage	N/A	minage=0 ALL dls_minage
maxage	Maximum age for password: Specifies the maximum number of weeks (13 weeks) that a password is valid	/etc/security/aixpert/bin/chusrattr	maxage=13 ALL hls_maxage	maxage=13 ALL mls_maxage	maxage=13 ALL lls_maxage	maxage=0 ALL dls_maxage
maxexpired	Time to change password after the expiration: Specifies the maximum number of weeks to 2 weeks after maxage that an expired password can be changed by the user	/etc/security/aixpert/bin/chusrattr	maxexpired=2 ALL hls_maxexpired	maxexpired=4 ALL mls_maxexpired	maxexpired=8 ALL lls_maxexpired	maxexpired=-1 ALL dls_maxexpired
minlen	Minimum length for password: Specifies the minimum length of a password to 8	/etc/security/aixpert/bin/chusrattr	minlen=8 ALL hls_minlen	minlen=8 ALL mls_minlen	minlen=8 ALL lls_minlen	minlen=0 ALL dls_minlen
minalpha	Minimum number of alphabetic chars: Specifies the minimum number of alphabetic	/etc/security/aixpert/bin/chusrattr	minalpha=2 ALL hls_minalpha	minalpha=2 ALL mls_minalpha	minalpha=2 ALL lls_minalpha	minalpha=0 ALL dls_minalpha

	characters in a password to 2		nalph a	minalph		
minother	Minimum number of non-alphabetic chars: Specifies the minimum number of non-alphabetic characters in a password to 2	/etc/security/aixpert/bin/chusrattr	minother=2 ALL hls_minother	minother=2 ALL mls_minother	minother=2 ALL lls_minother	minother=0 ALL dls_minother
maxrepeats	Maximum times a char can appear in a password: Specifies the maximum number of times a character can appear in a password to 2	/etc/security/aixpert/bin/chusrattr	maxrepeats=2 ALL hls_maxrepeats	N/A	N/A	maxrepeats=8 ALL dls_maxrepeats
mindiff	Minimum number of chars: Specifies the minimum number of characters required in a new password to 4 that were not in the old password	/etc/security/aixpert/bin/chusrattr	mindiff=4 ALL hls_mindiff	mindiff=4 ALL mls_mindiff	mindiff=4 ALL lls_mindiff	mindiff=0 ALL dls_mindiff
histexpire	Password reset time: Specifies the number of weeks to 13 weeks before a password can be reused	/etc/security/aixpert/bin/chusrattr	histexpire=1 3 ALL hls_histexpire	histexpire=13 ALL mls_histexpire	histexpire=2 6 ALL lls_histexpire	histexpire=0 ALL dls_histexpire
histsize	Password reuse time: Specifies the number of previous passwords a user cannot reuse to 20	/etc/security/aixpert/bin/chusrattr	histsize=20 ALL hls_histsize	histsize=4 ALL mls_histsize	histsize=4 ALL lls_histsize	histsize=0 ALL dls_histsize
pwdwarntime	Password expiration warning time: Specifies the number of days to 5 days before the system issues a warning that a password change is required	/etc/security/aixpert/bin/chusrattr	pwdwarntime=5 ALL hls_pwdwarntime	pwdwarntime=5 ALL mls_pwdwarntime	pwdwarntime=5 ALL lls_pwdwarntime	pwdwarntime=0 ALL dls_pwdwarntime
usrck	Check user definitions: Verifies the correctness of user definitions and fixes the errors	/etc/security/aixpert/bin/validate_check	usrck	usrck	usrck	N/A
pwdck	Check password definitions: Verifies the correctness of password definitions and fixes the errors	/etc/security/aixpert/bin/pwdckhls	None	pwdckk	pwdck	N/A

	also locks the users without a password					
grpck	Check group definitions: Verifies the correctness of group definitions and fixes the errors	/etc/security/aixpert/bin/validate_check	grpck	grpck	grpck	N/A
tcbupdate	TCB update: Updates Trusted Computing Base	/etc/security/aixpert/bin/validate_check	tcbck	tcbck	tcbck	tcbck
loginretries	Number of login attempts before locking the account: Specifies the number of consecutive unsuccessful login attempts to 3 for each non-root user account before the account is disabled	/etc/security/aixpert/bin/chusrattr	loginretries=3 NONROOT hls_loginretries	loginretries=4 NONROOT Tmls_loginretries	loginretries=5 NONROOT lls_loginretries	loginretries=0 ALL dls_loginretries
logindelay	Delay between unsuccessful logins: Specifies the delay between unsuccessful logins to 10 seconds	/etc/security/aixpert/bin/chdefstanza	/etc/security/login.cfg logindelay=10 default hls_logindelay	/etc/security/login.cfg logindelay=5 default mls_logindelay	/etc/security/login.cfg logindelay=5 default lls_logindelay	/etc/security/login.cfg logindelay=0 default dls_logindelay
logindisable	Disable login after unsuccessful login attempts: Specifies the number of unsuccessful login attempts on a port to 10 before the port is locked	/etc/security/aixpert/bin/chdefstanza	/etc/security/login.cfg logindisable=10 default hls_logindisable	/etc/security/login.cfg logindisable=10 default mls_logindisable	N/A	/etc/security/login.cfg logindisable=0 default dls_logindisable
logininterval	Interval between unsuccessful logins: Specifies the time interval(300 seconds) for a port in which the unsuccessful login attempts must occur before the port is disabled	/etc/security/aixpert/bin/chdefstanza	/etc/security/login.cfg logininterval=300 default hls_logininterval	/etc/security/login.cfg logininterval=60 default mls_logininterval	N/A	/etc/security/login.cfg logininterval=0 default dls_logininterval

			gininterval	interval		
loginreenable	Reenable login after locking: Specifies the time interval(360 minutes) after which a port is unlocked after being disabled by logindisable	/etc/security/aixpert/bin/chdefstanza	/etc/security/login.cfg loginreenable=360 default hls_loginreenable	/etc/security/login.cfg loginreenable=30 default mls_loginreenable	N/A	/etc/security/login.cfg loginreenable=0 default dls_loginreenable
logintimeout	Login timeout: Specifies the time interval(30 seconds) to type in a password	/etc/security/aixpert/bin/chdefstanza	/etc/security/login.cfg logintimeout=30 usw hls_logintimeout	/etc/security/login.cfg logintimeout=60 usw mls_logintimeout	/etc/security/login.cfg logintimeout=60 usw lls_logintimeout	/etc/security/login.cfg logintimeout=60 usw dls_logintimeout
rootlogin	Remote root login: Disables remote root login	/etc/security/aixpert/bin/chuserstanza	/etc/security/user rlogin=false root hls_rootlogin	/etc/security/user rlogin=false root mls_rootlogin	N/A	/etc/security/user rlogin=true root dls_rootlogin
rootlogin	Local login: Disables root to login locally	/etc/security/aixpert/bin/chuserstanza	/etc/security/user login=false root hls_rootlogin	N/A	N/A	/etc/security/user login=true root dls_rootlogin
binaudit	Enable binaudit: Enables bin auditing for HLS	/etc/security/aixpert/bin/binaudit	hls_binaudit	mls_binaudit	lls_binaudit	dls_binaudit
disqdaemon	Disable qdaemon: Stops qdaemon and comments the	/etc/security/aixpert/bin/comntrows	qdaemon: /etc/inittab :	qdaemon: /etc/inittab	N/A	qdaemon: /etc/inittab : a

	qdaemon entry in /etc/inittab		d hls_di sqdaemon	: d mls_ disqdaemon		dls_dis qdaemon
dispiobe	Disable piobe daemon: Stops piobe daemon and comments the piobe entry in /etc/inittab	/etc/security/aixpert/bin/comntrows	piobe: /etc/inittab : d hls_di spiobe	piobe : /etc/inittab : d mls_ dispiobe	N/A	piobe: /etc/inittab : a dls_dis piobe
dislpd	Disable lpd daemon: Stops lpd daemon and comments the lpd entry in /etc/inittab	/etc/security/aixpert/bin/comntrows	lpd: /etc/inittab : d hls_di slpd	lpd: /etc/inittab : d mls_ dislpd	N/A	lpd: /etc/inittab : d dls_dis lpd
discde	Disable CDE: Disables CDE when LFT is not configured	/etc/security/aixpert/bin/comntrows	dt: "/etc/inittab" ":" d hls_di scde	dt: "/etc/inittab" ":" d mls_ discde	N/A	dt: "/etc/inittab" ":" a dls_dis cde
disautoconf6	Stop autoconf6: Stops autoconf6 if it is running and comments the entry for autoconf6 in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	autoc onf6 d hls_di sautoc onf6	N/A	N/A	autoco nf6 d dls_dis autoco nf6
disrtnghmn	Disable routing daemon: Stops routed daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	routed d hls_di srtnghmn	N/A	N/A	routed d dls_dis rtnghmn
distimedmn	Disable timed daemon: Stops timed daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	timed d hls_di stimed mn	timed d mls_ distimed mn	timed d mls_ distimed mn	timed d dls_dis timedmn
disntpdmn	Disable NTP daemon: Stops NTP daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	xntpd d hls_di sntpd mn	xntpd d mls_ disntpd mn	N/A	xntpd d dls_dis ntpdmn
disrwhoddmn	Disable rwhod daemon: Stops rwhod daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	rwhod d hls_di srwhoddmn	N/A	N/A	rwhod d dls_dis rwhoddmn

dissnmpdmn	Disable SNMP daemon: Stops SNMP daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	snmp d d hls_di ssnmp dmn	snmp d d mls_ dissn mpd mn	snmpd d lls_dis snmpd mn	snmpd a dls_dis snmpd mn
dissnmpmibddmn	Disable SNMPMIBD daemon: Stops SNMPMIBD daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	snmp mibd d hls_di ssnmp mibdd mn	snmp mibd d mls_ dissn mpmi bddm n	snmp mibd d lls_dis snmp mibdd mn	snmpm ibd a dls_dis snmpm ibddmn
disaixmibddmn	Disable AIXMIBD daemon: Stops AIXMIBD daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	aixmib d d hls_di saixmi bddm n	aixmi bd d mls_ disai xmib ddmn	aixmib d d lls_dis aixmib ddmn	aixmib d a dls_dis aixmib ddmn
dishostmibddmn	Disable HOSTMIBD daemon: Stops HOSTMIBD daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	hostmi bd d hls_di shost mibdd mn	host mibd d mls_ disho stmib ddmn	hostmi bd d lls_dis hostmi bddm n	hostmi bd a dls_dis hostmi bddmn
disdpid2dmn	Disable DPID2 daemon: Stops DPID2 daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	dpid2 d hls_di sdpid2 dmn	N/A	N/A	dpid2 d dls_dis dpid2d mn
dismrouteddmn	Disable mrouted daemon: Stops mrouted daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	mrout ed d hls_di smrou teddm n	N/A	N/A	mroute d d dls_dis mroute ddmn
disprintdmn	Disable print daemon: Stops the print daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	lpd d hls_di sprint dmn	N/A	N/A	lpd d dls_dis printdm n
disdnstdmn	Disable DNS daemon: Stops DNS daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	name d d hls_di sdnsd mn	N/A	N/A	named d dls_dis dnstdm n
dismaildmn	Disable mail client: Stops Sendmail daemon and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	send mail d hls_di smaild mn	N/A	N/A	sendm ail a dls_dis maildm n
disdhcpserv	Stop DHCP Server: Stops DHCP server	/etc/security/aixpert/bin/rctcpip	dhcps d d	N/A	N/A	dhcpsd d

	daemon and comments it's entry in /etc/rc.tcpip		hls_di sdhcp serv			dls_dis dhcpse rv
disdhcpagent	Stop DHCP Agent: Stops DHCP relay agent and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	dhcpr d d hls_di sdhcp agent	N/A	N/A	dhcprd d dls_dis dhcpag ent
disdhcpclient	Stop DHCP Client: Stops DHCP client and comments it's entry in /etc/rc.tcpip	/etc/security/aixpert/bin/rctcpip	dhcpc d d hls_di sdhcp client	N/A	N/A	dhcpcd d dls_dis dhcpcli ent
disgateddmn	Disable gated daemon: Stops gated daemons and comments the entry for gated daemon in /etc/rc.tcpip if the system is not configured as a router	/etc/security/aixpert/bin/rctcpip	gated d hls_di sgate ddmn	gated d mls_ disga tedd mn	gated d lls_dis gated dmn	gated d dls_dis gatedd mn
shell	Disable rshd daemon: Comments the entry for rshd daemon in /etc/inetd.conf and kills all instances of rshd	/etc/security/aixpert/bin/cominetdconf	shell tcp d hls_sh ell	shell tcp d mls_ shell	shell tcp d lls_sh ell	shell tcp a dls_sh ell
kshell	Disable krshd daemon: Comments the entry for krshd daemon in /etc/inetd.conf and kills all instances of krshd	/etc/security/aixpert/bin/cominetdconf	kshell tcp d hls_ks hell	N/A	N/A	kshell tcp d dls_ks hell
rlogin	Disable rlogin in /etc/inetd.conf: Comments the entry for rlogind daemon in /etc/inetd.conf and kills all instances of rlogind	/etc/security/aixpert/bin/cominetdconf	login tcp d hls_rlo gin	login tcp d mls_r login	N/A	login tcp a dls_rlo gin
krlogin	Disable krlogind in /etc/inetd.conf: Comments the entry for krlogind daemon in /etc/inetd.conf and kills all instances of krlogind	/etc/security/aixpert/bin/cominetdconf	klogin tcp d hls_krl ogin	N/A	N/A	klogin tcp d dls_krl ogin
rexecd	Disable rexecd in /etc/inetd.conf: Comments the entry for rexecd daemon in /etc/inetd.conf and kills all instances of rexecd	/etc/security/aixpert/bin/cominetdconf	exec tcp d hls_re xecd	exec tcp d mls_r exec d	N/A	exec tcp a dls_rex ecd
comsat	Disable comsat in /etc/inetd.conf: Comments the entry for comsat daemon in	/etc/security/aixpert/bin/cominetdconf	comsa t udp d	N/A	N/A	comsat udp d dls_co msat

	/etc/inetd.conf and kills all instances of comsat		hls_co msat			
uucp	Enable uucpd in /etc/inetd.conf: Comments the entry for uucpd daemon in /etc/inetd.conf and kills all instances of uucpd	/etc/security/aixpert/bin/ cominetdconf	uucp tcp d hls_uu cp	N/A	N/A	uucp tcp a dls_uu cp
bootps	Disable bootpd in /etc/inetd.conf: Comments the entry for bootpd daemon in /etc/inetd.conf and kills all instances of bootpsd	/etc/security/aixpert/bin/ cominetdconf	bootp s udp d hls_bo otps	bootp s udp d mls_ bootp s	N/A	bootps udp d dls_bo otps
fingerd	Disable fingerd in /etc/inetd.conf: Comments the entry for fingerd daemon in /etc/inetd.conf and kills all instances of fingerd	/etc/security/aixpert/bin/ cominetdconf	finger tcp d hls_fin gerd	finger tcp d mls_f inger d	N/A	finger tcp d dls_fin gerd
systat	Disable sysstat in /etc/inetd.conf: Comments the entry for systat daemon in /etc/inetd.conf and kills all instances of systat	/etc/security/aixpert/bin/ cominetdconf	systat tcp d hls_sy stat	systa t tcp d mls_ systa t	N/A	systat tcp d dls_sys tat
netstat	Disable netstat in /etc/inetd.conf: Comments the entry for netstat daemon in /etc/inetd.conf and kills all instances of netstat	/etc/security/aixpert/bin/ cominetdconf	netsta t tcp d hls_ne tstat	netst at tcp d mls_ netst at	N/A	netstat tcp d dls_net stat
tftp	Disable tftp in /etc/inetd.conf: Comments the entry for tftp daemon in /etc/inetd.conf and kills all instances of tftpd	/etc/security/aixpert/bin/ cominetdconf	tftp udp d hls_tft p	tftp udp d mls_t ftp	N/A	tftp udp d dls_tftp
talk	Disable talk in /etc/inetd.conf: Comments the entry for talk daemon in /etc/inetd.conf and kills all instances of talkd	/etc/security/aixpert/bin/ cominetdconf	talk udp d hls_tal k	talk udp d mls_t alk	talk udp d lms_tal k	talk udp a dls_tal k
rquotad	Disable rquotad in /etc/inetd.conf: Comments the entry for rquotad daemon in /etc/inetd.conf and kills all instances of rquotad	/etc/security/aixpert/bin/ cominetdconf	rquota d udp d hls_rq uotad	rquot ad udp d mls_r quota d	rquota d udp d lms_rqu otad	rquota d udp d dls_rqu otad
rexid	Disable rexd in /etc/inetd.conf:	/etc/security/aixpert/bin/ cominetdconf	rexid tcp d	rexid tcp d	rexid tcp d	rexid tcp d

	Comments the entry for rexd daemon in /etc/inetd.conf and kills all instances of rexd		hls_rexd	mls_rexd	lls_rexd	dls_rexd
rstatd	Disable rstatd in /etc/inetd.conf: Comments the entry for rstatd daemon in /etc/inetd.conf and kills all instances of rstatd	/etc/security/aixpert/bin/cominetdconf	rstatd udp d hls_rstatd	rstatd udp d mls_rstatd	N/A	rstatd udp d dls_rstatd
rusersd	Disable rusersd in /etc/inetd.conf: Comments the entry for rusersd daemon in /etc/inetd.conf and kills all instances of rusersd	/etc/security/aixpert/bin/cominetdconf	rusersd udp d hls_rusersd	rusersd udp d mls_rusersd	N/A	rusersd udp d dls_rusersd
rwalld	Disable rwalld in /etc/inetd.conf: Comments the entry for rwalld daemon in /etc/inetd.conf and kills all instances of rwalld	/etc/security/aixpert/bin/cominetdconf	rwalld udp d hls_rwalld	rwalld udp d mls_rwalld	N/A	rwalld udp d dls_rwalld
sprayd	Disable sprayd in /etc/inetd.conf: Comments the entry for sprayd daemon in /etc/inetd.conf and kills all instances of sprayd	/etc/security/aixpert/bin/cominetdconf	sprayd udp d hls_sprayd	sprayd udp d mls_sprayd	N/A	sprayd udp d dls_sprayd
pcnfsd	Disable pcnfsd in /etc/inetd.conf: Comments the entry for pcnfsd daemon in /etc/inetd.conf and kills all instances of pcnfsd	/etc/security/aixpert/bin/cominetdconf	pcnfsd udp d hls_pcnfsd	N/A	N/A	pcnfsd udp d dls_pcnfsd
tcpecho	Disable TCP echo service in /etc/inetd.conf: Comments the entry for TCP Echo service in /etc/inetd.conf and kills all instances of echo(tcp)	/etc/security/aixpert/bin/cominetdconf	echo tcp d hls_tcpecho	N/A	N/A	echo tcp d dls_tcpecho
tcpdiscard	Disable TCP Discard service in /etc/inetd.conf: Comments the entry for TCP Discard service in /etc/inetd.conf and kills all instances of discard(tcp)	/etc/security/aixpert/bin/cominetdconf	discard tcp d hls_tcpdiscard	N/A	N/A	discard tcp d dls_tcpdiscard
tcpchargen	Disable TCP chargen service in /etc/inetd.conf:	/etc/security/aixpert/bin/cominetdconf	chargen tcp d	N/A	N/A	chargen tcp d dls_tcp

	Comments the entry for TCP Chargen service in /etc/inetd.conf and kills all instances of chargen(tcp)		hls_tcpchargen			chargen
tcpdaytime	Disable TCP daytime service in /etc/inetd.conf: Comments the entry for TCP Daytime service in /etc/inetd.conf and kills all instances of daytime(tcp)	/etc/security/aixpert/bin/cominetdconf	daytime tcp d hls_tcpdaytime	N/A	N/A	daytime tcp a dls_tcpdaytime
tcpdtime	Disable TCP time service in /etc/inetd.conf: Comments the entry for TCP Time service in /etc/inetd.conf and kills all instances of timed(tcp)	/etc/security/aixpert/bin/cominetdconf	time tcp d hls_tcpdtime	N/A	N/A	time tcp a dls_tcpdtime
udppecho	Disable UDP Echo service in /etc/inetd.conf: Comments the entry for UDP Echo service in /etc/inetd.conf and kills all instances of UDP echo	/etc/security/aixpert/bin/cominetdconf	echo udp d hls_udppecho	N/A	N/A	echo udp d dls_udppecho
udpdiscard	Disable UDP discard service in /etc/inetd.conf: Comments the entry for UDP Discard service in /etc/inetd.conf and kills all instances of UDP discard	/etc/security/aixpert/bin/cominetdconf	discard udp d hls_udpdiscard	N/A	N/A	discard udp d dls_udpdiscard
udpchargen	Disable UDP chargen service in /etc/inetd.conf: Comments the entry for UDP Chargen service in /etc/inetd.conf and kills all instances of chargen	/etc/security/aixpert/bin/cominetdconf	chargen udp d hls_udpchargen	N/A	N/A	chargen udp d dls_udpchargen
udpdaytime	Disable UDP daytime service in /etc/inetd.conf: Comments the entry for UDP Daytime service in /etc/inetd.conf and kills	/etc/security/aixpert/bin/cominetdconf	daytime udp d hls_udpdaytime	N/A	N/A	daytime udp a dls_udpdaytime

	all instances of daytime					
udptime	Disable UDP time service in /etc/inetd.conf: Comments the entry for UDP Time service in /etc/inetd.conf and kills all instances of time service(udp)	/etc/security/aixpert/bin/cominetdconf	time udp d hls_ud ptime	N/A	N/A	time udp a dls_ud ptime
ftp	Disable FTP: Comments the entry for ftpd daemon in /etc/inetd.conf and kills all instances of ftpd	/etc/security/aixpert/bin/cominetdconf	ftp tcp d hls_ftp	N/A	N/A	ftp tcp a dls_ftp
telnet	Disable telnet: Comments the entry for telnetd daemon in /etc/inetd.conf and kills all instances of telnetd	/etc/security/aixpert/bin/cominetdconf	telnet tcp d hls_tel net	N/A	N/A	telnet tcp a dls_tel net
imapd	Disable IMAPD: Comments the entry for imapd daemon in /etc/inetd.conf and kills all instances of imapd	/etc/security/aixpert/bin/cominetdconf	imap2 tcp d hls_im apd	N/A	N/A	imap2 tcp d dls_im apd
pop3d	Disable POP3D: Comments the entry for pop3d daemon in /etc/inetd.conf and kills all instances of pop3d	/etc/security/aixpert/bin/cominetdconf	pop3 tcp d hls_po p3d	N/A	N/A	pop3 tcp d dls_po p3d
dtspc	Disable dtspc in /etc/inetd.conf: Comments the entry for dtspc daemon in /etc/inetd.conf when LFT is not configured and CDE is disabled in /etc/inittab also kills all the instances of dtspc daemon	/etc/security/aixpert/bin/cominetdconf	dtspc tcp d hls_dt spc	N/A	N/A	dtspc tcp d dls_dts pc
ttdbserver	Disable ttdbserver service in /etc/inetd.conf: Comments the entry for ttdbserver service in /etc/inetd.conf and kills all instances of ttdbserver service	/etc/security/aixpert/bin/cominetdconf	ttdbse rver tcp d hls_ttd bserv er	N/A	N/A	ttdbser ver tcp a dls_ttd bserver
cmsd	Disable cmsd service in /etc/inetd.conf: Comments the entry for cmsd service in /etc/inetd.conf and kills all instances of cmsd service	/etc/security/aixpert/bin/cominetdconf	cmsd udp d hls_c msd	N/A	N/A	cmsd udp a dls_cm sd

rmsuidfrmcmds	Removes SUID from remote commands: Removes SUID from remote commands rcp rdist rexec remsh rlogin and rsh	/etc/security/aixpert/bin/rmsuidfrmcmds	r_hls_rmsuidfrmcmds	r_mls_rmsuidfrmcmds	r_lls_rmsuidfrmcmds	s_dls_rmsuidfrmcmds
filepermgr	File Permissions Manager: Runs fpm comamnd with high option to remove setuid setgid from privileged commands	/etc/security/aixpert/bin/filepermgr	h_hls_filepermgr	m_mls_filepermgr	l_lls_filepermgr	d_dls_filepermgr
disablenfs	Stop NFS daemon: Removes NFS mounts stops NFS daemons and removes NFS from startup	/etc/security/aixpert/bin/nfsconfig	d_hls_disablenfs	N/A	N/A	e_dls_disablenfs
disrmtcmds	Disable unsecure commands: Disables unsecure commands rlogin rsh rcp and tftp	/etc/security/aixpert/bin/disrmtcmds	d_hls_disrmtcmds	d_mls_disrmtcmds	N/A	e_dls_disrmtcmds
disrmtdmns	Disable unsecure daemons: Disables unsecure daemons rlogind rshd and tftpd	/etc/security/aixpert/bin/disrmtdmns	d_hls_disrmtdmns	d_mls_disrmtdmns	N/A	e_dls_disrmtdmns
rmrhostsnetrc	Remove rhosts and netrc services: Removes .rhosts and .netrc files from user's home directory	/etc/security/aixpert/bin/rmrhostsnetrc	h_hls_rmrhostsnetrc	m_mls_rmrhostsnetrc	l_lls_rmrhostsnetrc	d_dls_rmrhostsnetrc
rmetchostsequiv	Remove entries from /etc/hosts.equiv file: Removes entries from /etc/hosts.equiv file	/etc/security/aixpert/bin/rmetchostsequiv	hls_rmetchostsequiv	mls_rmetchostsequiv	lls_rmetchostsequiv	dls_rmetchostsequiv
bcastping	Network option bcastping: Set network option bcastping's value to 0	/etc/security/aixpert/bin/ntwkopts	bcastping=0 s_hls_bcastping	bcastping=0 s_mls_bcastping	bcastping=0 s_lls_bcastping	bcastping=NULL d_dls_bcastping
clean_partial_conns	Network option clean_partial_conns: Set network option clean_partial_conns's value to 1	/etc/security/aixpert/bin/ntwkopts	clean_partial_conns=1 s_hls_clean_partial_conns	clean_partial_conns=1 s_mls_clean_partial_conns	clean_partial_conns=1 s_lls_clean_partial_conns	clean_partial_conns=NULL d_dls_clean_partial_conns
directed_broadcast	Network option directed_broadcast: Set network option	/etc/security/aixpert/bin/ntwkopts	directed_broadcast	directed_broadcast	directed_broadcast	directed_broadcast

	directed_broadcast's value to 0		st=0 s hls_dir ected_ broa dcast	ast=0 s mls_ direct ed_b roadc ast	=0 s lls_dir ected_ broad cast	NULL d dls_dir ected_ broadc ast
icmpaddressmask	Network option icmpaddressmask: Set network option icmpaddressmask's value to 0	/etc/security/aixpert/bin/ ntwkopts	icm pa ddres smask =0 s hls_ ic mpad dress mask	icm p addr essm ask= 0 s lls_ ic mpad dress smas k	icm pa ddress mask= 0 s lls_ ic mpad dress mask	icm pad dressm ask=N ULL d dls_ ic mpad dressma sk
ipforwarding	Network option ipforwarding: Set network option ipforwarding's value to 0	/etc/security/aixpert/bin/ ntwkopts	ipforw arding =0 s hls_ ipf orwar ding	N/A	N/A	ipforwa rding= NULL d dls_ ipf orwardi ng
ipignoreredirects	Network option ipignoreredirects: Set network option ipignoreredirects's value to 1	/etc/security/aixpert/bin/ ntwkopts	ipigno reredir ects= 1 s hls_ ipi gnorer edirect s	N/A	N/A	ipignor eredire cts=NU LL d dls_ ipi gnorer edirect s
ipsendredirects	Network option ipsendredirects: Set network option ipsendredirects's value to 0	/etc/security/aixpert/bin/ ntwkopts	ipsend redire cts=0 s hls_ ip sendr edirect s	N/A	N/A	ipsendr edirect s=NUL L d dls_ ips endred irects
ipsrcrouteforward	Network option ipsrcrouteforward: Set network option ipsrcrouteforward's value to 0	/etc/security/aixpert/bin/ ntwkopts	ipsrcr outefo rward =0 s hls_ ip srcrou teforw ard	ipsrcr outef orwar d=0 s mls_ ip srcrou teforw ard	N/A	ipsrcro uteforw ard=N ULL d dls_ ips rcroute forward
ipsrcrouterrecv	Network option ipsrcrouterrecv: Set network option ipsrcrouterrecv's value to 0	/etc/security/aixpert/bin/ ntwkopts	ipsrcr outere cv=0 s hls_ ip srcrou terecv	ipsrcr outer ecv= 0 s mls_ ip srcr	N/A	ipsrcro uterecv =NULL d dls_ ips rcroute recv

				outer ecv		
ipsrcroutesen d	Network option ipsrcroutesend: Set network option ipsrcroutesend's value to 0	/etc/security/aixpert/bin/ ntwkopts	ipsrcr outes end=0 s hls_ip srcrou tesen d	N/A	N/A	ipsrcro utesen d=NUL L d dls_ips rcrou tesen d
ip6srcroutefor ward	Network option ip6srcrouteforward: Set network option ip6srcrouteforward's value to 0	/etc/security/aixpert/bin/ ntwkopts	ip6src route forwar d=0 s hls_ip 6srcro utefor ward	N/A	N/A	ip6srcr outefor ward= NULL d dls_ip6 srcrou teforwar d
nonlocsrcrou te	Network option nonlocsrcroute: Set network option nonlocsrcroute's value to 0	/etc/security/aixpert/bin/ ntwkopts	nonloc srcrou te=0 s hls_no nlocsr crou te	nonlo csrcr oute =0 s mls_ nonlo csrcr oute	N/A	nonloc srcrou te=NUL L d dls_no nlocsrc route
tcp_pmtu_disc over	Network option tcp_pmtu_discover: Set network option tcp_pmtu_discover's value to 0	/etc/security/aixpert/bin/ ntwkopts	tcp_p mtu_d iscove r=0 s hls_tc p_pmt u_disc over	tcp_p mtu_ disco ver= NULL d dls_t cp_p mtu_ disco ver	tcp_p mtu_ disco ver =0 s lts_tcp _pmtu _disco ver	N/A
udp_pmtu_dis cover	Network option udp_pmtu_discover: Set network option udp_pmtu_discover's value to 0	/etc/security/aixpert/bin/ ntwkopts	udp_p mtu_d iscove r=0 s hls_ud p_pmt u_disc over	udp_ pmtu _disc over =0 s mls_ udp_ pmtu _disc over	udp_p mtu_ disco ver =0 s lts_ud p_pmt u_disc over	udp_p mtu_ disco ver =NULL d dls_ud p_pmt u_disc over
tcp_sendspac e	Network option tcp_sendspace: Set network option tcp_sendspace's value to 262144	/etc/security/aixpert/bin/ ntwkopts	tcp_se ndspa ce=26 2144 s hls_tc p_sen	tcp_s ends pace =262 144 s mls_t cp_s	tcp_se ndspa ce=26 2144 s lts_tcp _send space	tcp_se ndspa ce=NUL L d dls_tcp _send space

			dspac e	ends pace		
tcp_recvspace	Network option tcp_recvspace: Set network option tcp_recvspace's value to 262144	/etc/security/aixpert/bin/ ntwkopts	tcp_re cvspa ce=26 2144 s hls_tc p_rec vspac e	tcp_r ecvs pace =262 144 s mls_tc p_rec cvsp ace	tcp_re cvspa ce=26 2144 s mls_tc p_recv space	tcp_rec vspace =NULL d dls_tcp _recvs pace
rfc1323	Network option rfc1323: Set network option rfc1323's value to 1	/etc/security/aixpert/bin/ ntwkopts	rfc132 3=1 s hls_rfc 1323	rfc13 23=1 s mls_r fc132 3	rfc132 3=1 s lls_rfc 1323	rfc132 3=NUL L d dls_rfc 1323
tcp_mssdflt	Network option tcp_mssdflt: Set network option tcp_mssdflt's value to 1448	/etc/security/aixpert/bin/ ntwkopts	tcp_m ssdflt= 1448 s hls_tc p_mss dflt	tcp_m mssd flt=14 48 s mls_t cp_m ssdflt	tcp_m ssdflt= 1448 s lls_tcp _mssd flt	tcp_ms sdflt=N ULL d dls_tcp _mssdf lt
sb_max	Network option sb_max: Set network option sb_max's value to 1MB	/etc/security/aixpert/bin/ ntwkopts	sb_m ax=10 48576 s hls_sb _max	sb_m ax=1 0485 76 s mls_ sb_m ax	sb_ma x=104 8576 s lls_sb _max	sb_ma x=1048 576 s dls_sb _max
tcp_tcpsecure	Network option tcp_tcpsecure: Set network option tcp_tcpsecure's value to 7	/etc/security/aixpert/bin/ ntwkopts	tcp_tc psecu re=7 s hls_tc p_tcps ecure	tcp_t cpse cure =5 s mls_t cp_tc psec ure	tcp_tc psecu re=5 s lls_tcp _tcpse cure	tcp_tcp secure =NULL d dls_tcp _tcpse cure
sockthresh	Network option sockthresh: Set network option sockthresh's value to 60	/etc/security/aixpert/bin/ ntwkopts	sockth resh= 60 s hls_so ckthre sh	sockt hresh =70 s mls_ sockt hresh	sockth resh= 85 s lls_so ckthre sh	sockthr esh=N ULL d dls_so ckthres h
ipsecshunhost	Shun host for 5 minutes: Shuns the hosts for 5 minutes which tries to access un-used ports	/etc/security/aixpert/bin/ ipsecshunhosthls	hls_ip secsh unhos t	N/A	N/A	dls_ips ecshun host
ipsecshunports	Guard host against port scans: Shuns vulnerable ports for 5 minutes to guard the	/etc/security/aixpert/bin/ ipsecshunports	hls_ip secsh unport	mls_i psec shun ports	N/A	dls_ips ecshun ports

	host against port scans					
umask	Object creation permissions: Specifies default object creation permissions to 077	/etc/security/aixpert/bin/chusrattr	umask=77 ALL hls_umask	umask=27 ALL mls_umask	N/A	umask=22 ALL dls_umask
core	Set core file size: Specifies the core file size to 0 for root	/etc/security/aixpert/bin/chuserstanza	/etc/security/limits core=0 root hls_core	/etc/security/limits core=0 root mls_core	N/A	/etc/security/limits core=0 root dls_core
limitsysacc	Limit system access: Makes root the only user in cron.allow file and removes the cron.deny file	/etc/security/aixpert/bin/limitsysacc	hls_limitsysacc	N/A	N/A	dls_limitsysacc
crontabperm	Crontab permissions: Ensures root's crontab jobs are owned and writable only by root	/etc/security/aixpert/bin/rootcrnjobck	hls_crontabperm	mls_crontabperm	lms_crontabperm	N/A
loginherald	Set login herald: Set login herald in default stanza	/etc/security/aixpert/bin/loginherald	ahls_loginherald	ahls_loginherald	ahls_loginherald	dls_loginherald
rmidotfrmpathroot	Remove dot from path root: Remove dot from PATH environment variable from files .profile .kshrc .cshrc and .login in root's home directory	/etc/security/aixpert/bin/rmidotfrmpathroot	hls_rmidotfrmpathroot	mls_rmidotfrmpathroot	lms_rmidotfrmpathroot	dls_rmidotfrmpathroot
rmidotfrmpathnonroot	Remove dot from non-root path: Removes dot from PATH environment variable from files .profile .kshrc .cshrc and .login in user's home directory	/etc/security/aixpert/bin/rmidotfrmpathnonroot	None	N/A	N/A	None
xhost	Disable X-Server access: Disable access control for X-Server	/etc/security/aixpert/bin/disablexhost	true	true	N/A	false
chetcftpusers	Add root user in /etc/ftpusers file: Adds root username in /etc/ftpusers file	/etc/security/aixpert/bin/chetcftpusers	ahls_chetcftpusers	ahls_chetcftpusers	N/A	rdls_chetcftpusers

removeguest	Remove guest account: Removes guest account and its files	/etc/security/aixpert/bin/remove_guest	true	true	N/A	false
sedconfig	Enable SED feature: Enable Stack Execution Disable feature	/etc/security/aixpert/bin/sedconfig	hls_sedconfig	N/A	N/A	N/A
rootpwdintchk	Root Password Integrity Check: Makes sure that the root password being set is not weak	/etc/security/aixpert/bin/chuserstanza	/etc/security/userdictionary=/etc/security/aixpert/dictionary/Englishroot_hls_rootpwdintchk	/etc/security/userdictionary=/etc/security/aixpert/dictionary/Englishroot_hls_rootpwdintchk	N/A	N/A
pwdpolicyenf	SOX-cobit-best-practices-Password Policy Enforcement: Password Policy Enforcement	/etc/security/aixpert/bin/pwdpolicyenf	N/A	N/A	N/A	N/A
secactreport	SOX-cobit-best-practices-Security Activity Reports: Violation and Security Activity Reports	/etc/security/aixpert/bin/secactreport	N/A	N/A	N/A	N/A
virusdetsw	SOX-cobit-best-practices-Virus Detection Software: Malicious Software Prevention Detection and Correction	/etc/security/aixpert/bin/virusdetsw	N/A	N/A	N/A	N/A
firewsetup	SOX-cobit-best-practices-Firewall setup: Firewall Architecture and Connections with Public Networks	/etc/security/aixpert/bin/firewsetup	N/A	N/A	N/A	N/A
tcptr	TCP Traffic Regulation High: Enforces denial-of-service mitigation on popular ports.	/etc/security/aixpert/bin/tcptr_aixpert	hls	N/A	N/A	N/A
ISSServerSensorFull	Enable RealSecure Server Sensor Full:	/etc/security/aixpert/bin/ISSServerSensor	hls_IS	mls_I	lls_IS	dls_IS

	Enables high level policies for RealSecure Server Sensor Full		SServ erSen sorFull	SSS erver Sens orFull	SServ erSen sorFull	SServe rSens orFull
ISSServerSen sorLite	Enable RealSecure Server Sensor Lite: Enables high level policies for RealSecure Server Sensor Lite	/etc/security/aixpert/bin/ ISSServerSensor	h hls_IS SServ erSen sorLit e	m mls_I SSS erver Sens orLite	l lls_IS SServ erSen sorLite	d dls_IS SServe rSens orLite
ipsecpermit	Allow the packets from HMC	/etc/security/aixpert/bin/ ipsecpermithostorport	Permit Host_I PSEC	Perm itHos t_IPS EC	N/A	N/A

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	Using this Benchmark		
1.1	Benchmark Scenarios		
1.2	Using the Build Kit		
1.3	AIX Installation		
1.4	AIX Maintenance Cadence and Security Management		
1.5	Summary		
2	AIX Security Expert - Technology		
2.1	AIXPERT: Basic usage		
2.2	AIXPERT: Standard policies		
2.3	AIXPERT: Custom Policies		
2.4	Role of AIXPERT in the CIS AIX benchmark		
2.5	Applying the CIS Policy		
3	AIX Recommendations		
3.1	Account Management		
3.1.1	Local Identification Management		
3.1.1.1	All accounts must have a hashed password (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.2	All user id's must be unique (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.1.3	All group id's must be unique (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2	Password Controls - Local Registry		
3.1.2.1	histexpire (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.2	histsize (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.3	loginretries (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.4	maxage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.5	maxexpired (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.6	maxrepeats (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.7	minage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.8	minalpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.9	mindiff (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.10	mindigit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.11	minlen (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.12	minloweralpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.13	minother (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.14	minspecialchar (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.2.15	minupperalpha (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.1.3	System Accounts		
3.1.3.1	adm (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.2	bin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.3	daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.4	guest (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.5	lpd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.6	nobody (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.7	nuucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.8	sys (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.9	uucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.3.10	Ensure System Accounts cannot access system using ftp. (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.1.4	User Attributes for Active Processes		
3.2	Access Control Management		
3.2.1	RBAC managed privilege escalation		
3.2.1.1	Privilege escalation: enhanced RBAC (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2	SUDO managed privilege escalation		
3.2.2.1	Privilege escalation: sudo (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2.2	Ensure sudo log file is active (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.2.3	Ensure sudo commands use pty (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.3	Special Permissions Management - suid, sgid, acl, and trusted-bit files and programs (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.4	Adding authorized users in at.allow (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.5	Services - at access is root only (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.6	Adding authorised users in cron.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2.7	Services - crontab access is root only (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Network Infrastructure Management		
3.3.1	Boot phase: /etc/inittab		
3.3.1.1	Disable writesrv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.2	dt (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.3	piobe (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.4	qdaemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.5	rcnfs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.1.6	cas_agent (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2	Boot phase: /etc/rc.tcpip: daemons		
3.3.2.1	Disable ntalk/talk/write (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.2	aixmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.3	dhcpcd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.4	dhcprd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.5	dhcpsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.6	dpid2 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.7	gated (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.8	hostmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.3.2.9	inetd - aka Super Daemon (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.10	mrouted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.11	named (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.12	portmap (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.13	routed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.14	rwhod (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.15	sendmail (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.16	snmpd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.17	snmpmibd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.2.18	timed (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3	Boot phase: IPv6		
3.3.3.1	autoconf6 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.2	ndpd-host (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.3.3	ndpd-router (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4	inetd services		
3.3.4.1	bootps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.2	chargen (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.3	comsat (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.4	daytime (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.5	discard (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.6	echo (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.7	exec (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.8	finger (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.9	ftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.10	imap2 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.11	instsrv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.12	klogin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.13	kshell (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.14	login (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.15	netstat (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.16	ntalk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.17	pcnfsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.18	pop3 (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.19	rexid (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.20	rquotad (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.21	rstatd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.22	rusersd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.23	rwalld (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.24	shell (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.25	sprayd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.26	xmquery (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.27	talk (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.3.4.28	telnet (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.29	tftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.30	time (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.4.31	uucp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5	NFS		
3.3.5.1	NFS - de-install NFS server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5.2	NFS - enable both nosuid and nodev options on NFS client mounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5.3	NFS - localhost removal (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5.4	NFS - restrict NFS access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5.5	NFS - no root access via NFS exports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.3.5.6	NFS - secure NFS (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Network Monitoring and Defense		
3.4.1	bcastping (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.2	clean_partial_conns (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.3	directed_broadcast (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.4	icmpaddressmask (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.5	ipforwarding (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.6	ipignoreredirects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.7	ipsendredirects (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.8	ipsrouteforward (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.9	ipsrouterecv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.10	ipsroutesev (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.11	ip6srouteforward (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.12	nfs_use_reserved_ports (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.13	nonlocsrcroute (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.14	sockthresh (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.15	tcp_pmtu_discover (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.16	tcp_tcpsecure (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.4.17	udp_pmtu_discover (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5	Data Protection		
3.5.1	Encrypted Filesystems (EFS)		
3.5.1.1	EFS - implementation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.2	Ensure default user umask is 027 or more restrictive (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.3	General Permissions Management - world writable directories (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.4	General Permissions Management - world writable files (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.5.5	Ensure no unowned files or directories exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Secure Configuration of Enterprise Assets and Software		
3.6.1	Common Desktop Environment (CDE)		
3.6.1.1	CDE - de-installing CDE (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.6.1.2	/etc/inetd.conf - cmsd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.3	CDE - disabling dtlogin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.4	/etc/inetd.conf - dtspc (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.5	CDE - sgid/suid binary lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.6	CDE - remote GUI login disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.7	CDE - screensaver lock (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.8	CDE - login screen hostname masking (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.9	CDE - /etc/dt/config/Xconfig permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.10	CDE - /etc/dt/config/Xservers permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.1.11	CDE - /etc/dt/config/*/Xresources permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2	OpenSSH		
3.6.2.1	OpenSSH - Installation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.2	OpenSSH - PermitRootLogin (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.3	OpenSSH - Banner (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.4	Ensure SSH IgnoreRhosts is enabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.5	Ensure SSH PermitEmptyPasswords is disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.6	Configuring SSH - disallow host based authentication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.7	Configuring SSH - removal of .shosts files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.8	Configuring SSH - removal of /etc/shosts.equiv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.9	Configuring SSH - set LogLevel to INFO or VERBOSE (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.10	OpenSSH - configure sftp-server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.11	OpenSSH: Ensure MaxAuthTries is set to 4 or less (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.12	OpenSSH: Ensure only strong ciphers are used (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.13	Ignore user-provided environment variables (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.2.14	OpenSSH: Regulate access to server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3	Sendmail Configuration		
3.6.3.1	/etc/mail/sendmail.cf - SmtptGreetingMessage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3.2	/etc/mail/sendmail.cf - permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.3.3	/var/spool/mqueue - permissions and ownership (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4	Login Controls: /etc/security/login.cfg		
3.6.4.1	/etc/security/login.cfg - logintimeout (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4.2	/etc/security/login.cfg - logindelay (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4.3	herald (logon message) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.4.4	/etc/security/login.cfg - pwd_algorithm (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.6.5	Remove or Disable Weak/Defunct Network Services		
3.6.5.1	NIS		
3.6.5.1.1	NIS - de-install NIS client (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.1.2	NIS - de-install NIS server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.1.3	NIS - remove NIS markers from password and group files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.1.4	NIS - restrict NIS server communication (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.2	SNMP		
3.6.5.2.1	SNMP - disable private community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.2.2	SNMP - disable system community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.2.3	SNMP - disable public community string (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.2.4	SNMP - disable Readwrite community access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.2.5	SNMP - restrict community access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.3	Remote command lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.4	Removal of entries from /etc/hosts.equiv (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.5	Removal of .rhosts and .netrc files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.5.6	Remote daemon lockdown (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.6	Service Accounts		
3.6.6.1	FTP: Prevent world access and group write to files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.6.2	FTP: Display acceptable usage policy during login (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.6.3	FTP: Disable root access to ftp (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.7	Trusted Execution (TE)		
3.6.7.1	TE - implementation (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8	Trusted Files and Directories		
3.6.8.1	Trusted Directories		
3.6.8.1.1	Ensure all directories in root PATH deny write access to all (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.2	Home directory must deny write to all except owner (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.3	/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.4	/etc/security (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.5	/etc/security/audit (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.6	/var/adm/ras (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.7	/var/adm/sa (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.1.8	/var/spool/cron/crontabs (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2	Trusted Files		
3.6.8.2.1	crontab entries - owned by userid (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.2	Home directory configuration files (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.3	/smit.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.4	/etc/group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.5	/etc/inetd.conf (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

3.6.8.2.6	/etc/motd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.7	/etc/passwd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.8	/etc/ssh/ssh_config (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.9	/etc/ssh/sshd_config (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.10	/var/adm/cron/at.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.11	/var/adm/cron/cron.allow (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.12	/var/ct/RMstart.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.13	/var/adm/cron/log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.14	/var/tmp/dpid2.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.15	/var/tmp/hostmibd.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.8.2.16	/var/tmp/snmpd.log (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.9	Ensure root access is controlled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.10	Disable core dumps (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.11	Remove current working directory from default /etc/environment PATH (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.12	Remove current working directory from root's PATH (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.13	Lock historical users (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.14	Configuration: /etc/motd (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6.15	Unattended terminal session timeout is 900 seconds (or less) (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Audit Log Management		
3.7.1	Syslog		
3.7.1.1	Configuring syslog - local logging (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1.2	Configuring syslog - remote logging (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.1.3	Configuring syslog - remote messages (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.7.2	AIX Auditing (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
May 4, 2021	2.0.0	Map to both version 8 and version 7 of the CIS Controls (Ticket 13856)
May 5, 2021	2.0.0	#31 4.16.1 General Permissions Management - suid and sgid files and programs (Ticket 3613)
May 5, 2021	2.0.0	#46 Typo in Section 4.4.6 (Ticket 3626)
May 6, 2021	2.0.0	#47 Section 4.2.1 - Shouldn't this be Level 1? (Ticket 3627)
May 6, 2021	2.0.0	#53 4.11.19 - Audit fails for user nobody (Ticket 3631)
May 6, 2021	2.0.0	#58 4.11.7 Permissions and Ownership - /var/adm/cron/log (Ticket 3633)
Jun 2, 2021	2.0.0	Introduction: needs update (Ticket 12668)
Jun 3, 2021	2.0.0	Move Items and delete Misc. Section (Ticket 12982)
Jun 4, 2021	2.0.0	Rename recommendations for /etc/security/user default stanza (Ticket 13071)
Jun 10, 2021	2.0.0	Rename individual recommendations within /etc/rc.tcpip (Ticket 13104)
Jun 10, 2021	2.0.0	Rename individual recommendations within /etc/inittab (Ticket 13105)
Jun 10, 2021	2.0.0	Recommendations on sudo configuration (Ticket 13074)
Jun 10, 2021	2.0.0	The introduction text exceeds a mere introduction. Reorganize. (Ticket 12823)
Jun 10, 2021	2.0.0	AIXPert Security Levels needs to be expanded to AIX 7.1 levels (Ticket 12669)
Jun 10, 2021	2.0.0	Review AIX 7.1 tickets for `Critical` to AIX Benchmark v2.0.0.0 (Ticket 13106)

Jun 10, 2021	2.0.0	Remove logindisable and related recommendations from Benchmark (Ticket 12971)
Jun 10, 2021	2.0.0	Is requirement for logininterval backwards? (Ticket 13049)
Jun 11, 2021	2.0.0	no_root_squash and use of smitty (Ticket 13110)
Jun 11, 2021	2.0.0	Add nodev option, also use lsnfsmnt and chnfsmnt for automation/audit/etc. (Ticket 13115)
Jun 11, 2021	2.0.0	NFS access: modify commands to improve automation (Ticket 13116)
Jun 11, 2021	2.0.0	Remove "backup and reboot" (Ticket 13068)
Jun 11, 2021	2.0.0	Benchmark Approach - what about existing systems? (Ticket 9852)
Jun 11, 2021	2.0.0	Create Milestone Object AIX 7.1 v2.1.0.0 (Ticket 13108)
Jun 17, 2021	2.0.0	remove TCP_Wrappers (Ticket 13143)
Jun 22, 2021	2.0.0	Overview/Summary - needs updates to reflect "the world in 2020" (Ticket 9854)
Jun 22, 2021	2.0.0	Validate whether Protocol 2 is still required (Ticket 13171)
Jun 22, 2021	2.0.0	Update ntalk/talk/write recommendation. Simply disable (Ticket 13048)
Jun 22, 2021	2.0.0	Duplicate and conflict with 3.1.2.8 (Ticket 13163)
Jun 23, 2021	2.0.0	rstatd - may be needed (Ticket 13180)
Jun 23, 2021	2.0.0	increase loginretries from 3 to 5 (Ticket 13156)
Jun 24, 2021	2.0.0	Switch recommendation from Level 2 to Level 1 (Ticket 13076)
Jun 25, 2021	2.0.0	locking down sshd_config breaks sftp access. This requires permissions of at least 644. Please revise test setting 600 breaks sftp users. (Ticket 6928)
Jun 25, 2021	2.0.0	Move sshd_config and ssh_config permissions checks to "Trusted Files and Directories" (Ticket 13216)

Jun 26, 2021	2.0.0	remove TCP_Wrappers: not standard AIX (was change to Level 2). (Ticket 13092)
Jun 26, 2021	2.0.0	remove from benchmark: archaic setting (Ticket 12973)
Jun 26, 2021	2.0.0	Set LogLevel to INFO or VERBOSE (Ticket 13203)
Jun 27, 2021	2.0.0	3.3.6.14 Configuring SSH - set Idle Timeout - remove as ineffective (Ticket 13198)
Jun 27, 2021	2.0.0	maxage should be 13 or less (Ticket 13157)
Jun 27, 2021	2.0.0	minage should be 0 (Ticket 13158)
Jun 27, 2021	2.0.0	maxrepeats=2 useless and dangerous; increase it (Ticket 13160)
Jun 27, 2021	2.0.0	verify including login=true rlogin=false with sugroups control (Ticket 13145)
Jun 29, 2021	2.0.0	Benchmark Scope - rewrite proposal (Ticket 13202)
Jun 29, 2021	2.0.0	Why is the 3.1 section only for local user accounts? (Ticket 5388)
Jun 29, 2021	2.0.0	Add command to detect OpenSSH is installed AND major version is at least `8`. (Ticket 13213)
Jul 3, 2021	2.0.0	Disable cas_agent in AIX 7.1 (Ticket 13093)
Jul 13, 2021	2.0.0	Reorganize Sub-section: "Disable execution" - rename and cleanup (Ticket 13241)
Jul 15, 2021	2.0.0	World writable files/directories - audit/remediation mismatch? (Ticket 13294)
Jul 20, 2021	2.0.0	Move de-install CDE to first recommendation (Ticket 13324)
Jul 20, 2021	2.0.0	remove rfc_1323 - as not a security setting (Ticket 13325)
Jul 20, 2021	2.0.0	UsePrivilegeSeparation is deprecated in OpenSSH 7.5 (Ticket 7186)
Jul 20, 2021	2.0.0	gated - change the Rationale (Ticket 13177)
Jul 20, 2021	2.0.0	Remove OpenSSH protocol check (Ticket 13218)
Jul 21, 2021	2.0.0	lock, rather than remove guest account (Ticket 13258)

Jul 22, 2021	2.0.0	check: login herald fails due to text error (Ticket 3636)
Jul 22, 2021	2.0.0	Remove recommendations as out of scope (Ticket 13066)
Jul 22, 2021	2.0.0	Remove recommendation as ineffective (Ticket 13067)
Jul 22, 2021	2.0.0	minother, minuppervalpha, minother, etc.: change the text (Ticket 13159)
Jul 22, 2021	2.0.0	Config - ftp umask (Ticket 3637)
Jul 22, 2021	2.0.0	Introduction - verify levels supported (Ticket 9851)
Jul 27, 2021	2.0.0	Verify new histexpire value is '13' (Ticket 13144)
Jul 28, 2021	2.0.0	remove submit.cf from 7.1 benchmark (Ticket 13382)
Jul 29, 2021	2.0.0	complete new recommendations for AIX 7.1 v2.0.0 inetd section (Ticket 13134)
Jul 29, 2021	2.0.0	Most audit checks in section 'inetd aka Super Daemon' don't do what is intended (Ticket 3628)
Jul 29, 2021	2.0.0	Check permissions on crontabs? (Ticket 13070)
Jul 29, 2021	2.0.0	portmap daemon: update audit and remediation to use AIX commands such as chrctcp. (Ticket 13240)
Jul 29, 2021	2.0.0	rsprayd - not for NFS (Ticket 13181)
Jul 29, 2021	2.0.0	Change Secure NFS to use chnfsexp -S (Ticket 13282)
Jul 29, 2021	2.0.0	timed = level 1 ? (Ticket 13179)
Jul 29, 2021	2.0.0	OpenSSH server: Add SFTP configuration (Ticket 13214)
Jul 29, 2021	2.0.0	Restructure trusted files & directories (Ticket 13391)
Jul 29, 2021	2.0.0	Rewrite recommendation to Lock rather than Remove historical accounts (Ticket 13256)
Aug 1, 2021	2.0.0	Host directory permissions needs update (Ticket 13395)
Aug 6, 2021	2.0.0	AIX Security Expert coverage presented as a table (Ticket 12894)

Aug 6, 2021	2.0.0	Remediation: lock accounts without password (Ticket 9850)
Aug 16, 2021	2.0.0	Draft published for consensus review
Sep 1, 2021	2.0.0	Audit procedure contains remediation (locking of users) (Ticket 13617)
Sep 1, 2021	2.0.0	Audit procedure doesn't check all the accounts (Ticket 13618)
Sep 1, 2021	2.0.0	Typo in Audit procedure (Ticket 13650)
Sep 1, 2021	2.0.0	Typo in Audit procedure (Ticket 13649)
Sep 1, 2021	2.0.0	Typo in Audit procedure (Ticket 13651)
Sep 1, 2021	2.0.0	Another variant of FTP banner (Ticket 13647)
Sep 1, 2021	2.0.0	sshd default value - prohibit-password (Ticket 13641)
Sep 3, 2021	2.0.0	Set LogLevel to INFO or VERBOSE (Ticket 13642)
Sep 3, 2021	2.0.0	Issues with 3.3.5.1 (Ticket 13638)
Sep 3, 2021	2.0.0	Rename the title (Ticket 13639)
Sep 27, 2021	2.0.0	Typo in remediation procedure (Ticket 13623)
Sep 27, 2021	2.0.0	The value should not be 0 (Ticket 13624)
Sep 27, 2021	2.0.0	Typo in the last sentence (Ticket 13625)
Sep 27, 2021	2.0.0	If ftp is not active, no sense to test it (Ticket 13626)
Sep 27, 2021	2.0.0	Check sudo (audit procedure) (Ticket 13627)
Sep 27, 2021	2.0.0	DPI is not SNMP v2 (Ticket 13634)
Sep 28, 2021	2.0.0	more information about CIS Critical Controls is required (Ticket 13615)
Sep 28, 2021	2.0.0	Impact statement - part of the text from another control (Ticket 13640)
Sep 28, 2021	2.0.0	3.2.4 and 3.2.5??? (Ticket 13628)
Sep 28, 2021	2.0.0	3.2.6 and 3.2.7? (Ticket 13629)

