

CIS IBM AIX 7 Benchmark

v1.2.0 - 03-31-2026

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/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

DRAFT

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	4
Important Usage Information.....	4
Target Technology Details	7
Intended Audience	7
Consensus Guidance	8
Typographical Conventions	9
Recommendation Definitions.....	10
Title	10
Assessment Status	10
Automated	10
Manual.....	10
Profile	10
Description	10
Rationale Statement	10
Impact Statement.....	11
Audit Procedure.....	11
Remediation Procedure	11
Default Value	11
References	11
CIS Critical Security Controls® (CIS Controls®)	11
Additional Information	11
Profile Definitions	12
Acknowledgements	13
Recommendations	14
Appendix: Summary Table	522
Appendix: CIS Controls v7 IG 1 Mapped Recommendations	Error! Bookmark not defined.
Appendix: CIS Controls v7 IG 2 Mapped Recommendations	Error! Bookmark not defined.
Appendix: CIS Controls v7 IG 3 Mapped Recommendations	Error! Bookmark not defined.

Appendix: CIS Controls v7 Unmapped Recommendations..... Error! Bookmark not defined.

Appendix: CIS Controls v8 IG 1 Mapped Recommendations Error! Bookmark not defined.

Appendix: CIS Controls v8 IG 2 Mapped Recommendations Error! Bookmark not defined.

Appendix: CIS Controls v8 IG 3 Mapped Recommendations Error! Bookmark not defined.

Appendix: CIS Controls v8 Unmapped Recommendations..... Error! Bookmark not defined.

Appendix: Change History 536

DRAFT

Overview

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

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

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

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

This document, Security Configuration Benchmark for AIX 7, provides prescriptive guidance for establishing a secure configuration posture for AIX version 7.x running on the POWER Systems platform.

This document was tested against AIX 7.2 TL05 and AIX 7.3 TL02.

The guidance within broadly assumes that operations are being performed as the **root** user, and executed under the default **ksh** version for the operating system. Operations performed using **sudo** instead of the **root** user, or executed under another shell, may produce unexpected results, or fail to make the intended changes to the system. Non-root users may not be able to access certain areas of the system, especially after remediation has been performed. If the **root** user has interactive commands within their **.profile** then operations may produce unexpected results or fail to run. 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.

The default prompt for the **root** user is **#**, and as such all sample commands will have **#** as an additional indication that it is to be executed as **root**.

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 on the POWER Systems platform.

A working knowledge of **vi** (or other editor already installed) is assumed in order to implement some of the configuration changes. A working knowledge of AIX **smit** is recommended as **\${HOME}/smit.scripts** and/or **F6** panel can help with implementing complex remediation and/or audit scripts.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<Monospace font in brackets>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Level-1 Benchmark recommendations are intended to:

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

- **Level 2**

Level-2 Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Acknowledgements

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

This benchmark is based upon previously published AIX benchmarks 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

Bhargavi Reddy
Graham Eames
Anoop Mourya

Editor

Eric Pinnell
Randie Bejar
Michael Wood
Gokhan Lus

Recommendations

1 Benchmark Organization

This benchmark provides security configuration guidance for use during the configuration of the AIX Operating System.

This guide has consolidated previous guides into one - for AIX version 7 - rather than two or three guides. Experience has shown that a new release of AIX has minimal impact on existing recommendations. Our goal is a single guide for the current releases of AIX - currently AIX 7.2 and AIX 7.3. The recommendations in this guide are regularly tested on different versions of AIX.

Recommendations are organized following the CIS Security Guidelines, version 8.

Differences with previous benchmarks

Nearly all recommendations have had their name changed. The goal is to have a uniform naming style for all *nix (ie, Linux and AIX) based benchmarks.

The required SHELL is /bin/ksh

AIX has used the Korn Shell for over 25 years as it's default shell. And AIX standard commands provided as part of BOS (base operating system) expect **ksh** to be the standard shell. When a different command interpreter is needed, e.g., `/usr/bin/perl` that is specified in the first line of the command using the "hash-bang" convention, i.e. `#!/usr/bin/perl ....`

In short, trying to use a different shell (e.g., bash) will likely break many of the recommended audit and/or remediation proposals.

ROOT user may not have an interactive login process

All **audit** and **remediation** proposals assume an automated (ie, non-interactive) process. If your **root** user definition starts an interactive login procedure this may prevent an automated **audit** from completing.

The **root** user cannot have an interactive command as part of the login procedure. An **AUDIT** or **REMEDIATION** of an AIX system requires root authority. Ideally, root access is gained using **su** (switch user) to *root* rather than a direct login session. A third party resource, e.g., from the AIX Toolbox, might be used to install the command **sudo** so that knowledge of the root password is not required. However, the command **sudo** (not covered in this benchmark) requires its own security audit and remediation process to make sure it's presence does not become an unwelcome backdoor.

More specifically, there are a few recommendations that require the use of **su - root -c "some command syntax"**. This means that an interactive login procedure will hang an *automated* hands-free **AUDIT** of an AIX system. Note: there is a new recommendation that states an interactive root login is not allowed.

CIS Controls Design Principles

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

CIS Defense Model (CDM) version 2

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

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

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

Implementation Groups

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

- IG1 - Implementation Group 1

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

- IG2 - Implementation Group 2 (Includes IG1)

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

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

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

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

Additional Information

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

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

Running the benchmark

As stated above, the benchmark **document** is organized into sections based on major *CIS Controls Sections*. Within these sections there are recommendations and sub-sections with recommendations. Wherever possible, recommendations are ordered alphabetically. As such, do not expect an **audit run** based on the document order to succeed in a single pass. This is a complex activity and you may need to re-run and remedy multiple times before the task is completed).

Security Management is an on-going process

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

1.1 Benchmark Principles, Conventions and Assumptions

This benchmark provides security configuration guidance for use during the configuration of the AIX 7 Operating System. The recommendations are organized into chapters based on **CIS Controls v8**. The chapters are organized into sub-sections, as needed, by AIX BOS OS technology and/or standard services.

Guiding principles

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

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

Section Naming and Recommendation Ordering

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

Implementation of Recommendations is not linear

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

Scenarios

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

Benchmark scope and prerequisites

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

Assumptions

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

1.2 HOWTO use this benchmark

Again, the benchmark envisions two scenarios:

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

Fresh Installation - better for first-time users

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

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

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

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

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

1.3 AIX - Installation methods

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

Below shows three methods to install AIX.

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

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

1.3.1 AIX RTE Installation

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

AIX Installation - RTE mode

- This example is to assist you with setting up an AIX system for the "First Time Scenario". This can also be used to build a new so-called "gold image".
- Within the AIX Base Operating System Installation Menus it is recommended that the following options are selected:
- **NOTE: *Trusted AIX* and *_Secure by Default_* installation modes are only available with AIX 7.2. *Secure by Default* is not recommended by CIS as an installation mode.**

```
Security Models

Type the number of your choice and press Enter.

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

Standard Security Options

Type the number of your choice and press Enter.

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

Install Options

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

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

```
Install More Software

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

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

Installation Summary

```
Overwrite Installation Summary

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

Optional Software being installed:

>>> 1 Continue with Install
```

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

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

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

- Secure By Default = no*

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

1.3.2 AIX MKSYSB Installation

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

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

DRAFT

1.3.3 AIX 7.2 installation

DRAFT

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

AIX Installation - Using security profiles

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

Review

- Security profile is a AIX product that specifies security requirements for general-purpose operating systems in

networked environments. This profile establishes the requirements necessary to achieve the security objectives of the Target of evaluation (TOE) security function and its environment. Security profile contains a base package and several extended packages. Products that are related to Security profile base package support are Identification and Authentication, Discretionary Access Control (DAC), Auditing, Cryptographic Services, Management of Security Mechanisms, and Trusted Channel communications. Security profile includes additional, optional packages for Labeled Security, Integrity Verification, Advanced Audit, General Purpose Cryptography, Advanced Management, Extended Identification and Authentication, Trusted Boot, and Virtualization.

- System administrators can install a system with the Base AIX Security (BAS) and Evaluation Assurance

Level 4+ (EAL4+) option or Labeled AIX Security (LAS) and Evaluation Assurance Level 4+ (EAL4+) during a base operating system (BOS) installation. A system with these options has restrictions on the software that is installed during BOS installation, plus network access is restricted.

- Above is taken from AIX Security.pdf

BAS (Basic AIX Security) Installation

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

Security Models

Type the number of your choice and press Enter.

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

- Choose option 2

Standard Security Options

Type the number of your choice and press Enter.

1. Secure by Default..... no
 2. BAS and EAL4+ Configuration Install..... yes
 3. Trusted Computing Base Install..... no
- >>> 0 Continue to more software options.
- 88 Help ?
99 Previous Menu
- >>> Choice [0]:

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

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

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

AIX BAS preparation

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

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

1.3.3.2 Ensure SSH client and server packages are installed on AIX 7.2

Profile Applicability:

- Level 1

Description:

SSH client and server packages can be automatically installed as part of the base system to provide secure network login capabilities.

On AIX 7.3 these packages are automatically installed on all systems, but on AIX 7.2 are an option.

Rationale:

The **telnet** protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The **ssh** protocol provides an encrypted session and stronger security.

Audit:

Remediation:

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	16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

1.3.4 AIX 7.3 Installation

DRAFT

1.3.4.1 Ensure Secure by Default is selected during the installation

Profile Applicability:

- Level 1

Description:

Secure By Default (SbD) is the concept of installing a minimal set of software in a secure configuration.

The AIX Secure by Default (SbD) installation option installs a lighter version of the TCP client and server filesets, that excludes vulnerable commands and files. The `bos.net.tcp.client` and `bos.net.tcp.server` filesets are part of the SbD installation and contain all commands and files except for any applications that allow for the transmission of passwords over the network in clear text format such as telnet and ftp. In addition, applications that might be used, such as rsh, rcp, and sendmail, are excluded from the SbD filesets.

The final automated process of the SbD install is to impose the AIX Security Expert high-level security configuration settings. You can do this by running the `aixpert` command from `/etc/firstboot` script: `/usr/sbin/aixpert -f /etc/security/aixpert/core/SbD.xml -p 2>/etc/security/aixpert/log/firstboot.log`

The differences between an SbD-installed system and a regular installation with an AIX Security Expert High Level Security configuration is best illustrated by examining the telnet command. In both cases, the telnet command is disabled. In an SbD installation, the telnet binary or application is never even installed on the system.

Rationale:

Many legacy services send passwords over the network in clear text and as such their use is discouraged. Whilst many of these packages can be uninstalled later, it is preferable that they are not installed on the system in the first place in order to minimise the risk.

Audit:

Remediation:

The Secure by Default option can be found under option 3 of the Installation and Settings menu

Installation and Settings

Either type 0 and press Enter to install with current settings, or type the number of the setting you want to change and press Enter.

```
1  System Settings:
    Method of Installation.....New and Complete Overwrite
    Disk Where You Want to Install.....hdisk0

2  Primary Language Environment Settings (AFTER Install):
    Cultural Convention.....English (United States)
    Language .....English (United States)
    Keyboard .....English (United States)
    Keyboard Type.....Default
3  Security Model.....Default
4  More Options  (Software install options)
5  Select Edition.....standard
>>> 0  Install with the current settings listed above.

88  Help ?          | +-----+
99  Previous Menu   | | WARNING: Base Operating System Installation will
                    | | destroy or impair recovery of ALL data on the
                    | | destination disk hdisk0.
>>> Choice [0]:
```

References:

1. <https://www.ibm.com/docs/en/aix/7.3?topic=expert-secure-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.		●	●

1.4 AIX Patch Management

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

No Security without regular updates/patching

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

- AIX Level Naming
 - Releases

Shipped approximately every 4 years

- Technology Levels

Technology Levels contain software enhancements, new hardware exploitation, and defect fixes.

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

- Service Packs

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

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

- Build Sequence Identifier
- Planned Maintenance and Service Pack Updates

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

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

Additional Hints and Recommendations in the *White Paper*.

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

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

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

AIX Resources

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

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

[AIX Service Strategy and Best Practices]

(<https://www.ibm.com/support/pages/aix-service-strategy-and-best-practices>)

Applying AIX updates/upgrades

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

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

1.5 Summary

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

Review Bulletins

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

- The security fixes published in the vulnerability advisories are posted here for download:

<https://aix.software.ibm.com/aix/efixes/security>

- The Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) provides security and HIPER (High Impact PERvasive) reports based on the inventory of your system. FLRTVC Script is a ksh script which uses FLRT security and HIPER data (CSV file) to compare the installed filesets and interim fixes against known vulnerabilities and HIPER issues.

- 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>

DRAFT

2 Inventory and Control of Assets

This section combines two controls:

- [CIS Control 01: Inventory and Control of Enterprise Assets](#)

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

- [CIS Control 02: Inventory and Control of Software Assets](#)

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Why Are These Controls Critical?

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

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

How do these controls apply to AIX and/or POWER

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

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

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

DRAFT

2.1 Ensure system configuration is documented and verified regularly

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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

Audit:

- Verify there is a regular, automated, process to extract the system configuration and append it to a syslog.

```
# /usr/bin/crontab -l | /usr/bin/egrep "/usr/sbin/lsconf -v" >/dev/null ||  
print "missing cronjob to call /usr/sbin/lsconf ' -v\'"
```

- Verify there is a setting in **/etc/syslog.conf** to collect **local1.info** messages to a local log file.

```
# /usr/bin/egrep "syslog/inventory.log " /etc/syslog.conf >/dev/null || print  
"Missing syslog/inventory.log entry in syslog.conf"
```

Both commands above should not return any output

Remediation:

- Below may be considered an example of how to setup a regular (daily) verification of the system configuration. The actual frequency you use might differ. The **keyword** in the recommendation is: *regular*.
- Further, the example also shows two **syslog** reporting lines: one to a system file, the second to a centralized **syslog** service.

The second entry is added as a comment because the hostname is likely not correct and/or there is not a centralized **syslog** server.

- The syslog **facility** *local1* is used to keep these reports out of the standard syslog facilities. There is not meant to establish a requirement to use facility **local1**. An alternate facility can be used as per site policy.

Ensure that the log directory and file exist

```
# /usr/bin/mkdir -p /var/log/syslog
# /usr/bin/touch /var/log/syslog/inventory.log
```

If logging for **local1.info** events is not already configured add this to the **syslog** configuration:

```
#!/usr/bin/ksh
/usr/bin/egrep "^local1.info /var/log/syslog/inventory.log" /etc/syslog.conf
>/dev/null
if [ $? != 0 ]; then
    print "local1.info /var/log/syslog/inventory.log rotate time 1d files 30
compress" >> /etc/syslog.conf
    refresh -s syslogd || startsrc -s syslogd
fi
```

Add an entry to the root **crontab** if it is not already present

```
#!/usr/bin/ksh
/usr/bin/crontab -l | /usr/bin/egrep "/usr/sbin/lsconf -v" >/dev/null
if [ $? != 0 ]; then
    print "0 0 * * * /usr/sbin/lsconf -v | /usr/bin/logger -p local1.info -t
Inventory" >> /var/spool/cron/crontabs/root
    /usr/sbin/lsconf -v | /usr/bin/logger -p local1.info -t Inventory
fi
```

The scheduling is an example and should be configured according to site policy

Additional Information:

NOTE: while the audit and remediation can verify and/or create commands to collect information a process outside of the system is needed to verify the reported information is the expected result.

CIS Controls:

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

2.2 Ensure Trusted Execution Path is enabled

Profile Applicability:

- Level 2

Description:

The recommendation is to activate **TE** to enhance system integrity by specifying authorized locations for applications to hamper attacks from unauthorized locations using *Trojan horse* style tactics.

Rationale:

TE provides a robust system integrity checking process.

Hackers utilize any opening they can find to infiltrate a system. One common attack pattern includes getting an unauthorized program (aka Trojan horse) installed anywhere on the target system. One of the integrity checks **TE** provides is an *authorized* aka *allowed* aka Trusted Execution Path (**TEP**).

Enforcing a **TEP** is a low invasive mechanism of TEP and provides a high level continuous system integrity. This ensures that programs are only executed from well-defined (*allowed*) locations. Best practice installation and maintenance (e.g., system updates) are needed to ensure only trusted programs are installed in these locations and not malicious code masquerading as a true program.

Impact:

Testing is recommended. An additional directory may be needed, e.g., for trusted applications not installed in the BOS default locations.

Additional QA testing should verify that only directories actually needed are included in the TEP - otherwise an unnecessary, perhaps un-watched, directory leaves a potential for an attack.

Audit:

- Ensure that TE and TEP are enabled
- Also verify that the output includes the expected `${PATH}` look-alike string. We do not provide a `${PATH}` here, that is for your implementation.

```
trustchk -p TE TEP
```

The above command should yield the following output:

```
TE=ON
TEP=ON
TEP=_A ${PATH} like string_ # Yours will be unique to your location
```

Remediation:

NOTE: Your configuration of TE is dependent on the unique requirements of your environment.

To configure **TE** to enforce a *Trusted Execution Path (TEP)* you need to know the intended secure path. e.g., `SecurePath="/usr/bin:/usr/sbin"`

Perform the following:

```
# First disable both TE and TEP
trustchk -p TE=OFF TEP=OFF
# Set the secure TEP variable
trustchk -p TEP=${SecurePath}
# Enable TE and TEP
trustchk -p TE=ON TEP=ON
```

Further details regarding planning and implementation of TE can be found within the IBM AIX 7 Infocentre:

<https://www.ibm.com/docs/en/aix/7.3?topic=configuration-trusted-execution>

Default Value:

Not enabled

References:

1. <https://www.ibm.com/docs/en/aix/7.3?topic=configuration-trusted-execution>

Additional Information:

Reversion:

- Disable only TEP

```
trustchk -p TEP=OFF
```

- Disable **all** Trusted Execution mechanisms including TEP, regardless of their settings

```
trustchk -p TE=OFF
```

DRAFT

2.3 Ensure Trusted Execution (TE) policies are locked

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Impact:

To revert this setting and/or to be able to make modifications this policy must first be switched off using **trustchk -p LOCK_KERN_POLICIES=OFF** followed by a **reboot**.

Audit:

Run the command

```
trustchk -p LOCK_KERN_POLICIES
```

The output should be

```
LOCK_KERN_POLICIES=ON
```

Remediation:

Execute the following command

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

2.4 Ensure Unauthorized Applications are reported

Profile Applicability:

- Level 1

Description:

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

Rationale:

Trusted Execution (TE) provides an additional layer of access controls to processes on top of the base Discretionary Access Controls. Monitoring how processes access system resources can improve awareness of system integrity.

Impact:

As long as the TE policies **STOP_UNTRUSTD** and **STOP_ON_CHKFAIL** are **OFF** the TE security subsystem will only log *allowlist* omissions.

Audit:

1. Run the following command to verify **TE=ON** and **CHKEEXEC=ON**:

```
# /usr/sbin/trustchk -p TE CHKEEXEC
```

Verify the output includes:

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

2. Run the following command to verify syslog is configured to collect **kern.info** data:

```
# /usr/bin/grep "kern.info" /etc/syslog.conf
```

Example output:

```
kern.info /var/log/syslog/kernel.log rotate time 1d files 30 compress
```

Note: Log retention periods should be configured as per site policy.

- This will provide entries similar to:

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

Remediation:

1. Run the following command:

```
# /usr/sbin/trustchk -p TE=ON CHKEEXEC=ON
```

2. If logging for **kern.info** events is not already configured:

Run the following commands:

```
# /usr/bin/mkdir -p /var/log/syslog  
# /usr/bin/touch /var/log/syslog/kernel.log  
# print "kern.info /var/log/syslog/kernel.log rotate time 1d files 30 compress" >> /etc/syslog.conf  
# /usr/bin/refresh -s syslogd || /usr/bin/startsrc -s syslogd
```

Note: Log retention periods should be configured as per site policy.

Default Value:

TE=OFF

CIS Controls:

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

2.5 Ensure Allowlist violations are enabled

Profile Applicability:

- Level 2

Description:

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

Rationale:

Trusted Execution (TE) provides an additional layer of access controls to processes on top of the base Discretionary Access Controls. Monitoring how processes access system resources can improve awareness of system integrity.

Impact:

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

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

TROJAN Stops the loading of files that do not belong to the TSD and have one of the following security settings:

- * Have suid/sgid bit set
- * Linked to a file in the TSD
- * Have entry in the privcmds Database
- * Be linked to a file in the privcmds database

Audit:

- Execute the command:

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

- This should return either:

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

or

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

Remediation:

- Execute one of the following commands:

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

or

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

Default Value:

TE=OFF

CIS Controls:

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

2.6 Ensure regular scans for unauthorized applications

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

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

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

What is a Trojan?

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

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

Summary:

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

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

Audit:

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

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

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

Remediation:

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

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

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

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

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

CIS Controls:

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

2.7 Ensure unused symbolic links are removed

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

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

Impact:

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

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

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

Audit:

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

```
find -L / \( -fstype jfs -o -fstype jfs2 \) -type l -ls 2> /dev/null
```

No output should be returned

Remediation:

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

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

CIS Controls:

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

3 Configure Data Protection

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

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

Why is this Section Critical

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

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

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

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

3.1 Ensure default user umask is configured

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 permissive **umask** value could result in directories or files with excessive permissions that can be read and/or written to by unauthorized users.

Audit:

Run the following to verify the default user **umask** is set to **027**(octal) or **u=rwx,g=rx,o=** (Symbolic) to enforce newly created directories' permissions to be **750** (**drwxr-x---**), and newly created file's permissions be **640** (**rw-r-----**), or more restrictive:

```
lssec -f /etc/security/user -s default -a umask | grep -Eq "^default  
umask=[0-7]?[2367]7$" || echo "umask is insufficiently restrictive"
```

No output should be returned.

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.			

3.2 Ensure world writable directories have the SVTX bit set

Profile Applicability:

- Level 1

Description:

The system is audited for world writable directories.

Rationale:

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

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

Impact:

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

Audit:

Execute the **find** command.

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

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

The output should be empty.

Remediation:

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

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

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

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

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

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

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

Default Value:

N/A

CIS Controls:

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

3.3 Ensure there are no system 'default group' writable files (objects)

Profile Applicability:

- Level 2

Description:

The system is audited for *group* writable files that belong to one of the default AIX groups.

Rationale:

An audit should be performed on the system to search for the presence of group writable files and devices. (Directories are covered in a separate recommendation).

The preference is **no** world writable files (objects) - using a group defined by system installation.

Audit:

Execute the script below.

Using the following find all world writable objects (excluding symbolic links and directories) on local filesystems only.

If you use the verbose (long) option and you see a symbolic link this means the target being referenced is not available.

```
#!/usr/bin/ksh -e
PID=$$
VERBOSE=$1
AUDIT=/var/tmp/cis-3.3.audit-${PID}.ksh
umask 077
print "find -L / \\( -fstype jfs -o -fstype jfs2 \\) ! -type d -perm -g+w \\\" >${AUDIT}
OR=" \"
lsgroup -a admin ALL | grep true | while read sys_group rest; do
    printf \"%s -group %s \\\"\\\"\\n\" ${OR} ${sys_group} >>${AUDIT}
    OR="-o \"
done
print \"\\\" \" ${VERBOSE:+-ls} >>${AUDIT}
ksh ${AUDIT}
rm ${AUDIT}
```

NOTE: If there is a lot of output repeat the command but add an argument to get the long listing. With the long list you can focus on one group at a time.

Remediation:

- Review the currently mounted local filesystems using the following to find all world writable files on local JFS/JFS2 filesystems only:
- Note: the list generated by the command below is for all groups, not just the default system groups.
- the command without the argument **-ls** will create a list than can be fed to **/usr/bin/xargs** to *blindly* remove the group write permissions.

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

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

Default Value:

N/A

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.4 Ensure world writable files are secured

Profile Applicability:

- Level 1

Description:

The system is audited for world writable files.

Rationale:

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

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

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

Audit:

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

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

No output should be returned

Remediation:

Run the following command to remove the write bit from other:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -o+w -exec chmod o-w {} +
```

Default Value:

N/A

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.5 Ensure there are no group staff writable files

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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

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

Audit:

Run the following command to find all group staff writable files:

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

Remediation:

Run the following command to remove the write bit for the group **staff**:

```
find / \( -fstype jfs -o -fstype jfs2 \) -type f -perm -g+w -group staff -  
exec chmod g-w {} +
```

Default Value:

N/A

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 <u>Configure Data Access Control Lists</u> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 <u>Protect Information through Access Control Lists</u> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

3.6 Ensure no files or directories without an owner and a group exist

Profile Applicability:

- Level 1

Description:

Administrators may delete users or groups from the system and neglect to remove all files and/or directories owned by those users or groups.

Rationale:

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

Audit:

Run the following command to verify no unowned or ungrouped files or directories exist:

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

No output should be returned.

NOTE: On systems with a large number of files and/or directories, this audit may be a long running process. Local knowledge of the system may be used to narrow the locations which are searched.

Remediation:

Set ownership and group ownership of these files and/or directories to an active user on the system:

```
# /usr/bin/chown <owner> <file>
# /usr/bin/chgrp <group> <file>
```

- **OR -**

Remove the file/directory:

```
# [[ -f <file> ]] && /usr/bin/rm -f <file>
# [[ -d <file> ]] && /usr/bin/rmdir <file>
```

Default Value:

N/A

Additional Information:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4 Secure Configuration of Enterprise Assets and Software

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

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

Why is this Section Critical?

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

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

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

4.1 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.

DRAFT

4.1.1 Configure Trusted Files

Trusted Files are files that are key to maintaining system integrity. Two common groups of trusted files are: a) user/application configuration files and b) log files.

Configuration Files should be added to the TSD database. If they are not meant to be changed under normal operations they should be added with a signature, otherwise add with SIZE=VOLATILE.

In all cases the file owner/group ids, and file mode should be specified.

- An excerpt of a VOLATILE file entry:

```
trustchk -q /etc/passwd
/etc/passwd:
    owner = root
    group = security
    mode = TCB,644
    type = FILE
    hardlinks =
    symlinks =
    size = VOLATILE
    cert_tag =
    signature = VOLATILE
    hash_value = VOLATILE
```

- An excerpt of a signed configuration file:

```
/usr/lib/boot/chrp.cd.proto:
    owner = root
    group = system
    mode = 400
    type = FILE
    hardlinks =
    symlinks =
    size = 3933
    cert_tag = 00d3cbd2922627b209
    signature =
7b41ae27dd44b543c35640e3e64c77ed7302c15e207855caa20e23f4fcf27db56dbfb854a24ee
a37fec15372a0f7c36467f325f5d8ad3a8256151a6a722d
416ad6b8676bcf70823ffb9fd3f890af0d8d8de51421e2fa2cb791556564873e605e4e455c587
42422c4f9580b6e44e0597ceb0f2fd6635af7f0b5bcc7d45d992600
    hash_value =
9f7592e3889cdb8825b641006bbdc855a9b036d3b9b11e6036d9faffda07eb3c
```

4.1.1.1 Ensure access on root user smit.log is configured

Profile Applicability:

- Level 1

Description:

The **smit.log** file in the HOME directory of root 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:

Run the following command to validate the permissions of the root user's **smit.log**:

```
HOME=~root
if (test ${HOME} != "/")
then
    HOME=${HOME}/
fi
ls -l ${HOME}smit.log | awk '{print $1 " " $3 " " $4 " " $9}' | grep -v "\-rw-r-----"
```

No output should be returned.

Remediation:

Remove world read and write access to the root user's **smit.log**:

```
HOME=~root
if (test ${HOME} != "/")
then
    HOME=${HOME}/
fi
chmod u=rw,g=r,o-rwx ${HOME}smit.log
chown root:system ${HOME}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.			

4.1.1.2 Ensure access on /etc/group is configured

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.			

4.1.1.3 Ensure access on /etc/inetd.conf is configured

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.			

4.1.1.4 Ensure access on /etc/motd is configured

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 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.1.1.5 Ensure access on /etc/passwd is configured

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.	●	●	●

4.1.1.6 Ensure /etc/mail/submit.cf access is configured

Profile Applicability:

- Level 1

Description:

From 7.2.4, sendmail is updated to version 8.15.2, there is a new configuration file /etc/mail/submit.cf. Ensure the permission is changed to -rw-r----- (0640).

Rationale:

Privileged access to make changes to this configuration file /etc/mail/submit.cf.

Impact:

It will not impact the usability of application or system.

Audit:

```
perl -e 'printf "%o\n", (stat shift)[2] & 07777' /etc/mail/submit.cf
```

The result should be:

640

Remediation:

```
chmod u=rw,g=r,o= /etc/mail/submit.cf
```

Default Value:

644 (-rw-r--r--)

References:

1. Reference to manpage

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.			

4.1.1.7 Ensure access to /etc/ssh/ssh_banner is configured

Profile Applicability:

- Level 1

Description:

The contents of the `/etc/ssh/ssh_banner` file are displayed to users prior to login for connections via SSH.

Rationale:

-IF- the `/etc/ssh/ssh_banner` file does not have the correct access configured, it could be modified by unauthorized users with incorrect or misleading information.

Audit:

Run the following command and verify **Access** is **644** or more restrictive and **Uid** is **0/root** and **Gid** is **0/system**:

```
# ls -l /etc/ssh/ssh_banner | awk '{print $1 " " $3 " " $4 " " $9}'  
-rw-r--r--    root      system      /etc/ssh/ssh_banner
```

Remediation:

Run the following commands to set mode, owner, and group on `/etc/ssh/ssh_banner`:

```
# chown root:system /etc/ssh/ssh_banner  
# chmod u=rw,go=r /etc/ssh/ssh_banner
```

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.			

4.1.1.8 Ensure access on /etc/ssh/ssh_config is configured

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:

Run the following commands to set the mode, owner and group owner for `/etc/ssh/ssh_config`:

```
chmod u-x,go-wx /etc/ssh/ssh_config  
chown root:system /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.			

4.1.1.9 Ensure access on /etc/ssh/sshd_config is configured

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:

```
chown root:system /etc/ssh/sshd_config
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.			

4.1.1.10 Ensure access on /var/adm/cron/at.allow is configured

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
v7	3.3 Protect Dedicated Assessment Accounts Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.1.1.11 Ensure access on /var/adm/cron/cron.allow is configured

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 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.1.1.12 Ensure access on /var/adm/cron/log is configured

Profile Applicability:

- Level 1

Description:

The `/var/adm/cron/log` file contains a log of all `cron` jobs run on the system.

Rationale:

The `/var/adm/cron/log`, records all cron jobs run on the system. The file permissions must ensure that it is accessible only to its owner and group.

Audit:

Validate the permissions of `/var/adm/cron/log`:

```
ls -l /var/adm/cron/log | awk '{print $1, $3, $4, $9}'
```

The above command should yield the following output:

```
-rw-rw---- bin cron /var/adm/cron/log
```

Remediation:

Specify exact permissions and user.group ids to `/var/adm/cron/log`:

```
chmod ug=rw,o= /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.	●	●	●

4.1.1.13 Ensure access on /var/ct/RMstart.log is configured

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`:

```
# /usr/bin/ls -l /var/ct/RMstart.log | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/ct/RMstart.log
```

Permissions which are more restrictive than those listed above are also acceptable.

Remediation:

Set ownership and permissions on `/var/ct/RMstart.log`:

```
# /usr/bin/chown root:system /var/ct/RMstart.log
# /usr/bin/chmod u-x,g-wx,o-rwx /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.			

4.1.1.14 Ensure access on /var/tmp/dpid2.log is configured

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`:

```
# /usr/bin/ls -l /var/tmp/dpid2.log | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----  root      system    /var/tmp/dpid2.log
```

Permissions which are more restrictive than those listed above are also acceptable.

Remediation:

Set ownership and permissions on `/var/tmp/dpid2.log`:

```
# /usr/bin/chown root:system /var/tmp/dpid2.log
# /usr/bin/chmod u-x,g-wx,o-rwx /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.			

4.1.1.15 Ensure access on /var/tmp/hostmibd.log is configured

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`:

```
# /usr/bin/ls -l /var/tmp/hostmibd.log | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/hostmibd.log
```

Permissions which are more restrictive than those listed above are also acceptable.

Remediation:

Set ownership and permissions on `/var/tmp/hostmibd.log`:

```
# /usr/bin/chown root:system /var/tmp/hostmibd.log
# /usr/bin/chmod u-x,g-wx,o-rwx /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.			

4.1.1.16 Ensure access on /var/tmp/snmpd.log is configured

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`:

```
# /usr/bin/ls -l /var/tmp/snmpd.log | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/snmpd.log
```

Permissions which are more restrictive than those listed above are also acceptable.

Remediation:

Set ownership and permissions on `/var/tmp/snmpd.log`:

```
# /usr/bin/chown root:system /var/tmp/snmpd.log
# /usr/bin/chmod u-x,g-wx,o-rwx /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.			

4.1.1.17 Ensure access is configured for commands referenced by crontab entries

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 $6}' |grep "^/" |sort -u | while read
CMD
do
# first examine the complete command, and later parse the command for it's
directory components.
CMD=${CMD:-$(pwd) }
while [[ -a ${CMD} ]]
do
[[ "$(ls -ld ${CMD})" = @([-d]?????w? *) ]] && print " WARNING ${CMD} is
world writable"
[[ "$(ls -ld ${CMD})" = @([-d]????w???? *) ]] && print " WARNING ${CMD} is
group writable"
[[ "$(ls -ld ${CMD} |awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${CMD} is not owned by root or bin"
# parse the command PATH for correct permissions
CMD=${CMD%/*}
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 $6}' | grep "^/" | sort -u | while read
CMD
do
CMD=${CMD:-$(pwd)}
while [[ -a ${CMD} ]]
do
[[ "$(ls -ld ${CMD})" = @([-d]???????w? *) ]] && print " WARNING ${CMD} is
world writable"
[[ "$(ls -ld ${CMD})" = @([-d]????w???? *) ]] && print " WARNING ${CMD} is
group writable"
[[ "$(ls -ld ${CMD} | awk '{print $3}')" != @(root|bin) ]] && print " WARNING
${CMD} is not owned by root or bin"
CMD=${CMD%/*}
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	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.			

4.1.1.18 Ensure local interactive user dot files access is configured

Profile Applicability:

- Level 1

Description:

USER configuration files in their respective *HOME* directory e.g. **\$HOME/.profile**, should only be accessible to the owner aka UID of the file.

Rationale:

Write access to **USER** or account configuration files may enable malicious users to steal or modify other user's data, or to gain elevated privileges while **read** access may reveal secrets.

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.			

4.1.1.19 Ensure SUID and SGID files are reviewed

Profile Applicability:

- Level 1

Description:

The system is audited for both **suid** and **sgid** files and programs.

Rationale:

An audit should be performed on the system to search for the presence of both **suid** and **sgid** files and programs. In order to prevent these files from being potentially exploited the **suid** and **sgid** permissions should be removed wherever possible.

Audit:

Re-execute the appropriate find command and review the output. This should reflect the changes made in the remediation section.

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

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -type f -ls
```

If all non-local filesystems are un-mounted:

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Remediation:

Review the currently mounted filesystems:

```
mount
```

Un-mount all non-local filesystems and cdrom media:

```
umount <mount point>
```

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

```
find / \( -fstype jfs -o -fstype jfs2 \) \( -perm -04000 -o -perm -02000 \) -type f -ls
```

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

```
find / \( -perm -04000 -o -perm -02000 \) -type f -ls
```

Review the files and where possible, use the **chmod** command to remove the appropriate **suid** or **sgid** bits:

```
chmod u-s <file>  
chmod g-s <file>
```

Default Value:

N/A

Additional Information:

Reversion:

Use the **chmod** command to re-instate the **suid** and **sgid** bits to the relevant files:

```
chmod u+s <file>  
chmod g+s <file>
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.1.1.20 Ensure access on /var/tmp/snmpdv3.log is configured

Profile Applicability:

- Level 1

Description:

`/var/tmp/snmpdv3.log` is the logfile used by `snmpd` daemon for SNMPv3 connections, and contains network and machine related information.

Rationale:

The `/var/tmp/snmpdv3.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/snmpdv3.log`:

```
# /usr/bin/ls -l /var/tmp/snmpdv3.log | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r----- root system /var/tmp/snmpdv3.log
```

Permissions which are more restrictive than those listed above are also acceptable.

Remediation:

Set ownership and permissions on `/var/tmp/snmpdv3.log`:

```
# /usr/bin/chown root:system /var/tmp/snmpdv3.log
# /usr/bin/chmod u-x,g-wx,o-rwx /var/tmp/snmpdv3.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.			

4.1.2 Configure 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 = VOLATILE
```

- NOTE: IBM AIX does not include directories in the TSD by default. Fortunately, adding a directory to the TSD is an easy process.

4.1.2.1 Ensure local user Home directories exists

Profile Applicability:

- Level 1

Description:

All accounts must have a trusted started point - a **HOME** directory.

Rationale:

A missing home directory on many systems places the account in a default directory. Examples include: `/` and `/home/guest`.

This recommendation is specifically about *locally* administered accounts (in AIX terms, *-R files*). If an account exists in the local registry it must have a home directory that is accessible. This is to ensure it is not an invalid account (e.g., restored via a backup accidentally). If a valid account - it still needs a home directory.

As the difference between: *valid* account but missing a HOME directory and *invalid* account but missing a HOME directory cannot be made by a script - the recommendation is to lock the account.

Impact:

A valid user can open a ticket and get a HOME directory created or restored.

The risk of an *invalid user* gaining access via an old username is reduced.

Audit:

Ensure HOME directories exists for **local** administered accounts.

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
  uid=$(echo ${ids} | cut -f2 -d =)
  if [[ ${uid} -ge 200 ]]; then
    home=$(echo ${homes} | cut -f2 -d =)
    locked=$(echo ${locks} | cut -f2 -d =)
    if [[ ${locked} == "true" ]]; then
      continue
    elif [[ ! -d ${home} ]]; then
      /usr/bin/printf "Recommend Lock Account [%s]: Missing \${HOME} at: %-
32s\n" ${name} ${home}
    fi
  fi
done
```

- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (**uid**) greater or equal to **200**.

Remediation:

Lock local accounts with UID >= 200 when HOME directory does not exist:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "Locked Account [%s]: Missing \${HOME} at: %-32s\n"
${name} ${home}
            /usr/bin/chuser -R files account_locked=true ${name}
        fi
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	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.			

4.1.2.2 Ensure HOME directories are owned by root or the UID specified in /etc/passwd

Profile Applicability:

- Level 1

Description:

All user home directories must have a suitable owner UID.

The recommendation is to lock accounts when the HOME directory is not owned by the user or by *root*.

This recommendation may be overruled by a site-specific policy statement.

When the account is the owner - the security policy must specify that (some) accounts may have DAC authorization to modify HOME directory contents. Security policy may also specify a special UID used to own HOME directories to prevent accounts from modifying the layout and/or content of the HOME directory.

Rationale:

Manipulating home directories may enable malicious users to steal or modify data, or to gain other user's system privileges. The UID (or owner) of the HOME directory needs to be either the account or a special account defined for this purpose.

Locally* administered accounts with HOME directories owned by a **random userid will be locked.

Valid users can open a ticket to get the UID of their HOME directory corrected.

The risk of a malicious user modifying an accounts HOME directory is reduced.

Audit:

Ensure HOME directory exists and is owned by account (or root)

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; Recommend Lock Account
[%s]\n" ${home} ${name}
            continue
        else
            /usr/bin/perl -e '
                $user=$ARGV[0]; $hd=$ARGV[1]; $uid=$ARGV[2]; $huid=((stat
$hd)[4]);
                if ($huid != $uid && $huid != 0) {
                    exit(1); # triggers command after OR (||)
                }' ${name} ${home} ${uid} || \
                /usr/bin/printf "Recommend Lock Account: %s does not own
%s\n" ${name} ${home}
            fi
        fi
    fi
done
```

- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (**uid**) greater or equal to **200**.

Also, if the **HOME** directory has already been defined to something *special* (here, **/dev/null**) no **audit** is performed.

Remediation:

Review the file(s) returned by the audit procedure and perform one of the following:

- Change the ownership of the <HOME_DIRECTORY> to the appropriate user. e.g. **chown** <USER> <HOME_DIRECTORY>.
- Lock the account incorrectly associated with the <HOME_DIRECTORY>.
- Delete the <HOME_DIRECTORY>. **WARNING** This will remove the directory and all files contained in the directory from the system.

The following script may be used to lock the account referring to the <HOME_DIRECTORY>:

For all local accounts with UID >= 200:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; Run appropriate CIS
remediation\n" ${home} ${name}
            continue
        else
            /usr/bin/perl -e '
                $user=$ARGV[0]; $hd=$ARGV[1]; $uid=$ARGV[2]; $huid=((stat
$hd)[4]);
                if ($huid != $uid && $huid != 0) {
                    printf("Locked Account: %s does not own %s.\n",
${user},${hd});
                    exit(1); # triggers command after OR (||)
                }' ${name} ${home} ${uid} || \
                /usr/bin/chuser -R files account_locked=true $name
        fi
    fi
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.3 Ensure Home directory write access is restricted to owner

Profile Applicability:

- Level 1

Description:

Home directories must be writeable only by the **owner**. This recommendation audits (or removes) any write permission given via traditional file mode permissions (using **chmod**). Neither should a home directory have any permissions managed (whether permit or deny) via ACL's.

Rationale:

HOME directories with *group* or *world* write access enable malicious users to add files or directories, or even remove them if the directory 'T' (SVTX) bit is not also set. While this does not necessarily allow access to data - existing data might be destroyed (`unlink()`) or replaced (new file added with same name). These modifications could be used, e.g., to use the users authorizations to gain other system privileges.

Disabling read and execute access for *world* and/or *group* might be part of a company security policy - and the audit and remediation scripts will need to be modified to reflect this addition.

The use of ACL's is discouraged because their effect is not immediately visible using standard tools. They must be identified (locating inodes with permission bit 0200000000 set) as active and read using **aclget** before the actual permissions granted or denied are known. Better is to deny outside access to home (ie, user) related data. When data must be shared create an area outside of **\${HOME}**.

Impact:

There should be no impact - at least as far as *world* permissions are concerned. There is a potential that all members in the group **staff** or **system** might see minimal impact - if their systems have, or had, a default **umask** of **002** when their accounts were created.

Accounts created with a default **umask** of **022** or stricter will not be impacted, unless a user account modified their HOME directory mode bits to permit *group* and/or *other* write access.

Audit:

Validate the permissions of all of the directories changed:

```
#!/usr/bin/ksh -e
lsuser -R files -a id home ALL | while read name ids homes rest;
do
    uid_check=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid_check} -ge 200 ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; recommend to lock account
named [%s]\n" ${home} ${name}
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            /usr/bin/perl -e '$f=$ARGV[0]; $m=(stat $f)[2]; \
printf("Recommend chmod on: %s: to remove group or world write
mode\n", $f) if $m & 022; \
printf("Recommend remove ACL on: %s\n ", $f) if $m & 0200000000; \
exit($m & 0200000022)' ${home} \
|| (ls -led ${home} && (aclget ${home} | grep -ip Enabled))
        fi
    fi
done
```

- There should not be any output
- NOTE: The **audit** is performed only on accounts with a user ID (**uid**) greater or equal to **200**. Also, if the **HOME** directory has already been defined to something *special* (here, **/dev/null**) no **audit** is performed.

Remediation:

For all local accounts with UID >= 200:

- Remove write permission from home directories that have group or world write access:


```

#!/usr/bin/ksh -e
# home_mode_acl: 4.8.1.3
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022
typeset -i UIDCK=$1
typeset -i ret=0
if test $UIDCK == 0; then
    UIDCK=200
fi
lsuser -R files -a id home account_locked ALL | while read name ids homes
locks rest;
do
    uid_check=$(echo ${ids} | cut -f2 -d =)
    if [[ ${uid_check} -ge ${UIDCK} ]]; then
        home=$(echo ${homes} | cut -f2 -d =)
        locked=$(echo ${locks} | cut -f2 -d =)
        if [[ ${home} == "/dev/null" || ${locked} == "true" ]]; then
            continue
        elif [[ ! -d ${home} ]]; then
            /usr/bin/printf "%-32s does not exist; locking account named [%s]\n"
${home} ${name}
            chuser -R files account_locked=true $name
        else [[ ${home} != "/" && ${home} != "/dev/null" ]]
            perl -e '$f=$ARGV[0]; $m=(stat $f)[2];\
                exit (($m & 022) + 1) if ($m & 0200000000);\
                exit($m & 022);' $home
            # exit($m&022 +1) if ($m & 0200000000) else exit ($m &022); ' $home
            ret=$?
            [[ $ret == 0 ]] && continue
            if (( $ret & 022 )); then
                printf "%s: had group or world write mode\n" $home
                chmod og-w ${home}
            fi
            if (($ret & 1)); then
                printf "%s: had ACL defined and enabled\n" $home
                rm -rf /tmp/$$/${home}
                mkdir -p /tmp/$$/${home}
                aclget /tmp/$$/${home} | aclput ${home}
                rm -rf /tmp/$$/${home}
            fi
        fi
    fi
done

```

- NOTE: The permission change is automatically applied to all accounts with a user ID (**uid**) greater or equal to **200**. Also, if the **HOME** directory has already been defined to something *special* (here, **/dev/null**) no change is made to the account attributes.
- To automate the process for new users see **Additional Information** below.

Default Value:

drwxr-xr-x (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	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.			

4.1.2.4 Ensure access on /audit and /etc/security/audit is configured

Profile Applicability:

- Level 1

Description:

This recommendation verifies the access control settings for the default locations of AUDIT configuration and output files.

Rationale:

The default location for the **AUDIT** subsystem configuration files are in **/etc/security/audit**. The default location for output produced by the audit subsystem is the firectory **/audit**.

Access control must prevent unauthorized access.

NOTE: If your configuration does not store output in /audit ensure this directory is configured to prevent unauthorized access.

Audit:

Validate the permissions, UID and GID of **/etc/security/audit** and **/audit**:

```
# find /etc/security/audit /audit \( -perm -4 -o -perm -2 -o -perm -1 \) -o !  
-user root -o ! -group audit
```

There should not be any output.

Remediation:

Ensure correct ownership and permissions are in place for **/etc/security/audit** and **/audit**.

```
#!/usr/bin/ksh -e  
# Provided to CIS by AIXTools  
# Copyright AIXTools, 2022  
AUDITDIRS="/etc/security/audit /audit"  
find ${AUDITDIRS} | grep -v 'lost+found' | xargs chown root:audit  
find ${AUDITDIRS} -type d | grep -v 'lost+found' | xargs chmod g-w,o-rwx  
find ${AUDITDIRS} ! -type d | grep -v 'lost+found' | xargs chmod -R u-x,g-  
wx,o-rwx  
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.			

4.1.2.5 Ensure access to /etc/security is configured

Profile Applicability:

- Level 1

Description:

The `/etc/security` directory contains multiple files and directories used to keep the targeted AIX system secure. Most subsystems are owned by root:security (UID:GID). However, additional systems such as **AUDIT** and **AIXPERT** have their own permissions (and recommendations).

Traditionally, `/etc/security` has been identified as **USER** administration - including the shadow password file. But there is much more under `/etc/security`. Normal installations also have configuration files for security subsystems including: `aixpert`, `tsd`, `ice`, `ldap`, `rbac`, `audit`, `ipsec`, `fpm`, and `trusted computing (tscd)`.

While these subsystems may not be enabled - their configuration files need to be secured to ensure no unauthorized access.

Rationale:

The `/etc/security` directory contains sensitive files for multiple security systems. For the **USER** subsystem there are files such as `/etc/security/passwd`, `/etc/security/user` that must be secured from unauthorized access and modification.

Audit:

Validate the permissions of `/etc/security`:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022, 2025

EXCLUDE="security/(aixpert|audit|ice)"
find /etc/security -type d | \
  /usr/bin/egrep -v ${EXCLUDE} | \
  /usr/bin/sort | xargs ls -led | \
  /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}' | \
  /usr/bin/egrep -v "dr[w-]x[r-]-[sS-]----"
```

The command should not yield any output:

Remediation:

Ensure correct access control settings for security subsystem configuration files installed in **/etc/security**:

```
#!/usr/bin/ksh -e
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022, 2025

EXCLUDE="security/(aixpert|audit|ice)"

find /etc/security -type d | \
  /usr/bin/egrep -v ${EXCLUDE} | \
  /usr/bin/sort | xargs ls -led | \
  /usr/bin/awk '{print $1 " " " $3 " " " $4 " " " $9}' | \
  /usr/bin/grep -v drwxr-s--- | \
  awk '{print $NF}' | while read SECDIR; do
    /usr/bin/find ${SECDIR} | /usr/bin/grep -v ${EXCLUDE} | /usr/bin/xargs
chown root:security
  /usr/bin/find ${SECDIR} -type d | /usr/bin/grep -v ${EXCLUDE} |
  /usr/bin/xargs chmod g-w+s,o-rwx
  /usr/bin/find ${SECDIR} -type f | /usr/bin/grep -v ${EXCLUDE} |
  /usr/bin/xargs chmod u-x,g-wx,o-rwx
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.			

4.1.2.6 Ensure access on /var/adm/ras is configured

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`:

```
# /usr/bin/ls -l /var/adm/ras | /usr/bin/awk '{print $1 " " $3 " " $4 " " $9}'
```

NOTE: The output from the command above will contain numerous files.

- No files should have write permission for other
- No files except for `SRCKeyID` should have read permission for other

Remediation:

Remove world read and write access from all files in `/var/adm/ras`:

```
# /usr/bin/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.			

4.1.2.7 Ensure access on /var/adm/sa is configured

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=r-x /var/adm/sa
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.1.2.8 Ensure access on /var/spool/cron/crontabs is configured

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`:

```
find /var/spool/cron/crontabs -type d -prune \( -perm -4 -o -perm -2 -o -perm -1 -o -perm -2000000000 \) -o ! -user bin -o ! -group cron
find /var/spool/cron/crontabs \( -perm -4 -o -perm -2 -o -perm -1 -o -perm -2000000000 \) -o ! -group cron
trustchk -n /var/spool/cron/crontabs >/dev/null 2>&1 || echo trustchk failed
```

There should be no output.

Remediation:

Use the following script to apply settings to `/var/spool/cron/crontabs`:

```
#!/usr/bin/ksh -e
#; remove any extended ACL information
echo | aclput /var/spool/cron/crontabs

#; remove other access from all
chmod -R o= /var/spool/cron/crontabs
#; set UID:GID to bin:cron to `/var/spool/cron/crontabs` and correct modes on
directory and files within directory
chown bin:cron /var/spool/cron/crontabs
chgrp -R cron /var/spool/cron/crontabs
#; set modes on directory and files within directory
chmod ug=rwx,o= /var/spool/cron/crontabs
chmod a-w /var/spool/cron/crontabs

#; add or update entry in TCB
trustchk -a /var/spool/cron/crontabs size=VOLATILE >/dev/null 2>&1 ||
trustchk -u /var/spool/cron/crontabs owner=bin group=cron mode=770
```

Default Value:

N/A

Additional Information:

Some platforms, e.g., Linux, prefer the **owner** to be **root**. As the owner **bin** is also a protected account there is no need to force the directory **owner** attribute to the name **root**.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.1.2.9 Ensure access on /var/spool/cron/atjobs is configured

Profile Applicability:

- Level 1

Description:

The `/var/spool/cron/atjobs` directory contains scripts submitted by authorized users using the command `at`.

Rationale:

The `/var/spool/cron/atjobs` directory contains all of the `at` jobs for the users on the system. Atjob files present a security problem because they are run using SUID and SGID of the user who submits the job.

Allowing other users to have read/write permissions on these files may allow them to escalate their privileges to that user and/or group.

To negate this risk, the directory and all the files that it contains must be secured.

Audit:

Validate the permissions of `/var/spool/cron/atjobs`:

```
find /var/spool/cron/atjobs -type d -prune \( -perm -4 -o -perm -2 -o -perm -1 -o -perm -2000000000 \)
find /var/spool/cron/atjobs ! -type d -perm -2
trustchk -n /var/spool/cron/atjobs >/dev/null 2>&1 || echo trustchk failed
```

There should be no output.

Remediation:

Use the following script to apply settings to `/var/spool/cron/atjobs`:

```
#!/usr/bin/ksh
#; remove any extended ACL information
echo | aclput /var/spool/cron/atjobs

#; remove other access from all
chmod -R o= /var/spool/cron/atjobs
#; set UID:GID to bin:cron to `/var/spool/cron/atjobs` and correct modes on
directory
chown bin:cron /var/spool/cron/atjobs

#; remove world access on directory and files within directory
chmod -R o= /var/spool/cron/atjobs

#; add or update entry in TCB
trustchk -a /var/spool/cron/atjobs size=VOLATILE >/dev/null 2>&1 || trustchk
-u /var/spool/cron/atjobs owner=bin group=cron mode=770
```

Default Value:

N/A

Additional Information:

Some platforms, e.g., Linux, prefer the **owner** to be **root**. As the owner **bin** is also a protected account there is no need to force the directory **owner** attribute to the name **root**.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.10 Ensure all directories in root PATH access are configured

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} | awk -F: '
{
    n = split($0, d, ":")
    for (i=0; ++i <= n;)
        if (length(d[i]) == 0) {
            print i
        }
        else
            print i, d[i]
    }' | while read cnt dirname ; do
    # if ${dirname} is zero length (current directory) - complain
    [[ -z ${dirname} ]] && print "Current Directory not allowed in \${PATH}" &&
continue
    # if first character in $dirname is not '/' complain
    first=$(echo ${dirname} | cut -c1)
    [[ ${first} != "/" ]] && print "PATH directories must begin with '/',
${dirname} not allowed"
    # if $dirname does not exist, complain
    [[ -d ${dirname} ]] || print "Non-existent directory ${dirname} in \${PATH}"
&& continue
    # if ${dirname} is group or other writeable complain
    [[ "$(ls -ld ${dirname})" = @(d??????w? *) ]] && print " WARNING ${dirname}
is world writable"
    [[ "$(ls -ld ${dirname})" = @(d????w???? *) ]] && print " WARNING ${dirname}
is group writable"
    # PATH directories must be owned by either root, or the AIX special user
`bin`
    [[ "$(ls -ld ${dirname} |awk '{print $3}')" != @(root|bin) ]] && print "
WARNING ${dirname} is not owned by root or bin"
done
```

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
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.			

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.			

4.2 Configure Network Services

This section provides guidance on the so-called historical services. These are services that are still installed - often by default - but the base recommendation is to uninstall the services whenever possible, and disable them when they cannot be removed.

The basic recommendations: remove or disable falls under IG1. Some of these services may be used, after proper configuration. Such a service should be viewed as part of an IG2 or IG3 solution.

In another section recommendations have already been made to disable the remote services in `/etc/inetd.conf`. While this stops the server from accepting connections disabling the binaries themselves ensures connections from the server to another host are further restricted, i.e., the daemons themselves are fully disabled.

There are many (well) known security vulnerabilities related to these services and they are a primary target for any DoS attack.

In short, unless otherwise required, the IG1 recommendation is that the services and daemons covered in this section and its subsections are either removed from the system or have their file mode permissions removed.

4.2.1 Ensure NIS client is not installed

Profile Applicability:

- Level 1

Description:

The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client was used to bind a machine to an NIS server and receive the distributed configuration files.

Rationale:

The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.

Impact:

If NIS is used for authentication, then removal of the files may prevent users from accessing the system. In this case, the package should remain installed but it is strongly recommended that you review options for moving to a more secure technology such as LDAP

Audit:

Ensure that the software has been successfully de-installed:

```
lsb_release -a |grep "bos.net.nis.client"
```

The above command should yield no output.

Remediation:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS client software:

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

Default Value:

N/A

CIS Controls:

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

4.2.2 Ensure NIS server services are not in use

Profile Applicability:

- Level 1

Description:

A Network Information Service (NIS) server is a host that provides configuration information to other hosts on a network. NIS servers store tables of information about users, groups, and more. They also maintain a set of maps and run the ypserv daemon, which processes requests from clients for information in those maps.

Rationale:

As NIS is extremely insecure, the NIS server packages must be removed from the system unless absolutely needed.

- **IF** - NIS must be used in the environment, and is approved by local site policy, limit access to the NIS data to specific subnets.

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:

Ensure that the software has been successfully de-installed:

```
lsrpm -L |grep "bos.net.nis.server"
```

The above should command should yield no output.

- **OR** -

- **IF** - the **NIS** server package is required as a dependency, or NIS must be used in the environment, and is approved by local site policy:

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:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS server software:

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

- OR -

- IF - the **NIS** server package is required as a dependency, or NIS must be used in the environment, and is approved by local site policy:

Ensure that all of the NIS daemons are inactive:

```
stopsrc -g yp
```

De-install the NIS server software:

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

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

4.2.3 Ensure legacy NIS markers are removed

Profile Applicability:

- Level 1

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
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.			

4.2.4 Ensure all entries in /etc/hosts.equiv are removed

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

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.			

4.2.5 Ensure that host based authentication files are not present

Profile Applicability:

- Level 2

Description:

This recommendation removes all instances of **.rhosts**, **.shosts** and **.netrc** files from the system.

Rationale:

The **.rhosts**, **.shosts** 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 / \( -fstype jfs -o -fstype jfs2 \) -name ".netrc" -print
find / \( -fstype jfs -o -fstype jfs2 \) -name ".rhosts" -print
find / \( -fstype jfs -o -fstype jfs2 \) -name ".shosts" -print
```

The above commands should not yield output

NOTE: On systems with large filesystems these commands may take some time to execute, local knowledge of the system may be used to narrow the locations which are searched

Remediation:

Remove the **.rhosts** and **.netrc** files from all user home directories:

```
find / \( -fstype jfs -o -fstype jfs2 \) -name ".netrc" -exec rm {} \;
find / \( -fstype jfs -o -fstype jfs2 \) -name ".rhosts" -exec rm {} \;
find / \( -fstype jfs -o -fstype jfs2 \) -name ".shosts" -exec rm {} \;
```

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.			

4.2.6 Ensure legacy remote daemon support is not available

Profile Applicability:

- Level 1

Description:

Ensure that software that supports passwordless and/or clear-text password connections is disabled. Examples include daemons such as: **rlogind**, **rshd** and **talkd**.

Rationale:

Remote services that either send or receive usernames and passwords in clear text and should not be used.

Impact:

Ideally, these packages were not installed. If they are installed during system installation and configuration they are practically impossible to *uninstall*. The alternative is to set the file mode bits to zero to block execution and/or copying.

Audit:

Execute the following script:

```
for fileset in bos.net.tcp.rcmd_server bos.net.tcp.rcmd
do
  lsclpp -L ${fileset} >/dev/null 2>&1
  if [[ $? -eq 0 ]] then
    lsclpp -f ${fileset} | /usr/bin/egrep "^ +\/" | while read filename rest
    do
      test -L ${filename} && continue
      test -d ${filename} && /usr/bin/ls -led ${filename} | /usr/bin/egrep -
v "^d-----"
      test -f ${filename} && /usr/bin/ls -led ${filename} | /usr/bin/egrep -
v "^------"
    done
  fi
done
```

There should not be any output.

Remediation:

Use the following script to disable the files in these packages:

Note: In this script, disable means **chmod 0 ...**; Remove any ACL; and update any entries in the TCB rather than remove entries.

```
for fileset in bos.net.tcp.rcmd_server bos.net.tcp.rcmd
do
  lslpp -L ${fileset} >/dev/null 2>&1
  if [[ $? -eq 0 ]] then
    lslpp -f ${fileset} | /usr/bin/egrep "^ +\/" | while read command rest
    do
      # aclput will also do a classic chmod on the standard file mode bits
      /usr/bin/aclput </dev/null ${command}
      /usr/sbin/chtcb off ${command}
      # if in the TSD as a privileged command - make sure accessauths
      attribute is cleared
      lssecattr -c ${command} && setsecattr -c accessauths= ${command}
      # ignore errors, if any, when the file is not already in the TSD
      # Note: trustchk does not (always) update the attribute 'accessauths'.
      Ignore this if it occurs
      trustchk -u ${command} mode accessauths
    done
    # update the kernel security tables
    setkst
  fi
done
```

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.		●	●

4.2.7 Ensure snmpd is not installed

Profile Applicability:

- Level 1

Description:

Simple Network Management Protocol (SNMP) is a widely used protocol for monitoring the health and welfare of network equipment, computer equipment and devices like UPSs.

`bos.net.tcp.snmpd` is a suite of applications used to implement SNMPv1 (RFC 1157), SNMPv2 (RFCs 1901-1908), and SNMPv3 (RFCs 3411-3418) using both IPv4 and IPv6.

SNMP server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The `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.

The SNMP server can communicate using `SNMPv1`, which transmits data in the clear and does not require authentication to execute commands. `SNMPv3` replaces the simple/clear text password sharing used in `SNMPv2` with more securely encoded parameters. If the the SNMP service is not required, the `bos.net.tcp.snmpd` fileset should be removed to reduce the attack surface of the system.

Note: If SNMP is required:

- The server should be configured for `SNMP v3` only. `User Authentication` and `Message Encryption` should be configured.
- If `SNMP v2` is **absolutely** necessary, modify the community strings' values.

Impact:

Removing `snmpd` will also remove a number of related services from the system, specifically `aixmibd`, `dpid2` and `snmpmib2`

Audit:

- From the command prompt, execute the following commands:

```
lsnmp -Lcq bos.net.tcp.snmp >/dev/null 2>&1 && echo " - SNMP client filesset exists on the system"

lsnmp -Lcq bos.net.tcp.snmpd >/dev/null 2>&1 && echo " - SNMP server filesset exists on the system"
```

Nothing should be returned

Remediation:

Execute the following command:

```
installp -ug bos.net.tcp.snmp bos.net.tcp.snmpd
```

Default Value:

Uncommented

CIS Controls:

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

4.3 Subsystems managing the system boot phases

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

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

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

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

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

4.3.1 Configure processes managed by /etc/inittab

The process `init` is the legacy parent application on *NIX* systems - and is expected to have *process ID 1*. The file `/etc/inittab` was the configuration file used to *autostart* and *restart* system services.

On AIX the parsing of the file `/etc/inittab` is the third phase of the boot process managed by the script `/sbin/rc.boot`. Note: the file `/sbin/rc.boot` is copied to the boot partition (*hd5*) during the creation of the boot block. In other words, local changes to the file are only seen *AFTER* the boot block is recreated using the command `bosboot`.

- Additional services are listed in other sections - and these correspond with base services initially started via a line in `/etc/inittab`.

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

4.3.1.1 Ensure writesrv service is not in use

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:

```
/usr/sbin/lsttab writesrv | /usr/bin/grep -v "off"  
/usr/bin/lssrc -s writesrv | /usr/bin/tail -n1 | /usr/bin/grep -v inoperative
```

The above commands should yield no output.

Remediation:

Use the **chitab** command to disable the **writesrv** start-up script in **/etc/inittab**:

Note: Do not use the **rmitab** to remove the writesrv start-up script from **/etc/inittab** as it may return during a update.

```
/usr/sbin/chitab "writesrv:23456789:off:/usr/bin/startsrc -swritesrv"
```

Use **stopsrv** to ensure that **writesrv** is not running

```
/usr/bin/stopsrv -s writesrv
```

Default Value:

N/A

CIS Controls:

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

4.3.1.2 Ensure dt service is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following commands:

```
lsitab dt
lsitab dt_nogb
```

The above commands should not yield output.

Remediation:

In **/etc/inittab**, remove the **dt** and **dt_nogb** entries:

```
rmitab dt
rmitab dt_nogb
```

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.		●	●

4.3.1.3 Ensure piobe service is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

piobe is a legacy daemon that has known vulnerabilities. This daemon should be disabled to reduce the attack surface of the system.

Impact:

Disabling **piobe** will remove the system's ability to support remote printing.

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.		●	●

4.3.1.4 Ensure qdaemon service is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

`qdaemon` is a legacy daemon that has known vulnerabilities. This daemon should be disabled to reduce the attack surface of the system.

Impact:

Disabling `qdaemon` will remove the system's ability to support local and remote printing.

Audit:

From the command prompt, execute the following command:

```
lsitab qdaemon
```

The above command should yield not yield output

Remediation:

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

```
rmitab qdaemon
```

Default Value:

Enabled

CIS Controls:

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

4.3.1.5 Ensure rcnfs service is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

```
lsitab rcnfs | grep -v "off"
```

The above command should not yield output

Remediation:

Use the **chitab** command to disable the NFS start-up script in **/etc/inittab**:

Note: Do not use the **rmitab** to remove the NFS start-up script from **/etc/inittab** as it may return during a update.

```
chitab "rcnfs:23456789:off:/etc/rc.nfs > /dev/console 2>&1 # Start NFS Daemons"
```

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

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

Default Value:

Uncommented

Additional Information:

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

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

CIS Controls:

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

4.3.1.6 Ensure snapp is not installed

Profile Applicability:

- Level 1

Description:

snapp provides a perl-based interface to do the initial network configuration of an IBM RISC System/6000, from a Palm Pilot, via RS232C.

Rationale:

Systems running as logical partitions will not have access to an RS232C port, network configuration is performed either via NIM or through the virtual terminal provided by the Hardware Management Console. The **snapp** service is therefore not required and should be removed to reduce the attack surface of the system.

Audit:

Run the following command:

```
lsnpp -L |grep -i bos.net.snapp
```

No output should be returned.

Remediation:

Remove the software

```
installp -u bos.net.snapp
```

CIS Controls:

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

4.3.1.7 Ensure NIM master is not installed

Profile Applicability:

- Level 1

Description:

The NIM master provides services to support network based installation, patching and automation against managed AIX client systems.

Rationale:

The filesset **bos.sysmgt.nim.master** is not installed by default IBM installation processes.

Only system(s) specifically designated and additionally hardened to safely perform the service *NIM master* should have this filesset installed.

Impact:

If system is intended to act as a NIM Master, removal of this package will prevent the system from acting as a NIM Master and performing package updates and installs.

Note: A NIM master should be properly documented with the exceptions needed to enable this service.

Audit:

Run the following command:

```
(lsllpp -Lc bos.sysmgt.nim.master bos.sysmgt.nim.spot | grep sysmgt.nim) &&  
echo "NIM master and/or spot installed"
```

No output should be returned.

Remediation:

Remove the software

```
installp -u bos.sysmgt.nim.master bos.sysmgt.nim.spot
```

Default Value:

The filesets **bos.sysmgt.nim.master** and **bos.sysmgt.nim.spot** are not installed by default.

CIS Controls:

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

4.3.2 Configure daemons managed by /etc/rc.tcpip

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](#).

DRAFT

4.3.2.1 Ensure inetd daemon is disabled when no additional services are required

Profile Applicability:

- Level 1

Description:

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

This is the preferred state.

Rationale:

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

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

Impact:

When an **inetd service** is required this service is permitted.

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.		●	●

4.3.2.2 Ensure dhcp client services are not in use

Profile Applicability:

- Level 1

Description:

The **dhcpcd** and **dhcpcd6** daemons receive address and configuration information from the DHCP server for IPv4 and IPv6 respectively.

Rationale:

Unless a system is specifically expected to receive IP address and configuration via DHCP, it is recommended that the dhcp client fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep dhcpcd
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

dhcpcd	tcpip	inoperative
dhcpcd6	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.dhcp bos.net.tcp.client
```

- OR -

- IF - the **bos.net.tcp.dhcp** fileset is required as a dependency:

Run the following script to stop and disable **dhcpcd** and **dhcpcd6**

```
#!/usr/bin/ksh
DAEMONS="dhcpcd dhcpcd6"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Commented out

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003049 | STIG RULE ID: SV-215355r958478 | CAT II
5. STIG Finding ID: V-215355

CIS Controls:

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

4.3.2.3 Ensure dhcp relay services are not in use

Profile Applicability:

- Level 1

Description:

The **dhcprd** daemon listens for broadcast packets, receives them, and forwards them to the appropriate DHCP or BOOTP server.

Rationale:

Unless a system is specifically set up to act as a DHCP relay server, it is recommended that the dhcprd fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep dhcprd
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

dhcprd	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.dhcpd bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.dhcpd** fileset is required as a dependency:

Run the following script to stop and disable **dhcprd**

```
#!/usr/bin/ksh
DAEMONS="dhcprd"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Commented out

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003050 | STIG RULE ID: SV-215356r958478 | CAT II
5. STIG Finding ID: V-215356

CIS Controls:

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

4.3.2.4 Ensure dhcp server services are not in use

Profile Applicability:

- Level 1

Description:

The **dhcpcsd** daemon is the DHCP server that serves addresses and configuration information to DHCP clients in the network.

Rationale:

Unless a system is specifically set up to act as a DHCP server, it is recommended that the dhcpcd fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep dhcpcsd
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

dhcpcsd	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.dhcpd bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.dhcpd** fileset is required as a dependency:

Run the following script to stop and disable **dhcpcd**

```
#!/usr/bin/ksh
DAEMONS="dhcpcd"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Commented out

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003104 | STIG RULE ID: SV-215405r958478 | CAT II
5. STIG Finding ID: V-215405

CIS Controls:

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

4.3.2.5 Ensure *gated* is not in use

Profile Applicability:

- Level 1

Description:

The **gated** daemon provides gateway routing functions for protocols such as RIP, OSPF and BGP.

Rationale:

Unless a system is specifically set up to act as a network router, it is recommended that the **gated** fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep gated
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

gated	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.gated bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.gated** fileset is required as a dependency:

Run the following script to stop and disable **gated**

```
#!/usr/bin/ksh
DAEMONS="gated"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Commented out

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003052 | STIG RULE ID: SV-215358r958478 | CAT II
5. STIG Finding ID: V-215358

CIS Controls:

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

4.3.2.6 Ensure hostmibd is not in use

Profile Applicability:

- Level 1

Description:

The **hostmibd** daemon is a dpi2 sub-agent which manages a number of MIB variables which may be required if the server runs SNMP.

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/7.2?topic=h-hostmibd-daemon>

Rationale:

Unless a system is specifically set up to provide SNMP services, it is recommended that the snmpd fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep hostmibd
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

hostmibd	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.snmpd bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.snmpd** fileset is required as a dependency:

Run the following script to stop and disable **hostmibd**

```
#!/usr/bin/ksh
DAEMONS="hostmibd"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Enabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)

CIS Controls:

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

4.3.2.7 Ensure multicast routing is not in use

Profile Applicability:

- Level 2

Description:

The **mrouted** daemon is an implementation of the multicast routing protocol.

Rationale:

Unless a system is specifically set up to act as a network router, it is recommended that the **mrouted** daemon is disabled to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -s mrouted
```

This should yield the following output:

mrouted	tcpip	inoperative

Remediation:

Run the following script to stop and disable **mrouted**

```
#!/usr/bin/ksh
DAEMONS="mrouted"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrctcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

NOTE: **mrouted** is provided by **bos.net.tcp.server_core** so it is not possible to remove this filesset.

Default Value:

Disabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003053 | STIG RULE ID: SV-215359r958478 | CAT II
5. STIG Finding ID: V-215359

CIS Controls:

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

4.3.2.8 Ensure dns server services are not in use

Profile Applicability:

- Level 1

Description:

The **named** daemon is the server for the DNS protocol and controls domain name resolution for its clients.

Rationale:

Unless a system is specifically designated to act as a DNS server, it is recommended that the named fileset be removed to reduce the potential attack surface.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep named
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

named	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.bind bos.net.tcp.server bind.rte
```

- OR -

- IF - the **bos.net.tcp.bind** or **bind.rte** filesets are required as a dependency:

Run the following script to stop and disable **named**

```
#!/usr/bin/ksh
DAEMONS="named"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

disabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003054 | STIG RULE ID: SV-215360r958478 | CAT II
5. STIG Finding ID: V-215360

CIS Controls:

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

4.3.2.9 Ensure portmap is not in use

Profile Applicability:

- Level 1

Description:

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

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

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

Rationale:

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

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

Audit:

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

```

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

```

Remediation:

- Review any active RPC services:

```
rpcinfo -p localhost
```

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

Default Value:

Enabled

Additional Information:

Reversion:

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

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

CIS Controls:

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

4.3.2.10 Ensure routed is not in use

Profile Applicability:

- Level 1

Description:

The **routed** daemon manages the network routing tables in the kernel.

Rationale:

The **routed** daemon should not be used as it only supports RIP1, it is recommended that the **routed** daemon is disabled to reduce the potential attack surface.

Should the AIX server need to communicate directly with routers (i.e., there is no default route but routes are managed by software) - the **gated** daemon should be used instead.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -s routed
```

This should yield the following output:

routed	tcpip	inoperative

Remediation:

Run the following script to stop and disable **routed**

```
#!/usr/bin/ksh
DAEMONS="routed"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrctcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

NOTE: **routed** is provided by **bos.net.tcp.server_core** so it is not possible to remove this fileset.

Default Value:

Disabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003055 | STIG RULE ID: SV-215358r958478 | CAT II
5. STIG Finding ID: V-215361

CIS Controls:

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

4.3.2.11 Ensure rwhod is not in use

Profile Applicability:

- Level 1

Description:

The **rwhod** daemon is the remote WHO service, which collects and broadcasts status information to peer servers on the same network.

Rationale:

Unless a system is specifically set up to provide WHO services, it is recommended that the **rcmd_server** fileset be removed to reduce the potential attack surface.

Impact:

As well as providing the **rwhod** command (and other insecure daemons), the **bos.net.tcp.rcmd_server** fileset also provides two commands related to configuring authentication setting - standard or **Kerberos**. If your authentication policy specifies **Kerberos** as the preferred authentication mechanism - you should not remove this fileset, but disable the daemons instead.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep rwhod
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

rwhod	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.rcmd_server bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.rcmd_server** fileset is required as a dependency:

Run the following script to stop and disable **rwhod**

```
#!/usr/bin/ksh
DAEMONS="rwhod"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrctcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Disabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003056 | STIG RULE ID: SV-215362r958478 | CAT II
5. STIG Finding ID: V-215362

CIS Controls:

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

4.3.2.12 Ensure sendmail is not in use

Profile Applicability:

- Level 1

Description:

The **sendmail** daemon 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. Unless a system is specifically designated to act as a mail server, it is recommended that the sendmail files be removed to reduce the potential attack surface.

Note: Historically, the AIX sendmail build has not supported the AUTH feature. Since AIX 7.2 TL4 a new packaging of sendmail (still as version 8.15.2, so version number is not the way to verify suitability) allows AUTH support indirectly via the SASLv2 (Simple Authentication and Security Layer) API interface. Our recommendation is to disable/remove sendmail programs that do not provide SASLv2 support.

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep sendmail
```

This should yield either no output (if the files are not present)

- OR -

the following output (if the files are present):

```
sendmail      tcpip      inoperative
```

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.sendmail bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.sendmail** fileset is required as a dependency:

Run the following script to stop and disable **sendmail**

```
#!/usr/bin/ksh
DAEMONS="sendmail"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Enabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003047 | STIG RULE ID: SV-215360r958478 | CAT II
5. STIG Finding ID: V-215353

CIS Controls:

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

4.3.2.13 Ensure timed is not in use

Profile Applicability:

- Level 1

Description:

The **timed** daemon implements the legacy UNIX time service.

Rationale:

The UNIX time service is obsolete and has been replaced by NTP, it is recommended that the timed fileset be removed to reduce the potential attack surface.

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

Audit:

- From the command prompt, execute the following command:

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

This should yield the following output:

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

- From the command prompt, execute the following command:

```
# /usr/bin/lssrc -a | /usr/bin/grep timed
```

This should yield either no output (if the fileset is not present)

- OR -

the following output (if the fileset is present):

timed	tcpip	inoperative

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u bos.net.tcp.timed bos.net.tcp.server
```

- OR -

- IF - the **bos.net.tcp.timed** fileset is required as a dependency:

Run the following script to stop and disable **timed**

```
#!/usr/bin/ksh
DAEMONS="timed"
for l_daemon in $DAEMONS;
do
    /usr/sbin/chrtcp -d $l_daemon
    /usr/bin/stopsrc -s $l_daemon
done
```

Default Value:

Disabled

References:

1. CCI-000381
2. NIST SP 800-53 :: CM-7
3. NIST SP 800-53A :: CM-7.1 (ii)
4. STIG ID: AIX7-00-003057 | STIG RULE ID: SV-215363r958478 | CAT II
5. STIG Finding ID: V-215363

CIS Controls:

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

4.3.3 Configure IPv6

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

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

Note: 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.

DRAFT

4.3.3.1 Ensure *autoconf6* is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

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

Remediation:

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

```
chrctcp -d autoconf6
```

Default Value:

Commented out

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.3.3.2 Ensure *ndpd-host* is not in use

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

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

Impact:

When **IPv6** is active and **NDP** is used to get a non-link-local IPv6 address (link-local addresses begin with **fe80::**) it is also likely that the MTU size of the interface will change from **1500** to **1492**. Additionally, it may add default route to the IPv6 router it received its 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	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.3.3.3 Ensure *ndpd-router* is not in use

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

Impact:

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

See: [manpage AIX 7.2 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>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.3.4 Configure services managed by the inetd process

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

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

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

DRAFT

4.3.4.1 Ensure bootps daemon is not in use

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 'bootps' -p udp  
lssrc -s inetd && refresh -s inetd
```

Default Value:

Disabled

CIS Controls:

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

4.3.4.2 Ensure chargen daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.3 Ensure comsat daemon is not in use

Profile Applicability:

- Level 1

Description:

This entry starts the **comsat** service.

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

The recommendation is to leave this service disabled.

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.4 Ensure daytime daemon is not in use

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.		●	●

4.3.4.5 Ensure discard daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Commented out

CIS Controls:

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

4.3.4.6 Ensure echo daemon is not in use

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.		●	●

4.3.4.7 Ensure exec daemon is not in use

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.8 Ensure finger daemon is not in use

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

4.3.4.9 Ensure `ftpd` daemon is not in use

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.		●	●

4.3.4.10 Ensure imap2 daemon is not in use

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

4.3.4.11 Ensure instsrv daemon is not in use

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. This is no longer applicable for modern AIX installations.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Commented out

CIS Controls:

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

4.3.4.12 Ensure klogin daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.13 Ensure kshell daemon is not in use

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.		●	●

4.3.4.14 Ensure netstat daemon is not in use

Profile Applicability:

- Level 1

Description:

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

The recommendation is to leave this disabled.

Rationale:

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

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

Audit:

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

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.15 Ensure *ntalk* daemon is not in use

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.		●	●

4.3.4.16 Ensure pcnfsd daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.17 Ensure pop3 daemon is not in use

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

4.3.4.18 Ensure rexd daemon is not in use

Profile Applicability:

- Level 1

Description:

This entry starts the **rexed** service when required.

This service should be disabled if it is not required.

Rationale:

The **rexed** 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 **rexed** 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 **rexed** 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:]]rexed" | 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 'rexed' -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.		●	●

4.3.4.19 Ensure rlogin daemon is not in use

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:

```
# /usr/bin/lssrc -s inetd -l | /usr/bin/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:

```
# /usr/sbin/chsubserver -r inetd -C /etc/inetd.conf -d -v 'login' -p tcp6
# /usr/bin/lssrc -s inetd && refresh -s inetd
```

Default Value:

Uncommented

CIS Controls:

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

4.3.4.20 Ensure rquotad daemon is not in use

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

4.3.4.21 Ensure rstatd daemon is not in use

Profile Applicability:

- Level 1

Description:

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

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

Rationale:

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

An attacker may use this information in a DoS attack.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.22 *Ensure rsync daemon is not in use*

Profile Applicability:

- Level 1

Description:

The **rsync** daemon can be used to synchronize files between systems over network links.

Rationale:

The **rsync** daemon presents a security risk as the **rsync** protocol is unencrypted.

The **rsync.rte** fileset should be removed to reduce the attack area of the system.

Impact:

The **rsync.rte** fileset also provides the **rsync** client. If the client is required, stop and disable the **rsync** daemon and leave the fileset installed

Audit:

From the command prompt, execute the following command:

```
# /usr/bin/lssrc -s inetd -l | /usr/bin/grep rsync
```

No output should be returned

Remediation:

Run the following command to remove the software:

```
# /usr/sbin/installp -u rsync.rte
```

- OR -

- IF - the **rsync.rte** fileset is required as a dependency, or the **rsync** client is required:

In **/etc/inetd.conf**, comment out the **rsync** entry:

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

4.3.4.23 Ensure rusersd daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.24 Ensure rwalld daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.25 Ensure shell daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield:

```
0
```

Remediation:

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

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

Default Value:

Enabled

CIS Controls:

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

4.3.4.26 Ensure sprayd daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
0
```

Remediation:

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

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

Default Value:

Disabled

CIS Controls:

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

4.3.4.27 Ensure talk daemon is not in use

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.		●	●

4.3.4.28 Ensure telnetd daemon is not in use

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.		●	●

4.3.4.29 Ensure tftpd daemon is not in use

Profile Applicability:

- Level 1

Description:

This entry starts the **tftpd** service when required.

Rationale:

The **tftpd** service allows remote systems to download or upload files to the **tftpd** 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:]]tftpd" | 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 'tftpd' -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.		●	●

4.3.4.30 Ensure time daemon is not in use

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.		●	●

4.3.4.31 Ensure uucp daemon is not in use

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield:

```
0
```

Remediation:

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

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

Default Value:

Enabled

CIS Controls:

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

4.3.4.32 Ensure xmquery daemon is not in use

Profile Applicability:

- Level 1

Description:

This entry starts the **xmquery** daemon when required.

Rationale:

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

Audit:

From the command prompt, execute the following command:

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

The above command should yield:

```
0
```

Remediation:

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

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

Default Value:

Enabled

CIS Controls:

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

4.4 Filesystem Configuration

AIX places certain directories that are used for system wide functions on their own LVM partition at installation time. This provides protection for resource exhaustion and enables the use of mounting options that are applicable to the directory's intended use.

Separating other directories onto their own filesystems can increase this protection.

DRAFT

4.4.1 Configure Network Filesystem (NFS)

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

If a system does not need to act as either an NFS server, the primary recommendation is to uninstall these services to reduce the attack surface. However, if the server acts as either an NFS server there is an additional recommendations to implement.

- Since it is not possible to uninstall NFS client software the recommendations 4.4.1.3 through 4.4.1.6 are valid.
- When 4.4.1.2 is not implemented (NFS server is installed) for Level 2 audits recommendation 4.4.1.7 is required.

DRAFT

4.4.1.1 Ensure NFS client mounts are disabled in /etc/filesystems

Profile Applicability:

- Level 1

Description:

Disable automated mount of remote NFS shares.

Rationale:

NFS is frequently exploited to gain unauthorized access to files and directories. Automated and/or pre-defined mounts should not exist.

AIX does not allow the *kernel* service that enables NFS mounts to be disabled.

The protection against unauthorized mounts is that only accounts in the group *system* can mount pre-existing (i.e., defined in **/etc/filesystems**) NFS mounts. Non-existing NFS mounts require root (euid==0) access.

Impact:

The use of NFS mounts is discouraged. The only expected use of NFS is when used in combination with a **NIM** server for system maintenance.

Audit:

Ensure that no NFS mounts are part of the standard mounts:

```
/usr/bin/grep -p nfs /etc/filesystems
```

The above command should yield no output.

Remediation:

Ensure that there are no current NFS client mounts:

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

The above commands should yield no output.

Stop NFS services:

```
stopsrc -g nfs
```

Default Value:

No pre-defined mounts

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.		●	●

4.4.1.2 Ensure NFS server services are not in use

Profile Applicability:

- Level 1

Description:

De-install NFS server if the server does not act as an NFS server to remote clients. An *expected exception* is a system configured as a **NIM** server.

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:

```
lslpp -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 latest fileset applicable for the OS level installed.

Note: Recommendation 4.1.4.7 is required when the server package is installed.

CIS Controls:

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

4.4.1.3 Ensure NFS client mounts include nosuid and nodev options

Profile Applicability:

- Level 1

Description:

When using NFS shares ensure that suid/sgid program execution and/or access to system devices via permissions set on any mounted NFS filesystem are disabled.

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

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

Default Value:

N/A

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.			

4.4.1.4 Ensure localhost aliases do not exist in /etc/exports

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	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.			

4.4.1.5 Ensure NFS exports use allow lists

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

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

Audit:

Examine exported directories for unmanaged (aka world) access:

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

The desired output is:

```
0
```

Remediation:

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

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

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

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

to:

```
/export/repo x071
```

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

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

Default Value:

N/A

Additional Information:

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

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

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.			

4.4.1.6 Ensure access by root over nfs is disabled or blocked

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

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

Many NFS servers call this **root_squash**. On AIX this option 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	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.4.1.7 Ensure secure RPC authentication is enabled

Profile Applicability:

- Level 2

Description:

To enhance server-client authentication ensure that the secure option is selected for every export.

Rationale:

RPC is a protocol used by NFS to communicate requests between hosts. **Secure NFS** uses encryption (DES or Kerberos) to secure host authentication in RPC transactions. Secure NFS mitigates attempts by an attacker to spoof RPC requests by encrypting the time stamp in the RPC requests.

While the data is not encrypted each package is verified by a successful decryption the timestamp in every incoming RPC request. This confirmation mitigates receiving requests from untrusted or unknown hosts.

Audit:

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

```
lsnfsexp | grep sec= | grep none  
lsnfsexp | grep -v sec=
```

No output should be returned.

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

4.4.2 Configure Filesystem Encryption

Data stored in files may need to be encryption to add an additional level of security. (Open)SSL is a technology well known for encrypting data in transport (over a network connection). Filesystem encryption provides protection at-rest (when the file system is unmounted, server is powered off) and, optionally, at all times unless you have access to a key to unlock (decrypt) the filedata on-demand.

Starting with AIX 6.1 AIX included the option to define encrypted filesystems (EFS). This implementation does not require any additional hardware - but it does require key management and processing power to decrypt and encrypt data read from/written to the filesystem. An advantage may be that files are always encrypted from those with no intended access.

Starting with AIX 7.2 TL5 supported was added to position encrypting at the filesystem partition (i.e., logical volume) level. At a user level this is much easier to utilize - as no user keys are needed. The disadvantage is that - to all appearances on a live system - there is no encryption. In other words, encryption is only effective when the filesystem is unmounted and/or the storage media is powered off.

4.4.2.1 Ensure File System Level encryption is enabled

Profile Applicability:

- Level 2

Description:

When there is a requirement for file based encryption for unauthorized users for both live systems and encryption at rest the preferred mechanism is **EFS** - encrypted file systems.

Rationale:

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

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

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

Impact:

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

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

Audit:

Validate the installation of the CLiC software:

```
lsbpc -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 files. The files are 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/install/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/loadkclib
```

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/7.2?topic=system-efs-encrypted-file>

Additional Information:

Reversion:

De-install the CLiC fileset:

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

Decrypt all files:

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

CIS Controls:

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

4.4.3 Configure ROOTVG

The rootvg volume group is created during installation. Many of the defaults chosen were applicable 30+ years ago and best practices have changed over the years - while these defaults have not. Some of the features aka settings we are recommending have been available for 30+ years as well. Time to make the the standard.

Some of the recommendations here will be one recommendation for all the standard file systems - created during install - rather than one recommendation for each filesystem - wherever possible.

DRAFT

4.4.3.1 Ensure only / permits device files.

Profile Applicability:

- Level 1

Description:

The filesystem mount option **nodev** ensures that special device files are not recognized as device files. This recommendation audits all **rootvg** filesystems to ensure that only the **root** filesystem **'/'** allows the use of *device* special files.

Rationale:

Impact:

If the system is acting as a WPAR host then restricting where device files may exist may impact on the ability to start WPARs. You should ensure that any filesystems which are used to host the root filesystem for a WPAR are excluded from remediation.

Note: WPARs built as filesystems should be considered non-production or test. Production WPARs should be located solely in WPAR storage devices. See the option **mkwpar -D**.

Audit:

These commands should not produce any output:

```
lsfs | /usr/bin/grep jfs | /usr/bin/egrep -v "/dev/hd4|nodev"  
mount | /usr/bin/grep jfs | /usr/bin/egrep -v "/dev/hd4|nodev"
```

Remediation:

- The following command remounts filesystems with 'nodev' added:

```
mount | grep jfs | /usr/bin/egrep -v "/dev/hd4|nodev" | while read lv fs jfs
m d t options
do
mount -o remount,${options},nodev $fs
done
```

- The following command updates the stanza in /etc/filesystems

```
lsfs | grep jfs | /usr/bin/egrep -v "/dev/hd4|nodev" | while read lv node fs
jfs size options rest
do
if [ ${options} == "--" ]; then
    chfs -a options=nodev $fs
else
    chfs -a options=${options},nodev $fs
fi
done
```

Default Value:

By default, AIX allows the definition of device files on any filesystem.

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.	●	●	●

4.5 Configure Network Options

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.

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.

These are recommendations that do not currently map directly to a CIS Control, however, they are directly related to the concept of a secure installation and system integrity.

The recommendations here are all managed by the program `/usr/sbin/no`.

We are not (currently) making a difference between IPv4 and IPv6 for these settings.

4.5.1 Ensure sockthresh is configured

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:

Run the following command to set the **sockthresh** entry:

```
no -p -o sockthresh=60
```

Default Value:

N/A

4.5.2 Ensure *bcastping* is disabled

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:

Run the following command to set the **bcastping** entry:

```
no -p -o bcastping=0
```

Default Value:

1

CIS Controls:

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

4.5.3 Ensure clean_partial_conns is enabled

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:

Run the following command to set the `clean_partial_conns` entry:

```
no -p -o clean_partial_conns=1
```

Default Value:

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.		●	●

4.5.4 Ensure directed_broadcast is disabled

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:

Run the following command to set the **directed_broadcast** entry:

```
no -p -o directed_broadcast=0
```

Default Value:

1

CIS Controls:

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

4.5.5 Ensure icmpaddressmask is disabled

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:

Run the following command to set the **icmpaddressmask** entry:

```
no -p -o icmpaddressmask=0
```

Default Value:

1

CIS Controls:

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

4.5.6 Ensure ipforwarding is disabled

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:

Run the following command to set the **ipforwarding** entry:

```
no -p -o ipforwarding=0
```

Default Value:

0

CIS Controls:

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

4.5.7 Ensure ip6forwarding is disabled

Profile Applicability:

- Level 1

Description:

The **ip6forwarding** parameter determines whether or not the system forwards IPv6 TCP/IP packets.

Rationale:

The **ip6forwarding** parameter will be set to **0**, to ensure that redirected packets do not reach remote networks. This should only be enabled if the system is performing the function of an IP router. This is typically handled by a dedicated network device.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ip6forwarding[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ip6forwarding = 0
```

Remediation:

Run the following command to set the **ip6forwarding** entry:

```
no -p -o ip6forwarding=0
```

Default Value:

0

CIS Controls:

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

4.5.8 Ensure `ipignoreredirects` is enabled

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:

Run the following command to set the `ipignoreredirects` entry:

```
no -p -o ipignoreredirects=1
```

Default Value:

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.			

4.5.9 Ensure ipsendredirects is disabled

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:

Run the following command to set the **ipsendredirects** entry:

```
no -p -o ipsendredirects=0
```

Default Value:

1

CIS Controls:

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

4.5.10 Ensure *ipsrcrouteforward* is disabled

Profile Applicability:

- Level 1

Description:

The **ipsrcrouteforward** parameter determines whether or not the system forwards IPV4 source-routed packets.

Rationale:

The **ipsrcrouteforward** 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 "ipsrcrouteforward[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcrouteforward = 0
```

Remediation:

Run the following command to set the **ipsrcrouteforward** entry:

```
no -p -o ipsrcrouteforward=0
```

Default Value:

1

CIS Controls:

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

4.5.11 Ensure ipsrcrouterecv is disabled

Profile Applicability:

- Level 1

Description:

The **ipsrcrouterecv** parameter determines whether the system accepts source routed packets.

Rationale:

The **ipsrcrouterecv** parameter will be set to 0, This means that the system will not accept source routed packets. By default, when this is enabled the system is susceptible to source routing attacks.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcrouterecv[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcrouterecv = 0
```

Remediation:

Run the following command to set the **ipsrcrouterecv** entry:

```
no -p -o ipsrcrouterecv=0
```

Default Value:

1

CIS Controls:

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

4.5.12 Ensure ipsrcroutesend is disabled

Profile Applicability:

- Level 1

Description:

The **ipsrcroutesend** parameter determines whether or not the system can send source-routed packets.

Rationale:

The **ipsrcroutesend** parameter will be set to 0, to ensure that any local applications cannot send source routed packets.

Audit:

From the command prompt, execute the following command:

```
no -a |grep "ipsrcroutesend[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
ipsrcroutesend = 0
```

Remediation:

Run the following command to set the **ipsrcroutesend** entry:

```
no -p -o ipsrcroutesend=0
```

Default Value:

1

CIS Controls:

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

4.5.13 Ensure `ip6srcrouteforward` is disabled

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:

Run the following command to set the `ip6srcrouteforward` entry:

```
no -p -o ip6srcrouteforward=0
```

Default Value:

1

CIS Controls:

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

4.5.14 Ensure `nfs_use_reserved_ports` is enabled

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:

```
nfso -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:

Run the following commands to set the `portcheck` and `nfs_use_reserved_ports` entries:

```
nfso -p -o portcheck=1
nfso -p -o nfs_use_reserved_ports=1
```

Default Value:

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.		●	●

4.5.15 Ensure nonlocsrcroute is disabled

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:

Run the following command to set the **nonlocsrcroute** entry:

```
no -p -o nonlocsrcroute=0
```

Default Value:

1

CIS Controls:

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

4.5.16 Ensure `tcp_pmtu_discover` is disabled

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 has the potential to disrupt network availability.

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:

Run the following command to set the `tcp_pmtu_discover` entry:

```
no -p -o tcp_pmtu_discover=0
```

Default Value:

1

CIS Controls:

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

4.5.17 Ensure tcp_tcpsecure is configured

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:

Run the following command to set the `tcp_tcpsecure` entry:

```
no -p -o tcp_tcpsecure=7
```

Default Value:

`tcp_tcpsecure = 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.		●	●

4.5.18 Ensure `udp_pmtu_discover` is disabled

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 has the potential to disrupt network availability.

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:

Run the following command to set the `udp_pmtu_discover` entry:

```
no -p -o udp_pmtu_discover=0
```

Default Value:

1

CIS Controls:

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

4.5.19 Ensure *icmptimestamp* is disabled

Profile Applicability:

- Level 1

Description:

The **icmptimestamp** parameter determines whether the system responds to an ICMP timestamp request.

Rationale:

Responding to an ICMP timestamp request may provide a remote user with more detailed information about the current date/time of the system. By accurately determining the target's clock state, an attacker can more effectively attack certain time-based pseudorandom number generators (PRNGs) and the authentication systems that rely on them

Audit:

From the command prompt, execute the following command:

```
no -a |grep "icmptimestamp[[:blank:]]=[[:blank:]]0"
```

The above command should yield the following output:

```
icmptimestamp = 0
```

Remediation:

Run the following command to set the **icmptimestamp** entry:

```
no -p -o icmptimestamp=0
```

Default Value:

AIX 7.2 = 1

AIX 7.3 = 0

References:

1. CVE-1999-0524

CIS Controls:

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

4.6 Standard Services and Applications

This sub-section presents recommendations on the configuration of standard applications and/or services.

The focus is on Application settings that enhance application security (thereby indirectly enhancing system integrity).

DRAFT

4.6.1 Configure Common Desktop Environment

Common Desktop Environment (CDE) has a history of security problems and should be disabled or removed. However, if the server, better workstation, has a graphics adapter and CDE is used as the graphical user interface (GUI) then the recommendations in this section should be followed to enhance security.

If CDE is not required the recommendation is that the filesets are de-installed to avoid exposure to potential security vulnerabilities. The recommendations that remain are only scored when CDE is installed.

DRAFT

4.6.1.1 Ensure CDE is not installed

Profile Applicability:

- Level 1

Description:

The recommendation is to de-install CDE aka X11.Dt from the system, assuming that it is not required and is already installed.

Rationale:

CDE has a history of security problems and should be disabled.

NOTE: If CDE is required, it is vital to patch the software and consider TCP Wrappers to further enhance security.

Audit:

Validate the de-installation of the software:

```
lslpp -L |grep -i X11.Dt
```

The above command should yield no output.

Remediation:

Identity if **CDE** is already installed:

```
lslpp -L |grep -i X11.Dt
```

If there are CDE filesets installed - de-install them if CDE is not required. For each fileset preview the de-installation:

```
installp -up <fileset name>
```

Review the fileset removal preview output, paying particular attention to the other pre-requisites that will also be removed. Typically only **X11.Dt** filesets should be de-installed as pre-requisites. Once reviewed, de-install the fileset and pre-requisites:

```
installp -ug <fileset name>
```

NOTE: Repeat until all CDE related filesets are de-installed

Default Value:

N/A

Additional Information:

Reversion:

Re-install the CDE software from the AIX media.

CIS Controls:

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

4.6.1.2 Ensure the cmsd service is not available

Profile Applicability:

- Level 1

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 'sunrpc_udp'
refresh -s inetd
```

Default Value:

Uncommented

CIS Controls:

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

4.6.1.3 Ensure dtlogin service is not available

Profile Applicability:

- Level 1

Description:

Do not start CDE automatically on system boot.

Rationale:

As the benchmark is intended for use on logical partitions which will not have a graphical console, CDE should not be started automatically to reduce the attack surface of the system.

Audit:

Validate that CDE start-up is disabled

```
lsitab dt
lsitab dt_nogb
```

The above commands should yield no output.

Remediation:

Disable CDE start up:

```
/usr/dt/bin/dtconfig -d
```

End any current instances:

```
/usr/dt/bin/dtconfig -kill
```

NOTE: If CDE is not installed the command will not be found

Default Value:

N/A

CIS Controls:

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

4.6.1.4 Ensure dtspc is not available

Profile Applicability:

- Level 1

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.		●	●

4.6.1.5 Ensure CDE daemons have sgid and suid mode disabled

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

4.6.1.6 Ensure CDE remote GUI login is disabled

Profile Applicability:

- Level 1

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.		●	●

4.6.1.7 Ensure CDE screensaver lock is enabled

Profile Applicability:

- Level 1

Description:

The timeout of keyboard and mouse inactivity before a password protected screensaver is invoked by the CDE session manager should be explicitly configured.

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 15 minutes or less to protect from unauthorized access on unattended systems.

Audit:

Validate the changes to the **sys.resources** files:

```
for file in /usr/dt/config/*/sys.resources; do
    etc_file=`echo $file | sed -e s/usr/etc/`
    echo "\nChecking config file \"$etc_file\"..."
    if [[ ! -f $etc_file ]]; then
        echo "Missing config file \"$etc_file"
    else
        grep 'dtsession*saverTimeout:' $etc_file || echo "Missing setting
dtsession*saverTimeout"
        grep 'dtsession*lockTimeout:' $etc_file || echo "Missing setting
dtsession*lockTimeout"
    fi
done
```

The above command should yield a similar output to the following:

```
Checking config file /etc/dt/config/C/sys.resources...
dtsession*saverTimeout: 15
dtsession*lockTimeout: 15
```

Any files or values which are listed as missing or have value which exceeds the recommended or site defined value are deemed to be a failure.

Remediation:

Set the default timeout parameters **dtsession*saverTimeout:** and **dtsession*lockTimeout:**

```
for file in /usr/dt/config/*/sys.resources; do
  etc_file=`echo $file | sed -e s/usr/etc/`
  echo "\nupdating config file \"$etc_file\"..."
  if [[ ! -f $etc_file ]]; then
    dir=`dirname $file | sed -e s/usr/etc/`
    mkdir -p $dir
    cp $file $etc_file
  fi

  cp $etc_file $etc_file.bak
  grep -v 'dtsession\*saverTimeout:' $etc_file > $etc_file.sav
  grep -v 'dtsession\*lockTimeout:' $etc_file.sav > $etc_file
  echo 'dtsession*saverTimeout: 15' >> $etc_file
  echo 'dtsession*lockTimeout: 15' >> $etc_file
  rm $etc_file.sav
done
```

Default Value:

N/A

References:

1. STIG ID: AIX7-00-003000 | SV-215318r958402 | CAT II

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.	●	●	●

4.6.1.8 Ensure CDE login screen hostname is masked

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:

```
for file in /usr/dt/config/*/Xresources; do
    etc_file=`echo $file | sed -e s/usr/etc/`
    echo "\nChecking config file \"$etc_file\"..."
    if [[ ! -f $etc_file ]]; then
        echo "Missing config file \"$etc_file"
    else
        grep 'Dtlogin*greeting.labelString:' $etc_file || echo "Missing setting
greeting.labelString"
        grep 'Dtlogin*greeting.persLabelString:' $etc_file || echo "Missing
setting greeting.persLabelString"
    fi
done
```

The above command should yield a similar output to the following:

```
Checking config file /etc/dt/config/C/Xresources...
Dtlogin*greeting.labelString: Authorized uses only. All activity may be
monitored and reported.
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
  etc_file=`echo $file | sed -e s/usr/etc/`
  echo "\nupdating config file \"$etc_file\"..."
  if [[ ! -f $etc_file ]]; then
    dir=`dirname $file | sed -e s/usr/etc/`
    mkdir -p $dir
    cp $file $etc_file
  fi

  WARN="Authorized uses only. All activity may be monitored and reported."
  cp $etc_file $etc_file.bak
  grep -v 'Dtlogin*greeting.labelString:' $etc_file > $etc_file.sav
  grep -v 'Dtlogin*greeting.persLabelString:' $etc_file.sav > $etc_file
  echo "Dtlogin*greeting.labelString: $WARN" >> $etc_file
  echo "Dtlogin*greeting.persLabelString: $WARN" >> $etc_file
  rm $etc_file.sav
done

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

References:

- 1. STIG ID: AIX7-00-001042 | SV-215201r958390 | CAT II

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.6.1.9 Ensure access to /etc/dt/config/Xconfig is configured

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	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.			

4.6.1.10 Ensure the file `/etc/dt/config/Xservers` is configured

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:

- IF - the file `/etc/dt/config/Xservers` exists, run the following commands:

Run the following command to 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
```

Run the following command to verify the absolute path is used:

```
/usr/bin/egrep '^s*dtlogin' /etc/dt/config/Xconfig
```

Verify the output includes:

```
Dtlogin*servers: /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.			

4.6.1.11 Ensure access to Xresources is configured

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 id `root`, group ownership is `sys`, and mode is `0644` or more restrictive:

```
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-x,go-wx /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.			

4.6.2 Configure FTPD

The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

FTP does not protect the confidentiality of data or authentication credentials. It is recommended SFTP be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the service be made unavailable.

Where an FTP server is required, this section contains recommendations for the secure configuration of FTPD.

DRAFT

4.6.2.1 Ensure root access to ftpd is disabled

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	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

4.6.2.2 Ensure ftpd login banner is configured

Profile Applicability:

- Level 1

Description:

Set an **ftpd** login banner which displays the acceptable usage policy.

Rationale:

The message in **banner.msg** is displayed for FTP logins. Banners display necessary warnings to users trying to gain unauthorized access to the system and are required for legal purposes. The recommendation is to set the banner as:

"Authorized uses only. All activity will be monitored and reported".

The content may be changed to reflect any corporate AUP.

Audit:

If **ftpd** is active verify the catalog is installed and the login banner has been updated:

```
if [[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]]; then
    lslpp -L "bos.msg.en_US.net.tcp.client" >/dev/null && print $(dspcat
/usr/lib/nls/msg/en_US/ftpd.cat 1 9)
else
    RC=0
fi
```

The above command should yield the following output:

```
"%s Authorized uses only. All activity may be monitored and reported"
```

Remediation:

Ensure that the **bos.msg.en_US.net.tcp.client** fileset is installed:

```
lslpp -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 **ftpd** AUP banner:

```
dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.tmp
sed "s/\"\\\"%s FTP server (\\%) ready.\\\"/\"\\\"%s Authorized uses only. All
activity may be monitored and reported\\\"/" /tmp/ftpd.tmp > /tmp/ftpd.msg
gencat /usr/lib/nls/msg/en_US/ftpd.cat /tmp/ftpd.msg
rm /tmp/ftpd.tmp /tmp/ftpd.msg
```

Default Value:

%s FTP server (%s) ready.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

DRAFT

4.6.2.3 Ensure `ftpd` umask is configured

Profile Applicability:

- Level 1

Description:

The umask of the `ftpd` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-accessable, group-writeable files by default.

Rationale:

The umask of the `ftpd` service should be set to at least 027 in order to prevent the FTP daemon process from creating world-accessable and group-writeable files by default. These files could then be transferred over the network which could result in compromise of the critical information.

Audit:

Validate the umask setting:

```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && grep  
"^ftp[[:blank:]]" /etc/inetd.conf |awk '{print $6, $7, $8, $9, $10}' || RC=0
```

The above command should yield the following output (only if the ftp daemon is not disabled):

```
/usr/sbin/ftpd ftpd -l -u 027
```

Remediation:

Set the default umask of the `ftp` daemon:

```
[[ $(grep -c "^ftp[[:blank:]]" /etc/inetd.conf) -gt 0 ]] && chsubserver -c -v  
ftp -p tcp "ftpd -l -u 027" && refresh -s inetd || RC=0
```

NOTE: The umask above restricts write permissions for both group and other. All access for other is removed.

Default Value:

```
/usr/sbin/ftpd ftpd -l
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	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.			

4.6.3 Configure OpenSSH

SSH is a secure, encrypted replacement for common clear-text login services such as telnet, ftp, rlogin, rsh, and rcp. Wherever remote access is required, SSH should be utilized to protect communications from unauthorized interception.

Other sections in this benchmark recommend disabling clear-text protocols. Although some legacy applications may still require clear-text protocols, SSH should still be used alongside the non-encrypted services.

This section contains recommendations for the secure configuration of OpenSSH.

Note: Some of the recommendations are default values. The best practice is to include the settings in the configuration file with an explicit statement - rather than implicit - as defaults may change. In other words: explicit declaration ensures that recommendations remain constant over time.

OpenSSH requires each side (client/server) to negotiate multiple connection parameters. These are corresponding `ssh_config`/`sshd_config` keywords:

- **KexAlgorithms**: the key exchange methods that are used to generate *per-connection keys*.
- **HostkeyAlgorithms**: the public key algorithms accepted for an SSH server to *authenticate itself to an SSH client*.
- **Ciphers**: the *ciphers to encrypt* the connection.
- **MACs**: the message authentication codes *used to detect traffic modification*.

4.6.3.1 Ensure latest version of openssh is installed

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 9.9p2 released February 18, 2025. IBM's policy is to stay at a constant level (currently 9.9) 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 9.9. The **openssh** fileset VRMF number should start with **9.9**.

Audit:

The following command should return **Version 9+**

```
test $(sshd -i </dev/null | cut -d _ -f 2) -ge 9 && print "Version 9+" ||  
print "Insufficient"
```

Remediation:

Install OpenSSH version 9.9 (or later), depending on package source.

The current version available from IBM via [AIX Web Download Pack Programs](#) is **9.9.3015.1000**.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.2 Ensure /etc/shosts.equiv and /etc/rhosts.equiv are removed

Profile Applicability:

- Level 1

Description:

The recommendation is to remove both the `/etc/shosts.equiv` and `/etc/rhosts.equiv` file. This is a consequence of the recommendation to not use `HostbasedAuthentication`.

Rationale:

The recommendation is to not use `HostbasedAuthentication` unless there is a documented need already exists the logical consequence is to remove these files, if they exist, to lower the risk of accidental activation.

In any case - the file `/etc/rhosts.equiv` should be removed - period. (**Note:** This is also recommended elsewhere.)

Impact:

The file `/etc/shosts.equiv`, in combination with the OpenSSH `sshd_config`: `HostbasedAuthentication`, can allow passwordless authentication between servers.

Without `HostbasedAuthentication` the file `/etc/shosts.equiv` has no purpose.

Audit:

Ensure that the files `/etc/shosts.equiv` and `/etc/rhosts.equiv` have been removed:

```
ls -l /etc/[rs]hosts.equiv && /usr/bin/printf "Remove file: %s\n"
/etc/[rs]hosts.equiv
```

The above command should yield no output.

Remediation:

Print (for review) and then remove the content of the `/etc/[rs]hosts.equiv` files:

```
for file in /etc/[rs]hosts.equiv; do
    print "+++ ${file} +++"
    /usr/bin/cat -n ${file}
    /usr/bin/rm -f ${file}
done
```

Default Value:

N/A

Additional Information:

Reversion:

- The `/etc/shosts.equiv` file would need to be restored from a backup or from the remediation log.
- The file `/etc/rhosts.equiv` should not be restored.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.6.3.3 Ensure sftp-server arguments are configured

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. The **sftp-server** does not inherit the logging levels from **sshd** and they must be configured manually.

SFTP provides several logging levels with varying amounts of verbosity. The **DEBUG** options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

Rationale:

The **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.

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

Audit:

Run the following command:

```
# /usr/sbin/sshd -T | /usr/bin/egrep -i 'subsystem sftp'
```

Verify that output matches one of the options below:

```
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l INFO
- OR -
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l VERBOSE
- OR -
Subsystem sftp internal-sftp -u 027 -f AUTH -l INFO
- OR -
Subsystem sftp internal-sftp -u 027 -f AUTH -l VERBOSE
```

Remediation:

Edit the `/etc/ssh/sshd_config` and set the sftp arguments to one of the following:

```
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l INFO
- OR -
Subsystem sftp /usr/sbin/sftp-server -u 027 -f AUTH -l VERBOSE
- OR -
Subsystem sftp internal-sftp -u 027 -f AUTH -l INFO
- OR -
Subsystem sftp internal-sftp -u 027 -f AUTH -l VERBOSE
```

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

```
# /usr/bin/stopsrc -s sshd; /usr/bin/sleep 5; /usr/bin/startsrc -s sshd
```

Additional Information:

The AIX implementation of OpenSSH does not make use of `Include` statements by default, so these are not considered within the audit or remediation. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

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.	●	●	●
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.6.3.4 Ensure sshd access is configured

Profile Applicability:

- Level 1

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged:

- **AllowUsers:**
 - The **AllowUsers** variable gives the system administrator the option of allowing specific users to **ssh** into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.
- **AllowGroups:**
 - The **AllowGroups** variable gives the system administrator the option of allowing specific groups of users to **ssh** into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.
- **DenyUsers:**
 - The **DenyUsers** variable gives the system administrator the option of denying specific users to **ssh** into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.
- **DenyGroups:**
 - The **DenyGroups** variable gives the system administrator the option of denying specific groups of users to **ssh** into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable.

Rationale:

By default, login is allowed for all users and all groups.

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

Audit:

Run the following command and verify the output:

```
# sshd -T | /usr/bin/egrep -i  
"^(AllowUsers|AllowGroups|DenyUsers|DenyGroups) [[:blank:]]"
```

The above command should yield at least one of the following output: Verify that the output of both commands matches at least one of the following lines:

```
allowusers <userlist>  
-OR-  
allowgroups <grouplist>  
-OR-  
denyusers <userlist>  
-OR-  
denygroups <grouplist>
```

- IF -

- **AllowUsers** and/or **AllowGroups** is returned, review the list(s) to ensure included users and/or groups follow local site policy

Remediation:

Edit the **/etc/ssh/sshd_config** file to set one or more of the parameter above any **Match** set entries as follows:

```
AllowUsers <userlist>  
-OR-  
AllowGroups <grouplist>  
-OR-  
DenyUsers <userlist>  
-OR-  
DenyGroups <grouplist>
```

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

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

Note: First occurrence of a option takes precedence, **Match** set statements withstanding.

Default Value:

All users from any host are permitted.

Additional Information:

The AIX implementation of OpenSSH does not make use of Include statements by default, so these are not considered within the audit or remediation. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the **Include** location used.

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.			

4.6.3.5 Ensure sshd Banner is configured

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command:

```
sshd -T | /usr/bin/egrep -i "^banner[[:blank:]]"
```

Verify the output matches:

```
banner /etc/ssh/ssh_banner
```

Run the following command to verify that `/etc/ssh/sshd_config` does not include setting **Banner** to **none**:

```
# /usr/bin/egrep -i '^s*Banner\s+\\"?none' /etc/ssh/sshd_config
```

Nothing should be returned

- **IF** - **Match** set statements are used in your environment, `/etc/ssh/sshd_config` should be reviewed to verify:

- the setting is not only in a **Match** block
- **Match** blocks do not contain any incorrect or conflicting options

Run the following command and verify that the contents or the file being called by the **Banner** argument match site policy:

```
# [ -e "$(sshd -T | awk '$1 == "banner" {print $2}')" ] && cat "$(sshd -T | awk '$1 == "banner" {print $2}')
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Match set entries as follows:

```
Banner /etc/ssh/ssh_banner
```

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

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

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Edit the file being called by the `Banner` argument with the appropriate contents according to your site policy.

Default Value:

No banner is configured

Additional Information:

The AIX implementation of OpenSSH does not make use of `Include` statements by default, so these are not considered within the audit or remediation. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.6 Ensure sshd Ciphers are configured

Profile Applicability:

- Level 1

Description:

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

Notes:

- Some organizations may have stricter requirements for approved ciphers.
- Ensure that ciphers used are in compliance with site policy.
- The only "strong" ciphers currently FIPS 140 compliant are:
 - aes256-gcm@openssh.com
 - aes128-gcm@openssh.com
 - aes256-ctr
 - aes192-ctr
 - aes128-ctr

Rationale:

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

- The Triple DES ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain clear text data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack.
- Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plain text data from an arbitrary block of cipher text in an SSH session via unknown vectors.

Audit:

Run the following command to verify none of the "weak" ciphers are being used:

```
# sshd -T | /usr/bin/egrep -i
'^ciphers[[:blank:]]\\"?([^\n\r]+,)?((3des|blowfish|cast128|aes(128|192|256))
-cbc|arcfour(128|256)?|rijndael-cbc@lysator.liu.se|chacha20-
poly1305@openssh.com)'
```

- **IF** - a line is returned, review the list of ciphers. If the line includes **chacha20-poly1305@openssh.com**, review **CVE-2023-48795** and verify the system has been patched. No ciphers in the list below should be returned as they're considered "weak":

```
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
```

Remediation:

Edit the **/etc/ssh/sshd_config** file and add/modify the **Ciphers** line to contain a comma separated list of the site unapproved (weak) Ciphers preceded with a **-**:

Example:

```
Ciphers -3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,chacha20-
poly1305@openssh.com
```

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

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

Additional Information:

The AIX implementation of OpenSSH does not make use of **Include** statements by default, so these are not considered within the audit or remediation. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

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.			

4.6.3.7 Ensure sshd HostbasedAuthentication is disabled

Profile Applicability:

- Level 1

Description:

The **HostbasedAuthentication** parameter specifies if authentication is allowed through trusted hosts via the user of **.rhosts**, or **/etc/hosts.equiv**, along with successful public key client host authentication.

Rationale:

Host-based authentication is a method to authenticate users (rather than requiring password or key-based authentication method). Used at a system level by OpenSSH requires the file **/etc/shosts.equiv** to contain a list of so-called *trusted* hosts. When this method is active any user on a trusted host can login to the server as *authenticated* because the server identity the user imitates the connection from (aka the OpenSSH client) authenticates the user as *trusted*.

Since this feature disables **user-based** authentication from some hosts - our recommendation is to disable host-based authentication.

Audit:

Run the following command to verify **HostbasedAuthentication** is set to **no**:

```
# sshd -T | grep hostbasedauthentication  
hostbasedauthentication no
```

Run the following command and verify the output:

```
# /usr/bin/egrep -i '^s*HostbasedAuthentication\s+\\"?yes'  
/etc/ssh/sshd_config
```

Nothing should be returned

- **IF - Match** set statements are used in your environment, **/etc/ssh/sshd_config** should be reviewed to verify:

- the setting is not only in a **Match** block
- **Match** blocks do not contain any incorrect or conflicting options

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any **Match** entries as follows:

```
HostbasedAuthentication no
```

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

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

Note: First occurrence of a option takes precedence, **Match** set statements withstanding.

Default Value:

HostbasedAuthentication no

Additional Information:

The AIX implementation of OpenSSH does not make use of Include statements by default, so these are not considered within the audit or remediation. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

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

4.6.3.8 Ensure sshd IgnoreRhosts is enabled

Profile Applicability:

- Level 1

Description:

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

Rationale:

Setting this parameter forces users to enter a password or provide an SSH key when authenticating with SSH, rather than trusting the remote host.

Audit:

Run the following command:

```
# sshd -T | grep ignorerhosts
```

Verify the output matches:

```
ignorerhosts yes
```

Run the following command to verify that **/etc/ssh/sshd_config** does not include setting **IgnoreRhosts** to **no**:

```
# /usr/bin/egrep -i '^s*IgnoreRhosts\s+\\"no' /etc/ssh/sshd_config
```

Nothing should be returned

- **IF** - **Match** set statements are used in your environment, **/etc/ssh/sshd_config** should be reviewed to verify:

- the setting is not only in a **Match** block
- **Match** blocks do not contain any incorrect or conflicting options

Remediation:

Edit the **/etc/ssh/sshd_config** file to set the parameter above any **Match** set entries as follows:

```
IgnoreRhosts yes
```

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

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

Note: First occurrence of a option takes precedence, **Match** set statements withstanding.

Default Value:

IgnoreRhosts yes

References:

1. sshd_config(5)

Additional Information:

The AIX implementation of OpenSSH does not make use of **Include** statements by default, so these are not considered within the audit or remediation. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.6 Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

4.6.3.9 Ensure sshd KexAlgorithms is configured

Profile Applicability:

- Level 1

Description:

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

Notes:

- Kex algorithms have a higher preference the earlier they appear in the list
- Some organizations may have stricter requirements for approved Key exchange algorithms
- Ensure that Key exchange algorithms used are in compliance with site policy
- The only Key Exchange Algorithms currently FIPS 140-2 approved are:
 - ecdh-sha2-nistp256 - ecdh-sha2-nistp384 - ecdh-sha2-nistp521 - diffie-hellman-group-exchange-sha256 - diffie-hellman-group16-sha512 - diffie-hellman-group18-sha512 - diffie-hellman-group14-sha256
- The Key Exchange algorithms supported by OpenSSH 8.2 are:

```
curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
sntrup4591761x25519-sha512@tinyssh.org
```

Rationale:

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

Impact:

Weak clients no longer connect.

Audit:

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

```
# sshd -T -C user=root -C host="$(hostname)" -C addr="$(grep $(hostname) /etc/hosts | awk '{print $1}')" | grep kexalgorithms
```

Weak Key Exchange Algorithms:

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

Remediation:

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

Example:

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

Default Value:

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

References:

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

Additional Information:

Following CIS Debian Family Linux benchmarks.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	16.4 <u>Encrypt or Hash all Authentication Credentials</u> Encrypt or hash with a salt all authentication credentials when stored.		●	●

4.6.3.10 Ensure sshd LogLevel is configured

Profile Applicability:

- Level 1

Description:

SSH provides several logging levels with varying amounts of verbosity. The **DEBUG** options are specifically not recommended other than strictly for debugging SSH communications. These levels provide so much data that it is difficult to identify important security information, and may violate the privacy of users.

Rationale:

The **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.

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

Audit:

Run the following command and verify that output matches **loglevel VERBOSE** or **loglevel INFO**:

```
# sshd -T | grep loglevel  
  
loglevel VERBOSE  
- OR -  
loglevel INFO
```

- **IF - Match** set statements are used in your environment, **/etc/ssh/sshd_config** should be reviewed to verify:

- the setting is not only in a **Match** block
- **Match** blocks do not contain any incorrect or conflicting options

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter above any Match set entries as follows:

```
LogLevel VERBOSE
- OR -
LogLevel INFO
```

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

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

Note: First occurrence of a option takes precedence, `Match` set statements withstanding.

Default Value:

`#LogLevel INFO`

Additional Information:

The AIX implementation of OpenSSH does not make use of `Include` statements by default, so these are not considered within the audit or remediation. If `Include` locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

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.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

4.6.3.11 Ensure sshd MACs are configured

Profile Applicability:

- Level 1

Description:

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

Notes:

- Some organizations may have stricter requirements for approved MACs.
- Ensure that MACs used are in compliance with site policy.
- The only "strong" MACs currently FIPS 140 approved are:
 - HMAC-SHA1
 - HMAC-SHA2-256
 - HMAC-SHA2-384
 - HMAC-SHA2-512

Rationale:

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

Audit:

Run the following command to verify none of the "weak" MACs are being used:

```
# sshd -T | /usr/bin/egrep -i 'macs[[:blank:]]([^\n\r]+,)?(hmac-md5|hmac-md5-96|hmac-ripemd160|hmac-sha1-96|umac-64@openssh\.com|hmac-md5-etm@openssh\.com|hmac-md5-96-etm@openssh\.com|hmac-ripemd160-etm@openssh\.com|hmac-sha1-96-etm@openssh\.com|umac-64-etm@openssh\.com|umac-128-etm@openssh\.com) '
```

Nothing should be returned

Note: Review [CVE-2023-48795](#) and verify the system has been patched. If the system has not been patched, review the use of the Encrypt Then Mac (etm) MACs.

The following are considered "weak" MACs, and should not be used:

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

Remediation:

Edit the `/etc/ssh/sshd_config` file and add/modify the **MACs** line to contain a comma separated list of the site unapproved (weak) MACs preceded with a `-`:

Example:

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

- **IF - CVE-2023-48795** has not been reviewed and addressed, the following **etm** MACs should be added to the exclude list: **hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com**

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

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

Default Value:

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

Additional Information:

The AIX implementation of OpenSSH does not make use of **Include** statements by default, so these are not considered within the audit or remediation. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

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.		●	●

4.6.3.12 Ensure sshd MaxAuthTries is configured

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

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

```
sshd -T | grep maxauthtries
```

Remediation:

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

```
MaxAuthTries 4
```

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

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.13 Ensure sshd PermitEmptyPasswords is disabled

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	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.14 Ensure sshd PermitRootLogin is configured

Profile Applicability:

- Level 1

Description:

This recommendation disables direct root login via SSH using a password. To be absolutely certain direct login is disabled the recommendation requires this variable is set rather than rely on a default that might change after an update to SSH.

The recommendation requires an edit of the file `/etc/ssh/sshd_config` file to disable direct root login.

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.

Direct root login via SSH was enabled by default with prior versions of OpenSSH.

Impact:

The level 1 recommendation does not *require* a setting of `no` - setting the attribute to `no` requires either sharing a root password (to use `su`), the installation of `sudo`, or a configuration using `extended RBAC` for actions that require enhanced privileges.

The recommendation `4.3.6.10` specifies a `LOG_LEVEL` of `INFO` or `DEBUG`.

To resolve, partially, the accountability concerns, permitting `publickey` authentication as root together with `LogLevel INFO` (minimum) provides the following `syslog` information:

```
Jun 25 09:26:41 x071 auth|security:info sshd[8323282]: Accepted publickey for michael from 192.168.129.11 port 54278 ssh2: RSA  
SHA256: dRHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk  
Jun 25 09:26:52 x071 auth|security:info sshd[8847396]: Accepted publickey for root from 192.168.129.11 port 54279 ssh2: RSA  
SHA256: dRHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk  
Jun 25 09:26:53 x071 auth|security:info sshd[9044142]: Accepted publickey for root from 192.168.129.11 port 54280 ssh2: RSA  
SHA256: dRHxa5CGr5HCdC89suwYIBtAT8lyogz4SErSxTq0JXk
```

Local site policy might decide that publickey accountability is sufficient and a setting of `PermitRootLogin prohibit-password` (the new default) provides sufficient accountability and security.

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

Audit:

Ensure that the **PermitRootLogin** parameter has been changed:

```
/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config
```

The above command should yield one of the following:

```
PermitRootLogin prohibit-password
PermitRootLogin no
PermitRootLogin forced-commands-only
```

Remediation:

```
#!/usr/bin/ksh
PREFERRED_SETTING="prohibit-password"
umask 077
set $(/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config)
echo $?
if [[ ! -z $1 ]]; then
    # Look for a setting and change to no if anything else
    if [[ $2 != ${PREFERRED_SETTING} ]]; then
        sed "s/^PermitRootLogin \\{1\\}[^ ]\\{1,\\}/PermitRootLogin
${PREFERRED_SETTING}/" /etc/ssh/sshd_config >/tmp/sshd_config.$$
    fi
else
    # Look for a comment and append
    sed "/^# \\{0,\\}PermitRootLogin/ a\\^JPermitRootLogin ${PREFERRED_SETTING}/"
/etc/ssh/sshd_config >/tmp/sshd_config.$$
fi

if [[ -e /tmp/sshd_config.$$ ]]; then
    diff -u /tmp/sshd_config.$$ /etc/ssh/sshd_config
    rm /tmp/sshd_config.$$
elif
    # Verify setting is specified
    /usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config >>/dev/null
    if [[ $? -ne 0 ]]; then
        print "PermitRootLogin ${PREFERRED_SETTING}" >> /etc/ssh/sshd_config
    fi
fi
```

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

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

Default Value:

PermitRootLogin prohibit-password

Additional Information:

The values for this parameter have been **yes** (not recommended), **no** (not recommended, but accepted), **prohibit-password** (recommended setting), **forced-commands-only** (not recommended, but accepted) and **without-password** (deprecated setting).

PermitRootLogin:

Specifies whether root can log in using ssh(1). The argument must be yes, prohibit-password, forced-commands-only, or no. The default is prohibit-password. If this option is set to prohibit-password (or its deprecated alias, without-password), password and keyboard-interactive authentication are disabled for root. If this option is set to forced-commands-only, root login with public key authentication will be allowed, but only if the command option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root. If this option is set to no, root is not allowed to log in.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.15 Ensure sshd PermitRootLogin is disabled

Profile Applicability:

- Level 2

Description:

The `PermitRootLogin` parameter specifies if the root user can log in using SSH. The current default is `prohibit-password`.

Rationale:

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

Impact:

The level 1 recommendation does not *require* a setting of `no` - 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.

Level 2 recommendation is to align with other Benchmarks that set `PermitRootLogin` to `no`.

Audit:

Ensure that the **PermitRootLogin** parameter has been changed:

```
/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config
```

The above command should yield the following:

```
PermitRootLogin no
```

Remediation:

```
#!/usr/bin/ksh
PREFERRED_SETTING="no"
umask 077
set $(/usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config)
echo $?
if [[ ! -z $1 ]]; then
    # Look for a setting and change to no if anything else
    if [[ $2 != ${PREFERRED_SETTING} ]]; then
        sed "s/^PermitRootLogin \\{1\\}[^ ]\\{1,\\}/PermitRootLogin
${PREFERRED_SETTING}/" /etc/ssh/sshd_config >/tmp/sshd_config.$$
    fi
else
    # Look for a comment and append
    sed "/^# \\{0,\\}PermitRootLogin/ a\\^JPermitRootLogin ${PREFERRED_SETTING}/"
/etc/ssh/sshd_config >/tmp/sshd_config.$$
fi

if [[ -e /tmp/sshd_config.$$ ]]; then
    diff -u /tmp/sshd_config.$$ /etc/ssh/sshd_config
    rm /tmp/sshd_config.$$
elif
    # Verify setting is specified
    /usr/bin/egrep "^PermitRootLogin" /etc/ssh/sshd_config >>/dev/null
    if [[ $? -ne 0 ]]; then
        print "PermitRootLogin ${PREFERRED_SETTING}" >> /etc/ssh/sshd_config
    fi
fi
```

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

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

Default Value:

PermitRootLogin prohibit-password

Additional Information:

The values for this parameter have been **yes** (not recommended), **no** (not recommended, but accepted), **prohibit-password** (recommended setting), **forced-commands-only** (not recommended, but accepted) and **without-password** (deprecated setting).

PermitRootLogin:

Specifies whether root can log in using ssh(1). The argument must be yes, prohibit-password, forced-commands-only, or no. The default is prohibit-password. If this option is set to prohibit-password (or its deprecated alias, without-password), password and keyboard-interactive authentication are disabled for root. If this option is set to forced-commands-only, root login with public key authentication will be allowed, but only if the command option has been specified (which may be useful for taking remote backups even if root login is normally not allowed). All other authentication methods are disabled for root. If this option is set to no, root is not allowed to log in.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

4.6.3.16 Ensure sshd PermitUserEnvironment is disabled

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:

Run the following command:

```
# sshd -T | grep permituserenvironment
```

Verify the output matches:

```
permituserenvironment no
```

Remediation:

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

```
PermitUserEnvironment no
```

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

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

Additional Information:

The AIX implementation of OpenSSH does not make use of **Include** statements by default, so these are not considered within the audit or remediation. If **Include** locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location. The audit will need to be modified to account for the Include location used.

4.6.3.17 Ensure sshd ReKeyLimit is configured

Profile Applicability:

- Level 1

Description:

This variable specifies the maximum amount of data that may be transmitted before the session key is renegotiated, optionally followed by a maximum amount of time that may pass before the session key is renegotiated.

Rationale:

This recommendation is based on the guidelines outlined in Chapter 9 in [RFC4253], i.e. the recommendation is to release/renew Session keys after one hour or after the transfer of one gigabyte (depending on whichever comes first).

Audit:

Run the following command:

```
sshd -T | grep rekeylimit
```

Verify the output matches:

```
rekeylimit 1073741824 3600
```

Remediation:

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

```
RekeyLimit 1G 3600
```

Default Value:

RekeyLimit default None

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			
v7	14.4 <u>Encrypt All Sensitive Information in Transit</u> Encrypt all sensitive information in transit.			

4.6.3.18 Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured

Profile Applicability:

- Level 1

Description:

Note: To clarify, the two settings described below are only meant for idle connections from a protocol perspective and are not meant to check if the user is active or not. An idle user does not mean an idle connection. SSH does not and never had, intentionally, the capability to drop idle users. In SSH versions before 8.2p1 there was a bug that caused these values to behave in such a manner that they were abused to disconnect idle users. This bug has been resolved in 8.2p1 and thus it can no longer be abused to disconnect idle users.

The two options `ClientAliveInterval` and `ClientAliveCountMax` control the timeout of SSH sessions. Taken directly from `man 5 sshd_config`:

- `ClientAliveInterval` Sets a timeout interval in seconds after which if no data has been received from the client, `sshd(8)` will send a message through the encrypted channel to request a response from the client. The default is 0, indicating that these messages will not be sent to the client.
- `ClientAliveCountMax` Sets the number of client alive messages which may be sent without `sshd(8)` receiving any messages back from the client. If this threshold is reached while client alive messages are being sent, `sshd` will disconnect the client, terminating the session. It is important to note that the use of client alive messages is very different from `TCPKeepAlive`. The client alive messages are sent through the encrypted channel and therefore will not be spoofable. The `TCP keepalive` option enabled by `TCPKeepAlive` is spoofable. The client alive mechanism is valuable when the client or server depend on knowing when a connection has become unresponsive.

The default value is 3. If `ClientAliveInterval` is set to 15, and `ClientAliveCountMax` is left at the default, unresponsive SSH clients will be disconnected after approximately 45 seconds. Setting a zero `ClientAliveCountMax` disables connection termination.

Rationale:

In order to prevent resource exhaustion, appropriate values should be set for both **ClientAliveInterval** and **ClientAliveCountMax**. Specifically, looking at the source code, **ClientAliveCountMax** must be greater than zero in order to utilize the ability of SSH to drop idle connections. If connections are allowed to stay open indefinitely, this can potentially be used as a DDOS attack or simple resource exhaustion could occur over unreliable networks.

The example set here is a 45 second timeout. Consult your site policy for network timeouts and apply as appropriate.

Audit:

Run the following command and verify **ClientAliveInterval** and **ClientAliveCountMax** are greater than zero:

```
# /usr/sbin/sshd -T | /usr/bin/egrep -i  
'(clientaliveinterval|clientalivecountmax) '
```

Example Output:

```
clientaliveinterval 15  
clientalivecountmax 3
```

- **IF - Match** set statements are used in your environment, specify the connection parameters to use for the **-T** extended test mode and run the audit to verify the setting is not incorrectly configured in a match block

*Example additional audit needed for a match block for the user **sshuser**:*

```
# /usr/sbin/sshd -T -C user=sshuser | /usr/bin/egrep -i  
'(clientaliveinterval|clientalivecountmax) '
```

Note: If provided, any Match directives in the configuration file that would apply are applied before the configuration is written to standard output. The connection parameters are supplied as keyword=value pairs and may be supplied in any order, either with multiple **-C** options or as a comma-separated list. The keywords are **addr** (source address), **user** (user), **host** (resolved source host name), **laddr** (local address), **lport** (local port number), and **rdomain** (routing domain).

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the `ClientAliveInterval` and `ClientAliveCountMax` parameters above any `Include` and `Match` entries according to site policy.

Example:

```
ClientAliveInterval 15
ClientAliveCountMax 3
```

Note: First occurrence of a option takes precedence, Match set statements withstanding. If Include locations are enabled, used, and order of precedence is understood in your environment, the entry may be created in a file in Include location.

Default Value:

`ClientAliveInterval` 0

`ClientAliveCountMax` 3

References:

1. NIST SP 800-53 Rev. 5: CM-1, CM-2, CM-6, CM-7, IA-5

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.6.4 Configure Sendmail

The base recommendation is to not run **sendmail** on any server not specifically configured and hardened as a MTA (mail transfer agent).

The basic exception - *for a not specifically MTA hardened servers* is to permit MSP (mail submission program) via **localhost** (127.0.0.1).

DRAFT

4.6.4.1 Ensure sendmail version information is hidden

Profile Applicability:

- Level 1

Description:

The recommendation is to change both the default **sendmail** greeting and HELP output to not display the **sendmail** version.

Rationale:

The **sendmail** daemon has a history of security vulnerabilities. The recommendation is to change the default **sendmail** settings that display the **sendmail** version and other related information. Sendmail version information can be used by an attacker for fingerprinting purposes.

Audit:

- Validate the configuration of the software:
 - The command should **NOT** yield: **0 SmtgGreetingMessage=\$j Sendmail \$b**
 - **Note:** No output is also an error.

```
/usr/bin/egrep -i "^O SmtgGreetingMessage" /etc/mail/sendmail.cf
```

- Verify a sendmail helpfile exists:

```
test -e /etc/mail/helpfile || echo "Sendmail HELP file is missing"
```

Remediation:

Create a backup copy of `/etc/mail/sendmail.cf`:

```
cp -p /etc/mail/sendmail.cf /etc/mail/sendmail.cf.pre_cis
```

Edit:

```
vi /etc/mail/sendmail.cf
```

Replace:

```
O SmtgGreetingMessage=$j Sendmail $b
```

With:

```
O SmtgGreetingMessage=mailerready
```

- Ensure Sendmail helpfile exists

```
test -e /etc/mail/helpfile || touch /etc/mail/helpfile
```

Default Value:

`SmtgGreetingMessage=$j Sendmail $b`

Additional Information:

Reversion:

Copy back the original `/etc/sendmail.cf` file:

```
cp -p /etc/mail/sendmail.cf.pre_cis /etc/mail/sendmail.cf
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.6.4.2 Ensure sendmail PrivacyOptions is configured

Profile Applicability:

- Level 1

Description:

The recommendation is to ensure that PrivacyOptions includes at least three settings:

- authwarnings (a default)
- novrfy
- noexpn

Rationale:

The **sendmail** daemon has a history of security vulnerabilities. The recommendation is to modify default **sendmail** settings that otherwise may provide information that can be used by an attacker.

- novrfy: No Verify: do not verify valid email addresses. This can be used by attackers, e.g., phishing attacks.
- noexpn: no expansion: do not verify/expand email list addresses - providing attackers with a list of valid email addresses.

Audit:

- Validate the configuration of the software:

```
popt=$(/usr/bin/egrep -i "^O PrivacyOptions" /etc/mail/sendmail.cf)
for option in authwarnings novrfy noexpn; do
echo ${popt} | /usr/bin/grep -i ${option} >/dev/null && continue
echo Missing sendmail PrivacyOption: $option
done
```

Remediation:

Edit the **/etc/mail/sendmail.cf** file and add any missing options to the **O PrivacyOptions** directive.

Example

```
O PrivacyOptions=authwarnings noexpn novrfy
```

NOTE: **sendmail.cf** supports the use of both the comma and space characters to separate the options.

Default Value:

PrivacyOptions=authwarnings noexpn novrfy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

DRAFT

4.6.4.3 Ensure access to /etc/mail/sendmail.cf is configured

Profile Applicability:

- Level 1

Description:

The access controls for `/etc/mail/sendmail.cf` are applied.

Rationale:

The `/etc/mail/sendmail.cf` file is used by the `sendmail` daemon to determine its default configuration. This file must be protected from unauthorized access and modifications.

Audit:

From the command prompt, execute the following command:

```
ls -l /etc/mail/sendmail.cf | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

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

Remediation:

Set the recommended permissions and ownership on `/etc/mail/sendmail.cf`:

```
chmod u=rw,g=r,o= /etc/mail/sendmail.cf
chown root.system /etc/mail/sendmail.cf
trustchk -u /etc/mail/sendmail.cf mode owner group
```

Default Value:

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


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.			

4.6.4.4 Ensure access to /var/spool/clientmqueue is configured

Profile Applicability:

- Level 1

Description:

The recommended DAC (discretionary access control) settings for the `/var/spool/clientmqueue` directory are applied.

Rationale:

Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access. The clientmqueue (`/var/spool/clientmqueue`) is the mail queue for handling locally generated outbound emails. This queue is used when mail is submitted to `sendmail` as an **MSP** rather than as an **MTA**.

Note: It is possible to specify an alternate spool directory in the `/etc/mail/submit.cf` file via the `QueueDirectory` parameter. When this is used **that** directory name needs identical DAC settings.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
drwxrwx--- smmsp smmsp /var/spool/clientmqueue
```

Remediation:

Set the recommended permissions and ownership on `/var/spool/mqueue`:

```
chmod ug=rwx,o= /var/spool/clientmqueue  
chown smmsp.smmsp /var/spool/clientmqueue
```

Default Value:

```
drwxrwx--- smmsp smmsp /var/spool/clientmqueue
```

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.			

4.6.4.5 Ensure access to /var/spool/mqueue is configured

Profile Applicability:

- Level 1

Description:

The recommended DAC (discretionary access control) settings for the `/var/spool/mqueue` directory are applied.

Rationale:

The `sendmail` daemon stores its queued mail in the `/var/spool/mqueue` directory. Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access.

NOTE: It is possible to specify an alternate spool directory in the `/etc/mail/sendmail.cf` file via the `QueueDirectory` parameter. When this is used **that** directory name needs identical DAC settings.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
drwx----- root system /var/spool/mqueue
```

Remediation:

Set the recommended permissions and ownership on `/var/spool/mqueue`:

```
chmod u=rwx,go= /var/spool/mqueue
chown root /var/spool/mqueue
```

Default Value:

```
drwxrwx--- root system /var/spool/mqueue
```

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.			

4.7 Configure Login Controls

The files `/etc/security/login.cfg` and `/etc/security/user` manages several settings for managing the login process.

The related CIS controls include: [4.3 Configure Automatic Session Locking on Enterprise Assets](#) and [4.10 Enforce Automatic Device Lockout on Portable End-User Devices](#)

DRAFT

4.7.1 Ensure herald is configured

Profile Applicability:

- Level 1

Description:

The contents of the **herald** are displayed to users prior to login for local terminals.

Rationale:

Warning messages inform users who are attempting to login to the system of their legal status regarding the system and should include the name of the organization that owns the system and any monitoring policies that are in place.

Displaying OS and patch level information in login banners is highly discouraged because this provides detailed system information to attackers attempting to target specific exploits of a system.

Authorized users can easily get this information once they have logged in.

Audit:

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

```
lssec -f /etc/security/login.cfg -s default -a herald | read stanza herald  
print ${herald}
```

Example output:

```
herald="Authorized users only. All activity may be monitored and  
reported.\nlogin: "
```

Remediation:

Add a default login herald to **/etc/security/login.cfg** with the appropriate contents according to your site policy:

```
chsec -f /etc/security/login.cfg -s default -a herald="Authorized users only.  
All activity may be monitored and reported.\nlogin: "
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

DRAFT

4.7.2 Ensure logindelay is configured

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.7.3 Ensure loginretries is configured

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.			

4.7.4 Ensure logintimeout is configured

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	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.7.5 Ensure TMOUT is configured

Profile Applicability:

- Level 1

Description:

TMOUT and **TIMEOUT** are environmental settings 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 its 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.

Audit:

Execute the following command:

```
export | /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
- verify `export` statement is the last statement

```
/usr/bin/egrep -e "TMOUT|TIMEOUT" /etc/profile
```

This should return something similar to:

```
TMOUT=900
TIMEOUT=900
export TMOUT TIMEOUT
```

If either setting is missing, and/or the export statement, add these to `/etc/profile`.

Default Value:

`TMOUT=0`

References:

1. <https://www.ibm.com/docs/en/aix/7.2.0?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.			

4.7.6 Unattended terminal session timeout is 900 seconds (or less) - readonly

Profile Applicability:

- Level 2

Description:

TMOUT and **TIMEOUT** are environmental settings 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 its 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 duplicates a recommendation with the addition that the variables are set to **readonly** (rather than **export**). And the recommendation level is set to level 2.

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` and `TIMEOUT` are configured to:

- include a timeout of no more than `900` seconds
- to be `readonly`
- verify `readonly` statement is the last statement

```
/usr/bin/egrep -e "TMOUT|TIMEOUT" /etc/profile
```

This should return something similar to:

```
# TMOUT=120
TMOUT=900
TIMEOUT=900
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.			

4.8 Verify Integrity of Installation Settings

During installation a number of critical variables such as PATH as access to root user are configured. The following recommendations are to verify that these settings have not changed.

DRAFT

4.8.1 Ensure root access is controlled

Profile Applicability:

- Level 1

Description:

Restricts access to root via **su** to members of a specific group. Direct login via console and/or remote login via **telnet** is blocked.

Rationale:

- For accountability, no direct access to root is allowed.
- The attributes here control access to root for programs other than OpenSSH.
- Setting the **sugroups** attribute to **SUADMIN** ensures that only members of the this group are able to **su** root. This makes it more difficult for an attacker to use a stolen root password as the attacker first has to get access to a system user ID.
- Access via a *console* (e.g., /dev/vty0 or /dev/tty0) is only permitted when there are external controls managing accountability of access to the console. For example, HMC access must not be via the account **hscroot**; a physical console is accessible only after a hard-copy log has been entered and verified before physical access is granted to the (data center) console terminal.
- The group **system** is not recommended as it is not uncommon for other accounts to be included in this OS-provided group (gid==0).

Impact:

- When scoring - the attribute **login** may be true as long as access to the HMC is not via the account name **hscroot**.
- In any case, sugroups should not equal **ALL**.

Audit:

- From the command prompt, execute the following commands:

```
#!/usr/bin/ksh -e
lsuser -a login rlogin su sugroups root | tr '=' ' ' | read user a1 login a2
rlogin a3 su a4 sugroups
[[ ${su} != "false" && ${sugroups} == "ALL" ]] && print $0 failed :
${a3}==${su}, ${a4}==${sugroups}
[[ ${login} == "true" || ${rlogin} == "true" ]] && print $0 failed :
${a1}==${login}, ${a2}==${rlogin}

- No output should be returned
```

Remediation:

In `/etc/security/user`, set the root stanza `sugroups` attribute to `SUADMIN` and ensure the `login` and `rlogin` attributes are set to `false`:

```
lsgroup SUADMIN >/dev/null || mkgroup -a SUADMIN
chuser login=false rlogin=false sugroups=SUADMIN root
```

- **NOTE:** For the remediation the setting of `su` is irrelevant.

Default Value:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v8	<u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	<u>4.1 Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.8.2 Ensure root user default shell is ksh

Profile Applicability:

- Level 1

Description:

Ensure that the shell for the root user is set to `/usr/bin/ksh`

Rationale:

Although the bash shell is available there are administrative processes that require the root user to be configured with the `ksh` shell as its default shell. If the root user is configured with a different default shell, these processes will not work as expected.

Audit:

Execute the following command

```
lsuser -a shell root
```

The output should match

```
root shell=/usr/bin/ksh
```

Remediation:

Execute the following command

```
chuser shell=/usr/bin/ksh root
```

Default Value:

`/usr/bin/ksh`

4.8.3 Ensure core dumps are disabled

Profile Applicability:

- Level 1

Description:

This change disables core dumps in the default user stanza of `/etc/security/limits` and also ensures the `fullcore` kernel parameter is set to false.

Rationale:

The creation of core dumps can reveal pertinent system information, potentially even passwords, within the core file. The ability to create a core dump is also a vulnerability to be exploited by a hacker.

The commands below disable core dumps by default, but they may be specifically enabled for a particular user in `/etc/security/limits`.

Audit:

From the command prompt, execute the following command to validate the `/etc/security/limits` changes:

```
lssec -f /etc/security/limits -s default -a core -a core_hard
```

The above command should yield the following output:

```
default core=0 core_hard=0
```

Ensure that the `fullcore` kernel parameter has been set to false:

```
lsattr -El sys0 -a fullcore
```

The above command should yield the following output:

```
fullcore false Enable full CORE dump True
```

Remediation:

Change the default user stanza attributes `core` and `core_hard` in `/etc/security/limits` and then set the `fullcore` kernel parameter to false:

```
chsec -f /etc/security/limits -s default -a core=0 -a core_hard=0  
chdev -l sys0 -a fullcore=false
```

Default Value:

Core dumps enabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<u>5.1 Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

4.8.4 Ensure default path does not include current working directory

Profile Applicability:

- Level 1

Description:

This change removes any "." or ":" entries from `/etc/environment`. If a "." or ":" is present the current working directory is included in the default search path.

Rationale:

Any "." and ":" will be removed from `/etc/environment`. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Examine PATH in `/etc/environment` to see if it contains any "." or ":" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine PATH in `/etc/environment` to see if it contains any "." or ":" entries:

```
grep "^PATH=" /etc/environment |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[\t]*:)|(^.:)|(:.$)|(:.:))/'
```

If the command above yields output, remove the "." and ":" entries from:

```
vi /etc/environment
```

Default Value:

Dot present

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.8.5 Ensure root user path does not include current working directory

Profile Applicability:

- Level 1

Description:

This change removes any "." or ":" entries from the root PATH. If a "." or ":" is present the current working directory is included in the search path.

Rationale:

Any "." and ":" will be removed from the root PATH. This means that any harmful programs placed in common PATH locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Audit:

Ensure that root's PATH does not contain any "." or ":" entries:

```
su - root -c 'echo ${PATH}' |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[ \t]*:)|(^.:)|(:.$)|(:.:))/'
```

The above command should yield no output.

Remediation:

Examine root's PATH to see if it contains any "." or ":" entries:

```
su - root -c 'echo ${PATH}' |awk '/((:[ \t]*:)|(:[ \t]*$)|(^[ \t]*:)|(^.:)|(:.$)|(:.:))/'
```

If the command above yields output, remove the "." and ":" entries from the relevant initialization files. The files to examine are dependant on the root users shell definition in **/etc/passwd**. Once the file or files have been identified remove the "." and ":" from the PATH variable

```
vi <filename>
```

Default Value:

Dot not present

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

DRAFT

4.8.6 Ensure motd is configured

Profile Applicability:

- Level 1

Description:

Create a `/etc/motd` file which displays, post initial logon, a statutory warning message.

Rationale:

The creation of a `/etc/motd` file which contains a statutory warning message could aid in the prosecution of offenders guilty of unauthorized system access. The `/etc/motd` is displayed after successful logins from the console, SSH and other system access protocols.

Audit:

Log back into the system via SSH:

```
ssh localhost
```

NOTE: The `/etc/motd` file will now be displayed

Validate that `/etc/motd` is not writable by group or other

```
ls -l /etc/motd
```

Remediation:

Create a `/etc/motd` file:

```
touch /etc/motd
chmod u=rw,go=r /etc/motd
chown bin:bin /etc/motd
```

Below is a sample banner:

```
*****
NOTICE TO USERS
This computer system is the private property of its owner, whether
individual, corporate or government. It is for authorized use only. Users
(authorized or unauthorized) have no explicit or implicit expectation of
privacy. Any or all uses of this system and all files on this system may be
intercepted, monitored, recorded, copied, audited, inspected, and disclosed
to your employer, to authorized site, government, and law enforcement
personnel, as well as authorized officials of government agencies, both
domestic and foreign. By using this system, the user consents to such
interception, monitoring, recording, copying, auditing, inspection, and
disclosure at the discretion of such personnel or officials. Unauthorized or
improper use of this system may result in civil and criminal penalties and
administrative or disciplinary action, as appropriate. By continuing to use
this system you indicate your awareness of and consent to these terms and
conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this warning.
*****
```

NOTE: Replace "its owner" with the relevant company name

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

4.9 Configure Memory Options

DRAFT

4.9.1 Ensure Address space layout randomization is enabled

Profile Applicability:

- Level 1

Description:

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

Rationale:

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

Audit:

Run the following command to obtain a list of the current ASLR tunable values:

```
# /usr/sbin/vmo -aF | grep aslr
```

Verify output is:

```
aslr = 2
aslr32 = "0"
aslr64 = "0"
aslr32r = 333
aslr64r = 33333
aslr_r = 0
```

Remediation:

Run the following command to enable ASLR for all programs:

```
# /usr/sbin/vmo -r -o aslr=2 -o aslr32=0 -o aslr32r=333 -o aslr64=0 -o
aslr64r=33333 -o aslr_r=0
```

A reboot is required before this change takes effect.

Default Value:

```
aslr=0
aslr32=1
aslr64=1
aslr32r=0
aslr64r=0
aslr_r=0
```

Additional Information:

For the global **aslr** tunable:

0: ASLR is disabled or controlled by a restricted tunable.

1: Randomization is used for shared library areas.

2: Randomization is used for shared library areas and for marked programs.

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.			

5 Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

See [CIS Controls v8: Section 5: Account Management](#)

Implementation Group 1 Recommendations (IG1)

The relevant CIS Controls are:

5.1 Establish and Maintain an Inventory of Accounts (Function: Identify)
5.2 Use Unique Passwords (Function: Protect)
5.3 Disable Dormant Accounts (Function: Respond)
5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts (Function: Protect)
5.5 Establish and Maintain an Inventory of Service Accounts (IG1, Function Identify)

Implementation Group 2 Recommendations (IG2)

The remainder of this section focuses on possible changes to the above recommendations that may be needed when multi-user access is 5.5 Establish and Maintain an Inventory of Service Accounts (IG2, Function Identify) 5.6 Centralize Account Management (Function: Protect)

IG1 and AIX Recommendations

The recommendations included in first sub-sections of the chapter are organized following the sub-sections of CIS (v8) Control 5: Account Management.

These recommendation address controls that manage **local** accounts, not accounts managed by an external service (e.g., LDAP).

Note: The **root** account (euid == 0) should never be managed by an external instance.

What is a System Account?

We define OS standard accounts (e.g., bin, daemon, sshd) as system accounts and these should be managed (and locked/disabled) via local controls. The other characteristic that is used to identify an account as *system* account is a) attribute **admin** is set to true; b) both attributes **login** and **rlogin** are set to false. System administrators are expected to have the attribute **login** set to true so that they could, if needed, login to the AIX console.

Basically, *system* accounts should be managed locally - and, with some exceptions - be (b)locked from command line access.

What is a *Regular Account*?

Classically, a *regular* account is any account that does not own application or service data and login to a command-line shell or menu application is expected. Userid (Account Name) and Password are the principle Security Identification and Authentication mechanisms used to validate and grant access to the system. In this sense a system administrator account is seen as a *regular* account. Also, on a multi-user system - any account not an application (data) owner nor a system administrator should be a regular account.

Regular accounts may, perhaps should, be managed by an external service. Ideally, this external service is also aware of the AIX user and group extended attributes.

DRAFT

5.1 Configure local accounts

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

CIS Control Description

"5.1 Establish and Maintain an Inventory of Accounts"

Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule, at a minimum quarterly, or more frequently.

Rationale

The recommendations here are focused on a system level rather than *enterprise*.

The controls mention both **user** and **administrator** accounts. For the purpose of this benchmark, an account is **administrator** when the AIX user attribute **admin** is **true**.

Additionally, the benchmark looks also at an inventory of **administrative** groups. Groups are defined as **administrator** when the AIX group attribute **admin** is **true**.

Note: The general recommendation to review **all** accounts every 13 weeks (or more frequently).

Including **password controls** (see sub-section for Unique Passwords) AIX has approximately 65 user attributes. These attributes include **ulimits**, **umask**, **rlogin** and more.

The recommendations in this section focus on the password related parameters specified in the **default:** user stanza in the file **/etc/security/user**. The values set are applicable if specific values are not defined in a **username:** stanza.

The recommended procedure for user or account management is to not set any of these attributes explicitly (i.e., in a user stanza in **/etc/security/user** unless there is a specific requirement to override setting in **default:** stanza. The exception is the account **root**. For the **root:** stanza specific recommendations will be made regarding the root (aka superuser) account.

The root account should always be locally managed.

User Management and External Services

When **user access credentials** are managed using an external service many, if not all, of the password related parameters may be managed by the external service. As to **other** attributes, when the external service does not support other AIX user attributes (e.g., LDAP and scheme **rfc2307** (or better, **not rfc2307aix**) **other** user attributes **not** managed by the LDAP server will be assigned from the **default: stanza** of the following files: **/etc/security/envIRON**, **/etc/security/limits**, **/etc/security/roles**, **/etc/security/user**, **/etc/security/user.roles**.

For local users (e.g. **root**) these attributes retain their importance. Remember, generally, only a small subset of the attributes are superseded by external authentication services.

DRAFT

5.1.1 Ensure all local user accounts have a hashed password

Profile Applicability:

- Level 1

Description:

All (unlocked) accounts on the server must have a password.

For this recommendation we look at the so-called **files** registry - as we cannot reliably review the entries kept in a centralized authentication system such as **LDAP** or **Kerberos**.

Rationale:

An account password is a secret code word that must be entered to gain access to the account. If an account exists that has a blank password, multiple users may access the account without authentication and leave a weak audit trail. An attacker may gain unauthorized system access or perform malicious actions, which then cannot be attributed to any specific individual.

Impact:

If no password hash is available and a locked account gets unlocked then the account is available without any verification aka authentication.

Audit:

Run the command:

```
/usr/bin/egrep -p "password = +$" /etc/security/passwd | grep ":" | awk -F: '{ print $1 } ' | \
while read user rest; do
    print "Account ${user} has a blank password in /etc/security/passwd"
done
```

- The command should not yield output.

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.

```
for user in $(/usr/bin/egrep -p "password = +$" /etc/security/passwd | awk
'/:/ {print $1;}')
do
    print "Locking account ${user} due to missing password"
    chuser account_locked='true' expires=0101000070 ${user}
    echo "$user:*" | chpasswd -e -f ADMCHG
done
```

Default Value:

N/A

CIS Controls:

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

5.1.2 Ensure usernames and UIDs are unique

Profile Applicability:

- Level 1

Description:

All users should have a unique UID. In particular the only user on the system to have a UID of 0 should be the root user. Likewise, usernames need to be verified as unique.

Rationale:

The only user with a UID of 0 on the system must be the **root** account. Any account (username) with a UID of 0 has super user privileges on the system and becomes root at login.

Access to the root account should be via **su**, **sudo** or PKI fingerprint. Logging must include sufficient information such that each action taken with root authority can be accounted to a specific account.

All accounts (or users) must have a unique UID to ensure that file and directory security is not compromised.

Impact:

Identification is the basis of Access Control. What you can access is determined by who you are (**uid**), OR by a group you belong to (resource **GID** and your group list) **OR** access is permitted to all (i.e., your **UID** and group list) do not match the resource **UID** and **GID** values.

Audit:

Run the commands:

```
cut -d: -f 3 /etc/passwd | sort -n | uniq -d  
cut -d: -f 1 /etc/passwd | sort      | uniq -d
```

The commands should not yield output

Remediation:

- Examine the user IDs of all configured accounts:

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

If a number, or numbers are returned from the command above, these are UID values which are not unique within the `/etc/passwd` file. Determine the effected accounts/s:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d | while read UID; do
  cut -f "1 3" -d : /etc/passwd | grep ":${UID}"
done
```

- Examine the usernames IDs of all configured accounts:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d
```

If a username, or usernames are returned from the command above, these are username values which are not unique within the `/etc/passwd` file. Determine the effected accounts/s:

```
cut -d: -f 1 /etc/passwd | sort -n | uniq -d | while read username; do
  cut -f "1 3" -d : /etc/passwd | grep "${username}:"
done
```

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

To remove:

```
rmuser <username>
```

To change the UID:

```
chuser id=<id> <username>
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			
v7	0.0 <u>Explicitly Not Mapped</u> Explicitly Not Mapped			

5.1.3 Ensure group names and GIDs are unique

Profile Applicability:

- Level 1

Description:

All groups should have a unique GID on the system.

Rationale:

All groups should have an individual and unique GID. If GID numbers are shared this could lead to undesirable file and directory access.

Audit:

Run the commands:

```
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 2 | sort -n | uniq -d  
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 1 | sort | uniq -d
```

The commands should not yield output

Remediation:

- Examine the *group IDs* (GID) of all locally configured accounts:

```
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 2 | sort -n | uniq -d
```

If the command has output there is at least one duplicate GID number. Determine any duplicates within the */etc/group* file:

```
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 2 | sort -n | uniq -d |  
while read GID; do  
    cut -f "1 3 4" -d : /etc/group | /usr/bin/sort -t: -k2n | grep ":{GID}:"  
done
```

- Examine the *names* of all locally configured groups:

```
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 1 | sort | uniq -d
```

If the command has output there is at least one duplicate group name. Determine any duplicates within the */etc/group* file:

```
cut -d: -f "1 3" /etc/group | sort -u | cut -d: -f 1 | sort | uniq -d | while  
read groupname; do  
    cut -f "1 3 4" -d : /etc/group | /usr/bin/sort -t: -k2n | grep  
"${groupname}:"  
done
```

NOTE: Any duplicates returned should either be deleted or have the GID changed. Be careful. We recommend you examine any accounts assigned to a duplicate and ensure the account is neither losing nor gaining authorized group access through any remedial action.

To remove:

```
rmgroup <groupname>
```

To change the GID:

```
chgroup id=<id> <groupname>
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			
v7	16.6 <u>Maintain an Inventory of Accounts</u> Maintain an inventory of all accounts organized by authentication system.			

5.1.4 Ensure an Inventory of Administrator accounts is established and maintained

Profile Applicability:

- Level 1

Description:

AIX defines *Administrator* accounts with the attribute *admin*. When *true* the account is **Administrator** and when *false* the account is considered **User**.

Rationale:

An inventory of accounts with the attribute "*admin=true*" allows verification that all accounts considered *administrative* are so labeled by the system.

Impact:

The impact of '*admin=true*' is two-fold. a) a label for identifying accounts considered related to system administration b) providing additional controls for account management. On AIX, an account with the attribute '*admin=true*' requires a security role of *Senior Security Admin* to make modifications to the account attributes.

Audit:

Verify that there is, off system, an inventory of Administrative accounts and that the date is not more 13 weeks old.

Remediation:

A printable report can be prepared using the following example:

```
cnt=0
printf "%4s%68s\n" "AIX" "Administator Accounts"

lsuser -R files -a admin ALL | while read usr adm; do
if [[ ${adm} = "admin=true" ]] ; then
    printf "%12s" ${usr}
    let cnt=cnt+1
    [[ $(expr ${cnt} % 6) == 0 ]] && print
fi
done
[[ $(expr ${cnt} % 6) != 0 ]] && print
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.5 <u>Establish and Maintain an Inventory of Service Accounts</u> Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.		●	●
v7	4.1 <u>Maintain Inventory of Administrative Accounts</u> Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

5.1.5 Ensure an Inventory of user accounts is established and maintained

Profile Applicability:

- Level 1

Description:

AIX defines *Administrator* accounts with the attribute *admin*. When *true* the account is **Administrator** and when *false* the account is considered **User**.

Rationale:

An inventory of accounts with the attribute "*admin=true*" allows verification that all accounts considered *administrative* are so labeled by the system.

Impact:

The impact of '*admin=true*' is two-fold. a) a label for identifying accounts considered related to system administration b) providing additional controls for account management. On AIX, an account with the attribute '*admin=true*' requires a security role of *Senior Security Admin* to make modifications to the account attributes.

Audit:

Verify that there is, off system, an inventory of User (not Administrative) accounts and that the date is not more 13 weeks old.

Remediation:

A printable report can be prepared using the following example:

```
cnt=0
printf "%4s%68s\n" "AIX" "User Accounts"

lsuser -R files -a admin ALL | while read usr adm; do
if [[ ${adm} = "admin=false" ]] ; then
    printf "%12s" ${usr}
    let cnt=cnt+1
    [[ $(expr ${cnt} % 6) == 0 ]] && print
fi
done
[[ $(expr ${cnt} % 6) != 0 ]] && print
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 <u>Establish and Maintain an Inventory of Accounts</u> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.			

5.1.6 Ensure all local user accounts have valid stanzas in /etc/security/passwd

Profile Applicability:

- Level 1

Description:

AIX uses two files to store information about local user accounts, the traditional `/etc/passwd` and also `/etc/security/passwd`. This latter file stores hashed passwords and metadata about the user account such as the last password change and whether the account is permitted to login.

Rationale:

If an account exists that does not have a valid stanza in `/etc/security/passwd` then it is possible that under certain combinations of circumstances this is equivalent to that account having a blank password and thus 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.

Audit:

Run the following command to verify that local user accounts have valid entries:

```
pwdck -n ALL
```

No output should be returned

Remediation:

Run the one of the following commands to remediate the identified issues:

```
pwdck -t ALL
```

-- OR --

```
pwdck -y ALL
```

Note: Running the command with the `-t` flag will provide information about each action and prompt you to approve, whilst running it with the `-y` flag will automatically fix all errors and report the changes.

References:

1. STIG ID: AIX7-00-001038 | SV-215197r991591 | CAT I

CIS Controls:

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

5.2 Password Management and Controls

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

Password policy attributes for password uniqueness include minimum length, reuse, and complexity.

AIX has nine individual *password attributes* that can be *tuned*. For each attribute a recommendation is expected. Nine (9) sounds like a lot of unique recommendations but you could also see the attributes as are 5 core attributes - and of these five, four have a min/max setting.

Defining policy based on nine recommendations, even with passwords of 14 characters. can complicate defining sufficient, yet usable password requirements. In other words define statements that provide sufficient protection from abuse yet give users some freedom of choice in creating strong, yet rememberable, passwords.

Remember: password attributes are not policy statements. They are the *knobs* that can be turned to implement a policy specification.

The challenge faced: which combination of attributes will satisfy a set of minimum requirements: *password length*, *number of different characters (including/excluding case)* each per characteristic: alpha, numeric, and other (so-called special).

Historically the core requirements has been based on setting minimums, e.g.,: *minlen*, *mindiff*, *maxrepeats*, *minalpha*, and *minother*. More recently additional *knobs* have been added to add further specification the characters *alpha* and *other*: *mindigit*, *minloweralpha*, *minupperalpha* and *minspecialchar*. This expansion was added in AIX 7.1 TL0 (and AIX 6.1 TL8). Remember: Historical recommendations are for the *core* attributes: **minlen**, **mindiff**, **maxrepeats**, **minalpha**, **minother**.

The four new attributes, according to the on-line manual - depend on, read modify, the historical attributes when certain conditions are met.

- Rules for Alphabetic Characters (**minalpha**)
 - If **minloweralpha** > **minalpha** then **minloweralpha=minalpha**
 - If **minupperalpha** > **minalpha** then **minupperalpha=minalpha**
 - If **minloweralpha + minupperalpha** > **minalpha**; then **minupperalpha=minalpha - minloweralpha**
- Rules for Non-Alphabetic Characters (**minother**)
 - If **mindigit** > **minother** then **mindigit=minother**
 - If **minspecialchar** > **minother** then **minspecialchar=minother**
 - If **minspecialchar + mindigit** > **minother** then **minspecialchar = minother - mindigit**

In effect this means **minalpha** and **minother** are still the leading attributes - but can be *fine-tuned*. **IMPORTANT:** to get your desired effect ensure **minalpha** >= **minloweralpha + minupperalpha**, and **minother** >= **mindigit + minspecialchar**.

5.2.1 Ensure *histsize* is configured

Profile Applicability:

- Level 1

Description:

Defines the number of previous passwords that a user may not reuse.

Rationale:

In setting the **histsize** attribute, it enforces a minimum number of previous passwords a user cannot reuse.

Impact:

The recommendation is to not use this attribute. This attribute was traditionally used together with *minage* to prevent rapid reuse of old passwords. Instead "Unique Passwords" relies solely on the time-based *histexpire* attribute.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default histsize=0
```

Remediation:

In **/etc/security/user**, set the default user stanza **histsize** attribute to be **0**:

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

This means that this setting is not being used for password management.

Default Value:

Disabled

CIS Controls:

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

5.2.2 *Ensure minimum password age is configured*

Profile Applicability:

- Level 2

Description:

The minimum password age determines the number of weeks that you must use a password before you can change it.

Rationale:

Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old, potentially compromised passwords, may cause a security breach. By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls

Impact:

By enforcing a minimum password age, a user will be unable to change their password if they observe a potential compromise of their password, e.g. "shoulder surfing", during the time defined by minimum password age. In this event the user should follow local site policy to report a compromised password.

If a users password is set by other personnel as a procedure in dealing with a lost or expired password, the user should be forced to update this "set" password with their own password. e.g. use the **ADMINCHG** flag on the account.

If it is not possible to have a user set their own password immediately, and this recommendation or local site procedure may cause a user to continue using a third party generated password, **minage** for the affected user should be temporally changed to 0, to allow a user to change their password immediately.

For applications where the user is not using the password at console, the ability to "change at next logon" may be limited. This may cause a user to continue to use a password created by other personnel.

The AIX community prefers to rely on the AIX attribute **histexpire** rather than a historical **minage** value as this better satisfies the need to prevent cycling through passwords. The CIS Password Policy still recommends the use of a minimum age, hence the retention of this recommendation at level 2.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minage=1
```

Remediation:

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

```
chsec -f /etc/security/user -s default -a minage=1
```

This means that a user can only change their password after one week.

Default Value:

`minage=0`

References:

1. CIS Password Policy Guide

CIS Controls:

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

5.2.3 Ensure password history expiry is configured

Profile Applicability:

- Level 1

Description:

The history expiry determines the number of weeks that a user will not be able to reuse a password.

Rationale:

Users may have favourite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise.

Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old, potentially compromised passwords, may cause a security breach.

By restricting the time period before a password can be re-used, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default histexpire=52
```

Remediation:

In `/etc/security/user`, set the default user stanza `histexpire` attribute to be greater than or equal to `52`:

```
chsec -f /etc/security/user -s default -a histexpire=52
```

This means that a user will not be able to reuse any password set in the last 52 weeks (one year).

Default Value:

`histexpire=0`

CIS Controls:

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

5.2.4 Ensure passwords are controlled by password attributes

Profile Applicability:

- Level 1

Description:

Ensure passwords are *required* to pass password attribute controls.

Rationale:

If password restrictions are not enforced for some accounts, those accounts represent a much greater risk of being compromised by an attacker as they may have weaker passwords vulnerable to brute force attack or provide an indefinite window of opportunity for the use of already compromised credentials if the same password has been used on multiple systems.

Impact:

When exceptions to the defaults are required - rather than disable all password checking - an account needs to have the attribute redefined *per account*.

SHA512 password encryption is recommended as the most secure.

Audit:

Execute the following command:

```
grep NOCHECK /etc/security/passwd
```

The exit status should be **1** and there should not be any output.

Remediation:

In the file `/etc/security/passwd` clear the **NOCHECK** attribute from all users:

```
#!/usr/bin/ksh -e
# Copyright AIXTools, 2022

/usr/bin/grep -p NOCHECK /etc/security/passwd | /usr/bin/egrep ":@" | sed -e
's/:/' | while read USER; do
    /usr/bin/pwdadm -c $USER
    /usr/bin/pwdadm -f ADMCHG $USER
done
```

CIS Controls:

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

5.2.5 Ensure maxexpired is configured

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 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

5.2.6 *Ensure password expiration is configured*

Profile Applicability:

- Level 1

Description:

The maximum password age attribute (**maxage**) determines the maximum number of weeks that you can use a password before you must change it.

Rationale:

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

We recommend a yearly password change. This is primarily because for all their good intentions users will share credentials across accounts. Therefore, even if a breach is publicly identified, the user may not see this notification, or forget they have an account on that site. This could leave a shared credential vulnerable indefinitely. Having an organizational policy of a 1-year (annual) password expiration is a reasonable compromise to mitigate this with minimal user burden.

Impact:

The password expiration must be greater than the minimum days between password changes or users will be unable to change their password.

Excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. In these cases, the next password can be predicted based on the previous one (incrementing a number used in the password for example). Also, password expiration requirements offer no containment benefits because attackers will often use credentials as soon as they compromise them. Instead, immediate password changes should be based on key events including, but not limited to:

- - o Indication of compromise
- - o Change of user roles
- - o When a user leaves the organization.

Not only does changing passwords every few weeks or months frustrate the user, but it's also been suggested that it does more harm than good, because it could lead to bad practices by the user such as adding a character to the end of their existing password.

Audit:

Run the following command and verify **maxage** is set to 52 weeks or less and conforms to local site policy:

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

Example output:

```
default maxage=52
```

Remediation:

In **/etc/security/user**, set the default user stanza **maxage** attribute to a number greater than **0** but less than or equal to **52** that follows local site policy:

```
chsec -f /etc/security/user -s default -a maxage=52
```

This means that a user password must be changed 52 weeks after being set. If 0 is set then this effectively disables password ageing.

Default Value:

maxage=0

CIS Controls:

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

5.2.7 Ensure `pwd_algorithm` is configured

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/pwdbalg.cfg`. The traditional UNIX password algorithm is `crypt`, which is a one-way hash function supporting only 8 character passwords. The use of brute force password guessing attacks means that `crypt` no longer provides an appropriate level of security and so other encryption mechanisms are recommended.

The recommendation of this benchmark is to set the password algorithm to `ssha512`. This algorithm supports long passwords, up to 255 characters in length and allows passphrases including the use of the extended ASCII table and the space character. Any passwords already set using `crypt` will be recognized. When the password is reset the new password hash algorithm will be used to encrypt the password.

Impact:

A password algorithm other than `crypt` is required to support a password *minlen* greater than 8 (eight) characters.

SHA512 password encryption is recommended as the most secure.

Audit:

Execute the following command:

```
#!/usr/bin/ksh -e
# chk_algorithm:5.2.1
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

EXPECT="usw pwd_algorithm=ssha512"
CMD="lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm"

TST=${${CMD}}
[[ ${TST} == ${EXPECT} ]] && exit 0
print "%0: password hash algorithm is not ssha512"
exit 1
```

Remediation:

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

```
#!/usr/bin/ksh -e
# chk_algorithm:5.2.1
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

EXPECT="usw pwd_algorithm=ssha512"
CMD="lssec -f /etc/security/login.cfg -s usw -a pwd_algorithm"

TST=$( ${CMD} )
[[ ${TST} == ${EXPECT} ]] && exit 0

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

Default Value:

crypt

Additional Information:

- Consider looking for passwords encrypted using `crypt` and set the `ADMCHG` flag to initiate a password change at next login.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.			

5.2.8 Ensure a strong password hashing algorithm is configured

Profile Applicability:

- Level 1

Description:

The recommendation is to change the default password hash algorithm to **ssha512** (see recommendation "Ensure pwd_algorithm is configured"). However, changing the default algorithm away from **crypt** is not enough. The user must supply a new password before a new hashed version of the password is stored in the *shadow* password file **/etc/security/password**.

Rationale:

The hash algorithm **crypt** is known by all *nix versions - so it has provided portability. And in the '70's processor power was weak enough that the mere 56 bits protection against brute-force attacks was reasonable to sufficient. Fifty (50) years later - this is not the case.

Impact:

The audit looks for hashed passwords that are 14 (fourteen) characters long. That is the length of the crypt hash. The remediation neither changes the password nor locks the account. However, it does clear (if present) and password flags (notably **NOCHECK** needs to be removed) and sets the flag **ADMCHG** so that the account will be required to reset their password during the next login.

Audit:

Use the following to find passwords using **crypt** hash method:

```
#!/usr/bin/ksh -e
# hash:5.2.2
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

grep 'password[[:blank:]]= .....$' /etc/security/passwd | \
while read pass equals cryptedhash; do
    user=$(grep -p $cryptedhash /etc/security/passwd | egrep '[a-zA-z0-9]+:$' |
sed -e s/:$//)
    print ${user}: needs to update passwd
done
```

Remediation:

Execute the following command to enable an administrative requirement to update password on next login - when current password is still *hashed* using the **crypt** algorithm.

```
#!/usr/bin/ksh -e
# hash_chk:5.2.12
# Provided to CIS by AIXTools
# Copyright AIXTools, 2022

#SystemAccounts are skipped, root is treated a regular account
#pconsole is no longer a system account - being deprecated/removed
SACTS1="(adm|bin|daemon|invscout|ipsec|lp|lpd|nobody|nuucp|sshd|sys|uucp) "
SACTS2="(esa|srvproxy|imnadm|anonymou|ftp) "
grep 'password[[:blank:]]= .....$' /etc/security/passwd | \
while read pass equals cryptedhash; do
    user=$(/usr/bin/grep -p $cryptedhash /etc/security/passwd | \
        /usr/bin/egrep -vp "${SACTS1}:$" | \
        /usr/bin/egrep -vp "${SACTS2}:$" | \
        /usr/bin/egrep '[a-zA-z0-9]+:~$' | sed -e s/:$//)
    print ${user}: needs to update passwd
    set -x
    /usr/bin/pwdadm -c ${user}
    /usr/bin/pwdadm -f ADMCHG ${user}
    set +x
done
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.			

5.2.9 Ensure minimum password length is configured

Profile Applicability:

- Level 1

Description:

The minimum password length setting determines the lowest number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "passphrase" is a better term than "password".

The **minlen** option sets the minimum acceptable size for the new password.

Rationale:

Strong passwords help protect systems from password attacks. Types of password attacks include dictionary attacks, which attempt to use common words and phrases, and brute force attacks, which try every possible combination of characters. Also, attackers may try to obtain the account database so they can use tools to discover the accounts and passwords.

Impact:

In general, it is true that longer passwords are better (harder to crack), but it is also true that forced password length requirements can cause user behavior that is predictable and undesirable. For example, requiring users to have a minimum 16-character password may cause them to choose repeating patterns like **fourfourfourfour** or **passwordpassword** that meet the requirement but aren't hard to guess. Additionally, length requirements increase the chances that users will adopt other insecure practices, like writing them down, re-using them or storing them unencrypted in their documents.

Having a reasonable minimum length with no maximum character limit increases the resulting average password length used (and therefore the strength).

Audit:

From the command prompt, execute the following command:

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

Example output:

```
default minlen=14
```

Verify returned value is no less than 14 characters and meets local site policy.

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 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.			

5.2.10 Ensure number of characters changed in new password is configured

Profile Applicability:

- Level 1

Description:

The **mindiff** option sets the number of characters in a password that must not be present in the old password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determines how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the command prompt, execute the following command:

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

Example output:

```
default mindiff=6
```

Verify returned value is **6** or more and meets local site policy.

Remediation:

In **/etc/security/user**, set the default user stanza **mindiff** attribute to be greater than or equal to **6**:

```
chsec -f /etc/security/user -s default -a mindiff=6
```

Default Value:

mindiff=0

CIS Controls:

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

5.2.11 Ensure minalpha is configured

Profile Applicability:

- Level 1

Description:

Defines the minimum number of alphabetic characters in a password.

Rationale:

In setting the **minalpha** attribute, it ensures that passwords have a minimum number of alphabetic characters.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minalpha=3
```

Remediation:

In **/etc/security/user**, set the default user stanza **minalpha** attribute to be greater than or equal to **3**:

```
chsec -f /etc/security/user -s default -a minalpha=3
```

This means that there must be at least 3 alphabetic characters (upper or lowercase) within a password.

Default Value:

minalpha=0

CIS Controls:

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

5.2.12 Ensure minother is configured

Profile Applicability:

- Level 1

Description:

Defines the number of characters within a password which must be non-alphabetic.

Rationale:

In setting the **minother** attribute, it increases password complexity by enforcing the use of non-alphabetic characters in every user password.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minother=3
```

Remediation:

In **/etc/security/user**, set the default user stanza **minother** attribute to be greater than or equal to **3**:

```
chsec -f /etc/security/user -s default -a minother=3
```

This means that there must be at least 3 non-alphabetic characters within a password.

Default Value:

default minother=0

CIS Controls:

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

5.2.13 Ensure password maximum repeated characters is configured

Profile Applicability:

- Level 1

Description:

maxrepeats defines the maximum number of times a character may appear in a password.

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Passwords which consist of too many repeated characters have lower complexity and thus are easier to compromise.

Impact:

Setting **maxrepeats** too low can prevent passwords which are sufficiently complex from being accepted. This value has been selected with respect to the recommended value of 14 for **minlen**. If local site policy requires a longer minimum password length, you should review this value.

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 **4**:

```
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.

Default Value:

maxrepeats=8

CIS Controls:

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

5.2.14 Ensure mindigit is configured

Profile Applicability:

- Level 1

Description:

Defines the minimum number of digits in a password.

Rationale:

In setting the **mindigit** attribute, the password must contain a digit when it is changed by the user.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default mindigit=1
```

Remediation:

In **/etc/security/user**, set the default user stanza **mindigit** attribute to **1**:

```
chsec -f /etc/security/user -s default -a mindigit=1
```

This means that there must be at least 1 digit within a password.

Default Value:

default mindigit=0

CIS Controls:

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

5.2.15 Ensure minloweralpha is configured

Profile Applicability:

- Level 1

Description:

Defines the minimum number of lower case alphabetic characters in a password.

Rationale:

In setting the **minloweralpha** attribute, the password must contain a lower case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minloweralpha=1
```

Remediation:

In **/etc/security/user**, set the default user stanza **minloweralpha** attribute to **1**:

```
chsec -f /etc/security/user -s default -a minloweralpha=1
```

This means that there must be at least 1 lower case alphabetic character within a password.

Default Value:

default minloweralpha=0

CIS Controls:

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

5.2.16 Ensure minupperalpha is configured

Profile Applicability:

- Level 1

Description:

Defines the minimum number of upper case alphabetic characters in a password.

Rationale:

In setting the **minupperalpha** attribute, the password must contain an upper case alphabetic character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minupperalpha=1
```

Remediation:

In **/etc/security/user**, set the default user stanza **minupperalpha** attribute to **1**:

```
chsec -f /etc/security/user -s default -a minupperalpha=1
```

This means that there must be at least 1 upper case alphabetic character within a password.

Default Value:

default minupperalpha=0

CIS Controls:

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

5.2.17 Ensure minspecialchar is configured

Profile Applicability:

- Level 1

Description:

Defines the minimum number of special characters in a password.

Rationale:

In setting the **minspecialchar** attribute, the password must contain a special character when it is changed by the user.

Audit:

From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minspecialchar=1
```

Remediation:

In **/etc/security/user**, set the default user stanza **minspecialchar** attribute to **1**:

```
chsec -f /etc/security/user -s default -a minspecialchar=1
```

This means that there must be at least 1 special character within a password.

Default Value:

default minspecialchar=0

CIS Controls:

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

5.3 Configure 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`).
- The list of system accounts in this section is not exhaustive. You should review other system accounts such as those used to run database or application servers and apply the same controls where possible

Motivation:

- There is no reason that these userid's have any access to a shell - whether through a login or `su(do)`.
- There is no need for an encrypted password in the shadow file. Better is to leave the shadow password as the single character `*` as that will never resolve to a normal password - effectively blocking `login` and `su` operations.
- Not even `su` as root needs to succeed.

Exception:

- There should not be a requirement to log in as any of these users directly. However, if a need does arise access should be regulated via the `sudoers` attribute (document the group creation and assignment) so that the legitimate user may `su` from there own account to ensure traceability and accountability. This also implies that a real encrypted (as sha512) password will exist in the shadow password file.

5.3.1 Ensure user adm is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **adm** user account.

Rationale:

This change disables direct local and remote login to the **adm** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **adm** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the **adm** user:

```
lsuser -a account_locked login rlogin adm
```

The above command should yield the following output:

```
adm account_locked=true login=false rlogin=false
```

Remediation:

Change the following user attributes to **adm** user:

```
chuser account_locked=true login=false rlogin=false adm
```

Default Value:

account_locked=false rlogin=true login=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.2 Ensure user bin is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **bin** user account.

Rationale:

This change disables direct local and remote login to the **bin** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **bin** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the **bin** user:

```
lsuser -a account_locked login rlogin bin
```

The above command should yield the following output:

```
bin account_locked=true login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable **bin** user access:

```
chuser account_locked=true login=false rlogin=false bin
```

Default Value:

account_locked=false rlogin=true login=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.3 Ensure user daemon is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **daemon** user account.

Rationale:

This change disables direct local and remote login to the **daemon** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **daemon** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the **daemon** user:

```
lsuser -a account_locked login rlogin daemon
```

The above command should yield the following output:

```
daemon account_locked=true login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable **daemon** user access:

```
chuser account_locked=true login=false rlogin=false daemon
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

5.3.4 Ensure user guest is secured

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 guest
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.5 Ensure user lpd is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **lpd** user account.

Rationale:

This change disables direct local and remote login to the **lpd** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **lpd** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure remote access has been disabled for the **lpd** user:

```
lsuser -a account_locked login rlogin lpd
```

The above command should yield the following output:

```
lpd account_locked=true login=false rlogin=false
```

Remediation:

Change the following user attributes to **lpd** user:

```
chuser account_locked=true login=false rlogin=false lpd
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.6 Ensure user nobody is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **nobody** user account.

Rationale:

This change disables direct local and remote login to the **nobody** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **nobody** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the **nobody** user:

```
lsuser -a account_locked login rlogin nobody
```

The above command should yield the following output:

```
nobody account_locked=true login=false rlogin=false
```

Remediation:

Change the login and remote login user flags to disable **nobody** user access:

```
chuser account_locked=true login=false rlogin=false nobody
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.7 Ensure user nuucp is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **nuucp** user account.

Rationale:

This change disables direct local and remote login to the **nuucp** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **nuucp** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the **nuucp** user:

```
lsuser -a account_locked login rlogin nuucp
```

The above command should yield the following output:

```
nuucp account_locked=true login=false rlogin=false
```

Remediation:

Change the following user attributes to **nuucp** user::

```
chuser account_locked=true login=false rlogin=false nuucp
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.8 Ensure user sys is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **sys** user account.

Rationale:

This change disables direct local and remote login to the **sys** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **sys** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the **sys** user:

```
lsuser -a account_locked login rlogin sys
```

The above command should yield the following output:

```
sys account_locked=true login=false rlogin=false
```

Remediation:

Change the following user attributes to **sys** user:

```
chuser account_locked=true login=false rlogin=false sys
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.9 Ensure user uucp is secured

Profile Applicability:

- Level 1

Description:

This change locks and disables login access for the **uucp** user account.

Rationale:

This change disables direct local and remote login to the **uucp** user account. Do not set a password on this account to ensure that the only access is via **su** from the root account.

There should not be a requirement to log in as the **uucp** user directly. All users should be given unique logon ids to ensure traceability and accountability.

Audit:

Ensure access has been disabled for the **uucp** user:

```
lsuser -a account_locked login rlogin uucp
```

The above command should yield the following output:

```
uucp account_locked=true login=false rlogin=false
```

Remediation:

Change the following user attributes to **uucp** user:

```
chuser account_locked=true login=false rlogin=false uucp
```

Default Value:

account_locked=false login=true rlogin=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.3.10 Ensure System Accounts cannot access system using ftp.

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	4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u> Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.			

5.4 User Attributes for Active Processes

Other attributes manage user/application settings for active processes. These attributes include `ulimits`, `umask`. Including password controls - there are approximately 65 user attributes.

The recommendations in this section focus on the parameters of the default user stanza in the file `/etc/security/user`. The values set are only applicable if specific values are not defined during the creation of a user.

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

DRAFT

5.5 Disable Dormant Accounts

Some attributes that previously were associated with *Unique Passwords* are actually attributes to automate disabling dormant accounts.

The attributes do not control the passwords. Instead they require an active account to create a new password, OR - be considered dormant and disabled. These attributes focus on how long a password is valid, when it should be changed, and disables an account when it not changed.

Other settings here, traditionally, have been characterized as "secure configuration of enterprise assets". We believe they fit better under the heading of automated "Disable Dormant Accounts"

DRAFT

6 Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

See [Control v8: Access Control Management](#)

Why Is This Control Critical?

Where CIS Control 5 (Account Management) deals specifically with account identification, authentication and status (active or dormant), CIS Control 6 (Access Control Management) focuses on managing what access these identities have, ensuring identities (processes or users) only have access to the data or enterprise assets appropriate for their role. Identities should only have the minimal authorization, i.e., access, needed for the role.

Defining roles, developing consistent access rights for each role and assigning roles to users is a best practice. Developing a program for complete provision and de-provisioning access is also important. Centralizing this function is ideal.

Access Control in AIX environment

Most AIX servers are used in a commercial environment and rely on classic UNIX File System DAC (discretionary access control) mechanisms based on the effective UID and list of GID's a process is associated with. Every object a process accesses using system calls `open()`, `read()`, and `write()` (and others) is determined by the UID/GID of the inode and the mode or permission bits associated with it. If the object UID and the EUID are equal then only the permission bits associated with the UID are relevant. If `UID != EUID` and `GID ==` one of the associated GIDs the the group bits are relevant. If neither are true then either the "other" permissions are valid, or an ACL (access control list) may be valid, or an enhanced RBAC setting may permit access. **Note:** a *deny* ACL supersedes file system DAC and/or enhanced RBAC permissions.

6.1 Configure 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).

DRAFT

6.1.1 Ensure sudo is installed

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:

```
# /usr/bin/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 1.9.17p1 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 1.9.17p1 or later.

Default Value:

Not installed

References:

1. NIST SP 800-53 Rev. 5: AC-6(2), AC-6(5)

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.			

6.1.2 Ensure sudo logging is active

Profile Applicability:

- Level 2

Description:

All commands executed via **sudo** should be logged to either syslog (default) or a dedicated log file

Note: visudo edits the sudoers file in a safe fashion, analogous to vipw(8). visudo locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks or parse errors. If the sudoers file is currently being edited you will receive a message to try again later.

Rationale:

Logging of commands executed via **sudo** enables auditing of those commands

Audit:

Verify that **syslog_badpri** and **syslog_goodpri** are not set to **none**

Run the following commands:

```
# /usr/bin/grep -Ei '^s*Defaults\s+syslog_badpri=none' /etc/sudoers
/etc/sudoers.d/*
# /usr/bin/grep -Ei '^s*Defaults\s+syslog_goodpri=none' /etc/sudoers
/etc/sudoers.d/*
```

No output should be returned

-OR-

Verify that sudo has a custom log file configured

Run the following command:

```
# /usr/bin/grep -Ei '^s*Defaults\s+logfile=\S+' /etc/sudoers
/etc/sudoers.d/*
```

Example output:

```
/etc/sudoers:Defaults logfile="/var/log/sudo.log"
```

Remediation:

Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `/usr/sbin/visudo -f <PATH TO FILE>`

Remove any lines which are found containing:

```
Defaults syslog_badpri=none

-OR-

Defaults syslog_goodpri=none
```

-OR-

If you do not want to log sudo commands to syslog, to use as sudo specific log file, edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with `/usr/sbin/visudo -f <PATH TO FILE>`:

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

Example:

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

Default Value:

All options are unset by default

References:

1. NIST SP 800-53 Rev. 5: AU-3, AU-12

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.1.3 Ensure sudo commands use pty

Profile Applicability:

- Level 2

Description:

sudo can be configured to run only from a pseudo terminal (**pseudo-pty**)

Rationale:

Attackers can run a malicious program using **sudo**, which would again fork a background process that remains even when the main program has finished executing.

Impact:

WARNING: Editing the **sudo** configuration incorrectly can cause **sudo** to stop functioning. Always use **visudo** to modify **sudo** configuration files.

Audit:

Verify that sudo can only run other commands from a pseudo-pty

Run the following command to verify **Defaults use_pty** is set:

```
# /usr/bin/grep -Eir  
'^\s*Defaults\s+([\^#]+,\s*)?use_pty(\s+\S+\s*)*(\s+#[.]*)?$\s*' /etc/sudoers*
```

Verify the output matches:

```
/etc/sudoers:Defaults use_pty
```

Run the follow command to to verify **Defaults !use_pty** is not set:

```
# /usr/bin/grep -Eir  
'^\s*Defaults\s+([\^#]+,\s*)?!use_pty(\s+\S+\s*)*(\s+#[.]*)?$\s*' /etc/sudoers*
```

Nothing should be returned

Remediation:

Edit the file **/etc/sudoers** with **visudo** or a file in **/etc/sudoers.d/** with **/usr/sbin/visudo -f <PATH TO FILE>** and add the following line:

```
Defaults use_pty
```

Edit the file **/etc/sudoers** with **visudo** and any files in **/etc/sudoers.d/** with **/usr/sbin/visudo -f <PATH TO FILE>** and and remove any occurrence of **!use_pty**

References:

1. NIST SP 800-53 Rev. 5: AC-6

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.			

6.2 Configure Services Management

Access controls for standard services

DRAFT

6.2.1 Ensure at is restricted to authorized users

Profile Applicability:

- Level 1

Description:

at allows fairly complex time specifications, extending the POSIX.2 standard. It accepts times of the form HH:MM to run a job at a specific time of day. (If that time is already past, the next day is assumed.) You may also specify midnight, noon, or teatime (4pm) and you can have a time-of-day suffixed with AM or PM for running in the morning or the evening. You can also say what day the job will be run, by giving a date in the form month-name day with an optional year, or giving a date of the form MMDD[CC]YY, MM/DD/[CC]YY, DD.MM.[CC]YY or [CC]YY-MM-DD. The specification of a date must follow the specification of the time of day. You can also give times like now + count time-units, where the time-units can be minutes, hours, days, or weeks and you can tell at to run the job today by suffixing the time with today and to run the job tomorrow by suffixing the time with tomorrow.

The `/var/adm/cron/at.allow` and `/var/adm/cron/at.deny` files determine which user can submit commands for later execution via at or batch. The format of the files is a list of usernames, one on each line. Whitespace is not permitted. If the file `/var/adm/cron/at.allow` exists, only usernames mentioned in it are allowed to use at. If `/var/adm/cron/at.allow` does not exist, `/var/adm/cron/at.deny` is checked, every username not mentioned in it is then allowed to use at. An empty `/var/adm/cron/at.deny` means that every user may use at.

Rationale:

An attacker may exploit use of the **at** to execute programs or processes automatically. Limiting access to **at** to authorised users reduces this risk.

It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Impact:

Any user(s), **including the root user**, not listed within `at.allow` will not be permitted to execute tasks via **at**.

Audit:

From the command prompt, execute the following command:

```
# /usr/bin/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:

```
# /usr/bin/cat /var/adm/cron/at.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 **at**

Remediation:

Remove **/var/adm/cron/at.deny** if it exists:

```
# /usr/bin/rm /var/adm/cron/at.deny
```

IF /var/adm/cron/at.allow does not exist, create the file:

```
# print "root\nadm" > /var/adm/cron/at.allow
```

IF /var/adm/cron/at.allow already exists, ensure that it contains at least the **root** and **adm** users.

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.			

6.2.2 Ensure access to crontab is configured

Profile Applicability:

- Level 1

Description:

crontab is the program used to install, deinstall, list or execute the tables used to drive the cron daemon. Each user can have their own crontab, and though files are created, they are not intended to be edited directly.

If the `/var/adm/cron/cron.allow` file exists, then you must be listed (one user per line) therein in order to be allowed to use this command. If the `/var/adm/cron/cron.allow` file does not exist but the `/var/adm/cron/cron.deny` file does exist, then you must not be listed in the `/var/adm/cron/cron.deny` file in order to use this command.

If neither of these files exists, then depending on site-dependent configuration parameters, only the super user will be allowed to use this command, or all users will be able to use this command.

If both files exist then `/var/adm/cron/cron.allow` takes precedence. Which means that `/var/adm/cron/cron.deny` is not considered and your user must be listed in `/var/adm/cron/cron.allow` in order to be able to use the crontab.

Rationale:

An attacker may exploit use of the **crontab** to execute programs or processes automatically. Limiting access to **crontab** to authorised users reduces this risk.

It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Impact:

Any user(s), **including the root user**, not listed within `cron.allow` will not be permitted to execute tasks via cron.

Audit:

From the command prompt, execute the following command:

```
# /usr/bin/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:

```
# /usr/bin/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:

Remove **/var/adm/cron/cron.deny** if it exists:

```
# /usr/bin/rm /var/adm/cron/cron.deny
```

IF /var/adm/cron/cron.allow does not exist, create the file:

```
# print "root\nadm" > /var/adm/cron/cron.allow
```

IF /var/adm/cron/cron.allow already exists, ensure that it contains at least the **root** and **adm** users.

Default Value:

N/A

References:

1. <https://www.ibm.com/docs/en/aix/7.2.0?topic=c-crontab-command>

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.			

7 Configure Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Why is this Control critical?

Cyber defenders are constantly being challenged from attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about: software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

7.1 Ensure Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) is regularly checked

Profile Applicability:

- Level 1

Description:

The Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) is a ksh script which uses data from the IBM website to compare the installed filesets and interim fixes on the system against known vulnerabilities and HIPER (High Impact PERvasive) issues.

Rationale:

Unpatched software can expose systems to known vulnerabilities that may be exploited by attackers. It is recommended that operating system updates be performed on enterprise assets through automated patch management on a monthly, or more frequent, basis. Knowledge of outstanding vulnerabilities is an important check within this process

Audit:

1. Obtain the latest version of [FLRTVC](#) from IBM and extract the script to a location on your server.
2. - **IF** - you are checking an air-gapped server obtain the latest version of [fix information](#) from IBM and place in the same directory.
3. Run the following command to check for known vulnerabilities # `./flrtvc.ksh`
4. The output should contain similar to the following:

```
# FLRTVC Script executed on Mon Oct 27 13:58:30 GMT 2025 using Version:
v0.8.12
# This report is based on APAR file dated : 2025.10.13

Fileset|Current Version|Type|EFix Installed|Abstract|Unsafe
Versions|APARs|Bulletin URL|Download URL|CVSS Base Score|Reboot Required|Last
Update|Fixed In
All vulnerabilities fixed.
```

Remediation:

If any vulnerabilities are reported above, you should review the details from the URL provided in the output before obtaining the fix from IBM support to install on the system.

Default Value:

Not installed

References:

1. <https://esupport.ibm.com/customercare/flrt/sas?page=../jsp/flrtvc.jsp>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v7	<u>3.1 Run Automated Vulnerability Scanning Tools</u> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			

7.2 Ensure system firmware updates are installed

Profile Applicability:

- Level 1

Description:

Security vulnerabilities and functional improvements are regularly addressed through firmware updates to the system and adapter firmware.

Rationale:

Unpatched system or adapter firmware can expose systems to known vulnerabilities that may be exploited by attackers. It is recommended that system and adapter firmware updates be performed on enterprise assets on a regular basis.

Impact:

Flexible Service Processor (FSP) firmware should only be updated from the Hardware Management Console (HMC) which is responsible for the hardware. I/O Adapter firmware should be updated from the LPAR to which the adapter is assigned.

Audit:

Execute the following command to obtain details of the hardware model and firmware

```
# /usr/sbin/lscfg 2> /dev/null | /usr/bin/grep -E "System Model|Firmware"
```

Compare the installed firmware with the latest available from [IBM FixCentral](#) for the identified hardware model.

Note: This command should only be run on a partition which has physical hardware adaptors assigned to it. e.g. a partition configured as VIOS.

Remediation:

Download the latest available from [IBM FixCentral](#) for the identified hardware model and follow the provided instructions to apply to the system/adapter

References:

1. <https://esupport.ibm.com/customercare/flrt/liteTable?prodKey=fw>

CIS Controls:

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

8 Logging and Auditing

CIS Control

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

AIX SYSLOG and AUDIT

SYSLOG is an application API. The application uses library calls to send messages to an optional syslog daemon that receives the messages and records them in a logfile. SYSLOG messages are grouped by message type (SYSLOG also refers to message type as message *facility*) and priority. Standard message facilities are: auth, mail, daemon, kern, user. See syslogd(AIX Commands Reference) for details.

AIX AUDIT is a kernel service that, when active, can report aka log system events as they occur. An application has no control over what or when these events are reported. That is the sole responsibility of the kernel – and the way the system mechanism is configured to report.

The key data reported in a system audit event are: header (info common to all audit events including: name, UID, time, return status) and so-called trail (event specific data).

AIX AUDIT has two operational states. These are called bin and stream. When bin mode is active audit events are written to a file. Once that file reaches a certain size that file is closed and a second file is opened (bina, binb). The file just collected gets processed – i.e., appended, to the so-called trail file – a historical log of all the events captured. This file can be processed by various programs to prepare and print the events in textual form. When stream mode is active audit events are written to the audit device (/dev/audit). This device is read by one (or more) instances of the auditstream utility. The key difference is that bin mode will only do optional processing when the so-called bin file reaches a predetermined size while stream processing supports near real-time reporting of system events.

8.1 Configure AIX Audit

AIX AUDIT provides a framework to capture system and security related information. This includes, but is not limited to: failed login attempts; cron usage; process init; failed file opens; etc. **AUDIT* is most effective when enabled as an additional of measure designed to track activity related to system and security changes.

The core documentation regarding the setup and management of **AIX AUDIT** can be found in the **redbook** [Accounting and Auditing for AIX 5L](#).

DRAFT

8.1.1 Ensure /audit filesystem has been created and configured

Profile Applicability:

- Level 2

Description:

This recommendation provides guidance for preparing an AIX system to operate with AUDIT active.

Rationale:

AIX Audit has been available as part of the kernel since 1995. The historical setup has all of its files in the *root* partition. This presents a risk that */* (*/dev/hd4*) may be (nearly) full and impact system availability. Further, while there is a separate user group defined (*audit*) the default configuration requires that an *audit admin* must be in two groups: *audit* and *security*. Better is to remove the requirement of the group *security*.

Impact:

This recommendation creates an additional logical volume (*hd12audit*) and filesystem (*/audit*) if the filesystem */audit* does not already exist.

The recommended minimum size of */audit* is 10G byte, but this is not scored. This is just a starting point for new systems. Usage will determine whether additional space is needed.

While an additional volume group could be created specifically for **AUDIT** this recommendation uses the default volume group *rootvg* to ensure that the volume group is always available when the system is operational.

Further, this recommendation moves the *audit* configuration to be parallel to */etc/security* rather than a subdirectory. A symbolic link points to the new location so that the AIX audit utilities (used as root) find the files via the expected pathname.

Audit:

- Ensure that the `/audit` filesystem has been created and mounted:

```
lsfs /audit > /dev/null || print "Audit Filesystem is missing"
```

The command should not yield any output:

- 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 <LV name> -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>

DRAFT

8.1.2 Ensure Audit bin(ary) audit event collection is configured

Profile Applicability:

- Level 2

Description:

This recommendation configures AIX auditing in bin mode.

Rationale:

The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Audit:

- 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
```

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	8.2 <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.			
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

8.1.3 Ensure modification to TE system is audited

Profile Applicability:

- Level 1

Description:

At Level 1, Trusted Execution (TE) should be actively monitoring for applications not yet allowlisted. The recommendation for this is in section two.

Additionally, the *AIX AUDIT* system needs to be configured for modifications to the TE subsystem.

Rationale:

Modification to security mechanisms need to be monitored to maintain system integrity.

Audit:

Run the following command and verify the output:

```
# /usr/bin/grep -p classes: /etc/security/audit/config | /usr/bin/egrep  
"default ="
```

Review the output and ensure that it contains at least the following entries:

```
TE_Untrusted,TE_FileWrite,TE_Policies,TEAdd_Stnz,TEDel_Stnz,TESwitch_algo,TEQ  
uery_Stnz
```

Remediation:

- Ensure AUDIT Trusted Execution events are in the class default.
 1. Edit the file `/etc/security/audit/config`
 2. Find the stanza named `classes:`
 3. If the class `default` does not exist add a line with:

```
default =
TE_Untrusted,TE_FileWrite,TE_Policies,TEAdd_Stnz,TEDel_Stnz,TESwitch_algo,TEQ
uery_Stnz
```

4. If the class `default` already exists ensure the following audit events are included in the class definition

```
TE_Untrusted,TE_FileWrite,TE_Policies,TEAdd_Stnz,TEDel_Stnz,TESwitch_algo,TEQ
uery_Stnz
```

CIS Controls:

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

8.2 Configure Syslog

This section will detail the recommendations regarding the configuration of syslog. By default the information sent to **syslogd** is not logged and important and pertinent information, such as failed switch user and login attempts are not recorded. The type of data which can be captured through this mechanism can be used for real-time and retrospective analysis, and is particularly useful for monitoring access to the system.

Logging data, via **syslogd**, may also provide unequivocal evidence against any individual or organization that successfully breach, or attempt to circumvent the security access controls surrounding a system.

Note:

- This section describes standard AIX **syslogd**. There is no *requirement* to use AIX syslog. In other words this section should be read that a **syslogd** is properly configured and minimally covers the recommendations listed. Some known alternative syslogd packages include *syslog-ng*, *rsyslogd* and *corelog*.
- If you use a different syslog it is your responsibility to modify commands used to audit and remediate the recommendation.

8.2.1 Ensure syslog local logging is configured

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 rotate time 1d files 30
compress archive /var/log/syslog/archive
auth.info /var/log/syslog/auth.log rotate time 1d files 30
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

If not already present, explicitly define a log file for the `auth.info` output in `/etc/syslog.conf`:

```
printf "auth.info\t\t/var/log/syslog/auth.log rotate time 1d files 30
compress\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:

```
# /usr/bin/touch /var/log/syslog/auth.log
# /usr/bin/chown root:system /var/log/syslog/auth.log
# /usr/bin/chmod u=rw,go= /var/log/syslog/auth.log
```

If not already present, 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/log/syslog/info.log`:

```
printf "%.info;auth.none\t/var/log/syslog/info.log rotate time 1d files 30
compress\n" >> /etc/syslog.conf
```

Create the **syslog** file:

```
# /usr/bin/touch /var/log/syslog/info.log
# /usr/bin/chown root:system /var/log/syslog/info.log
# /usr/bin/chmod u=rw,g=r,o= /var/log/syslog/info.log
```

Refresh **syslogd** to force the daemon to read the edited **/etc/syslog.conf**:

```
# refresh -s syslogd
```

Default Value:

Not configured

Additional Information:

Reversion:

Edit `/etc/syslog.conf` and remove the `authlog` and `syslog` entries:

```
vi /etc/syslog.conf
```

Remove:

```
auth.info          /var/adm/authlog rotate time 1w files 4
*.info;auth.none   /var/adm/syslog rotate time 1w files 4
```

Refresh **syslogd** to force the daemon to read the edited **/etc/syslog.conf**:

```
refresh -s syslogd
```

Delete the **authlog** and **syslog** files:

```
rm /var/adm/authlog /var/adm/syslog
```

8.2.2 Ensure syslog is configured to send logs to a remote log host

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:

```
grep -v '^s*#' /etc/syslog.conf | grep '@' | wc -l
```

Verify output is not equal to 0

Remediation:

Explicitly define a remote host for auth.info data in `/etc/syslog.conf` (enter the remote host IP address in the example below):

```
printf "auth.info\t\t@<IP address of remote syslog server>" >>  
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately

Create a remote host entry in `/etc/syslog.conf` to capture all other output of level info or higher (enter the remote host IP address in the example below):

```
printf "*.info;auth.none\t@<IP address of remote syslog server>\n" >>  
/etc/syslog.conf
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf`:

```
refresh -s syslogd
```

Default Value:

Not configured

Additional Information:

IBM POWER Systems can supply an additional security mechanism named **Trusted Logging** in it's PowerSC package.

This product writes logs to storage on a VIOS (Virtual I/O Server) without any need for an active/open IP path.

Since it is an additional product - we consider using **Trusted Logging** as Level 2, IG2 whereas remote syslog may be considered Level 1.

8.2.3 Ensure syslog is not configured to receive logs from a remote client

Profile Applicability:

- Level 1

Description:

This recommendation prevents the local **syslogd** daemon from accepting messages from other hosts on the network. Only central **syslog** servers, should accept remote **syslog** messages.

Rationale:

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:

```
# /usr/bin/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:

```
# /usr/bin/chssys -s syslogd -a "-r"
```

Re-cycle **syslogd** to activate the configuration change:

```
# /usr/bin/stopsys -s syslogd
# /usr/bin/startsys -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
```

DRAFT

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	Benchmark Organization		
1.1	Benchmark Principles, Conventions and Assumptions		
1.2	HOWTO use this benchmark		
1.3	AIX - Installation methods		
1.3.1	AIX RTE Installation		
1.3.2	AIX MKSYSB Installation		
1.3.3	AIX 7.2 installation		
1.3.3.1	AIX Secure Profile Installation (Basic AIX Security - BAS)		
1.3.3.2	Ensure SSH client and server packages are installed on AIX 7.2	☐	☐
1.3.4	AIX 7.3 Installation		
1.3.4.1	Ensure Secure by Default is selected during the installation	☐	☐
1.4	AIX Patch Management		
1.5	Summary		
2	Inventory and Control of Assets		
2.1	Ensure system configuration is documented and verified regularly	☐	☐
2.2	Ensure Trusted Execution Path is enabled	☐	☐
2.3	Ensure Trusted Execution (TE) policies are locked	☐	☐
2.4	Ensure Unauthorized Applications are reported	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.5	Ensure Allowlist violations are enabled	☐	☐
2.6	Ensure regular scans for unauthorized applications	☐	☐
2.7	Ensure unused symbolic links are removed	☐	☐
3	Configure Data Protection		
3.1	Ensure default user umask is configured	☐	☐
3.2	Ensure world writable directories have the SVTX bit set	☐	☐
3.3	Ensure there are no system 'default group' writable files (objects)	☐	☐
3.4	Ensure world writable files are secured	☐	☐
3.5	Ensure there are no group staff writable files	☐	☐
3.6	Ensure no files or directories without an owner and a group exist	☐	☐
4	Secure Configuration of Enterprise Assets and Software		
4.1	Trusted Files and Directories		
4.1.1	Configure Trusted Files		
4.1.1.1	Ensure access on root user smit.log is configured	☐	☐
4.1.1.2	Ensure access on /etc/group is configured	☐	☐
4.1.1.3	Ensure access on /etc/inetd.conf is configured	☐	☐
4.1.1.4	Ensure access on /etc/motd is configured	☐	☐
4.1.1.5	Ensure access on /etc/passwd is configured	☐	☐
4.1.1.6	Ensure /etc/mail/submit.cf access is configured	☐	☐
4.1.1.7	Ensure access to /etc/ssh/ssh_banner is configured	☐	☐
4.1.1.8	Ensure access on /etc/ssh/ssh_config is configured	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.1.9	Ensure access on /etc/ssh/sshd_config is configured	☐	☐
4.1.1.10	Ensure access on /var/adm/cron/at.allow is configured	☐	☐
4.1.1.11	Ensure access on /var/adm/cron/cron.allow is configured	☐	☐
4.1.1.12	Ensure access on /var/adm/cron/log is configured	☐	☐
4.1.1.13	Ensure access on /var/ct/RMstart.log is configured	☐	☐
4.1.1.14	Ensure access on /var/tmp/dpid2.log is configured	☐	☐
4.1.1.15	Ensure access on /var/tmp/hostmibb.log is configured	☐	☐
4.1.1.16	Ensure access on /var/tmp/snmpd.log is configured	☐	☐
4.1.1.17	Ensure access is configured for commands referenced by crontab entries	☐	☐
4.1.1.18	Ensure local interactive user dot files access is configured	☐	☐
4.1.1.19	Ensure SUID and SGID files are reviewed	☐	☐
4.1.1.20	Ensure access on /var/tmp/snmpdv3.log is configured	☐	☐
4.1.2	Configure Trusted Directories		
4.1.2.1	Ensure local user Home directories exists	☐	☐
4.1.2.2	Ensure HOME directories are owned by root or the UID specified in /etc/passwd	☐	☐
4.1.2.3	Ensure Home directory write access is restricted to owner	☐	☐
4.1.2.4	Ensure access on /audit and /etc/security/audit is configured	☐	☐
4.1.2.5	Ensure access to /etc/security is configured	☐	☐
4.1.2.6	Ensure access on /var/adm/ras is configured	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.2.7	Ensure access on /var/adm/sa is configured	☐	☐
4.1.2.8	Ensure access on /var/spool/cron/crontabs is configured	☐	☐
4.1.2.9	Ensure access on /var/spool/cron/atjobs is configured	☐	☐
4.1.2.10	Ensure all directories in root PATH access are configured	☐	☐
4.1.2.11	Ensure root user has a dedicated home directory	☐	☐
4.2	Configure Network Services		
4.2.1	Ensure NIS client is not installed	☐	☐
4.2.2	Ensure NIS server services are not in use	☐	☐
4.2.3	Ensure legacy NIS markers are removed	☐	☐
4.2.4	Ensure all entries in /etc/hosts.equiv are removed	☐	☐
4.2.5	Ensure that host based authentication files are not present	☐	☐
4.2.6	Ensure legacy remote daemon support is not available	☐	☐
4.2.7	Ensure snmpd is not installed	☐	☐
4.3	Subsystems managing the system boot phases		
4.3.1	Configure processes managed by /etc/inittab		
4.3.1.1	Ensure writesrv service is not in use	☐	☐
4.3.1.2	Ensure dt service is not in use	☐	☐
4.3.1.3	Ensure piobe service is not in use	☐	☐
4.3.1.4	Ensure qdaemon service is not in use	☐	☐
4.3.1.5	Ensure rcnfs service is not in use	☐	☐
4.3.1.6	Ensure snapp is not installed	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.1.7	Ensure NIM master is not installed	☐	☐
4.3.2	Configure daemons managed by /etc/rc.tcpip		
4.3.2.1	Ensure inetd daemon is disabled when no additional services are required	☐	☐
4.3.2.2	Ensure dhcp client services are not in use	☐	☐
4.3.2.3	Ensure dhcp relay services are not in use	☐	☐
4.3.2.4	Ensure dhcp server services are not in use	☐	☐
4.3.2.5	Ensure gated is not in use	☐	☐
4.3.2.6	Ensure hostmibd is not in use	☐	☐
4.3.2.7	Ensure multicast routing is not in use	☐	☐
4.3.2.8	Ensure dns server services are not in use	☐	☐
4.3.2.9	Ensure portmap is not in use	☐	☐
4.3.2.10	Ensure routed is not in use	☐	☐
4.3.2.11	Ensure rwhod is not in use	☐	☐
4.3.2.12	Ensure sendmail is not in use	☐	☐
4.3.2.13	Ensure timed is not in use	☐	☐
4.3.3	Configure IPv6		
4.3.3.1	Ensure autoconf6 is not in use	☐	☐
4.3.3.2	Ensure ndpd-host is not in use	☐	☐
4.3.3.3	Ensure ndpd-router is not in use	☐	☐
4.3.4	Configure services managed by the inetd process		
4.3.4.1	Ensure bootps daemon is not in use	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.4.2	Ensure chargen daemon is not in use	☐	☐
4.3.4.3	Ensure comsat daemon is not in use	☐	☐
4.3.4.4	Ensure daytime daemon is not in use	☐	☐
4.3.4.5	Ensure discard daemon is not in use	☐	☐
4.3.4.6	Ensure echo daemon is not in use	☐	☐
4.3.4.7	Ensure exec daemon is not in use	☐	☐
4.3.4.8	Ensure finger daemon is not in use	☐	☐
4.3.4.9	Ensure ftpd daemon is not in use	☐	☐
4.3.4.10	Ensure imap2 daemon is not in use	☐	☐
4.3.4.11	Ensure instsrv daemon is not in use	☐	☐
4.3.4.12	Ensure klogin daemon is not in use	☐	☐
4.3.4.13	Ensure kshell daemon is not in use	☐	☐
4.3.4.14	Ensure netstat daemon is not in use	☐	☐
4.3.4.15	Ensure ntalk daemon is not in use	☐	☐
4.3.4.16	Ensure pcnfsd daemon is not in use	☐	☐
4.3.4.17	Ensure pop3 daemon is not in use	☐	☐
4.3.4.18	Ensure rexd daemon is not in use	☐	☐
4.3.4.19	Ensure rlogin daemon is not in use	☐	☐
4.3.4.20	Ensure rquotad daemon is not in use	☐	☐
4.3.4.21	Ensure rstatd daemon is not in use	☐	☐
4.3.4.22	Ensure rsync daemon is not in use	☐	☐
4.3.4.23	Ensure rusersd daemon is not in use	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.4.24	Ensure rwalld daemon is not in use	☐	☐
4.3.4.25	Ensure shell daemon is not in use	☐	☐
4.3.4.26	Ensure sprayd daemon is not in use	☐	☐
4.3.4.27	Ensure talk daemon is not in use	☐	☐
4.3.4.28	Ensure telnetd daemon is not in use	☐	☐
4.3.4.29	Ensure tftpd daemon is not in use	☐	☐
4.3.4.30	Ensure time daemon is not in use	☐	☐
4.3.4.31	Ensure uucp daemon is not in use	☐	☐
4.3.4.32	Ensure xmquery daemon is not in use	☐	☐
4.4	Filesystem Configuration		
4.4.1	Configure Network Filesystem (NFS)		
4.4.1.1	Ensure NFS client mounts are disabled in /etc/filesystems	☐	☐
4.4.1.2	Ensure NFS server services are not in use	☐	☐
4.4.1.3	Ensure NFS client mounts include nosuid and nodev options	☐	☐
4.4.1.4	Ensure localhost aliases do not exist in /etc/exports	☐	☐
4.4.1.5	Ensure NFS exports use allow lists	☐	☐
4.4.1.6	Ensure access by root over nfs is disabled or blocked	☐	☐
4.4.1.7	Ensure secure RPC authentication is enabled	☐	☐
4.4.2	Configure Filesystem Encryption		
4.4.2.1	Ensure File System Level encryption is enabled	☐	☐
4.4.3	Configure ROOTVG		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.4.3.1	Ensure only / permits device files.	☐	☐
4.5	Configure Network Options		
4.5.1	Ensure sockthresh is configured	☐	☐
4.5.2	Ensure bcastping is disabled	☐	☐
4.5.3	Ensure clean_partial_conns is enabled	☐	☐
4.5.4	Ensure directed_broadcast is disabled	☐	☐
4.5.5	Ensure icmpaddressmask is disabled	☐	☐
4.5.6	Ensure ipforwarding is disabled	☐	☐
4.5.7	Ensure ip6forwarding is disabled	☐	☐
4.5.8	Ensure ipignoreredirects is enabled	☐	☐
4.5.9	Ensure ipsendredirects is disabled	☐	☐
4.5.10	Ensure ipsrouteforward is disabled	☐	☐
4.5.11	Ensure ipsrouterecv is disabled	☐	☐
4.5.12	Ensure ipsrouteseed is disabled	☐	☐
4.5.13	Ensure ip6srouteforward is disabled	☐	☐
4.5.14	Ensure nfs_use_reserved_ports is enabled	☐	☐
4.5.15	Ensure nonlocsrcroute is disabled	☐	☐
4.5.16	Ensure tcp_pmtu_discover is disabled	☐	☐
4.5.17	Ensure tcp_tcpsecure is configured	☐	☐
4.5.18	Ensure udp_pmtu_discover is disabled	☐	☐
4.5.19	Ensure icmptimestamp is disabled	☐	☐
4.6	Standard Services and Applications		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.6.1	Configure Common Desktop Environment		
4.6.1.1	Ensure CDE is not installed	☐	☐
4.6.1.2	Ensure the cmsd service is not available	☐	☐
4.6.1.3	Ensure dtlogin service is not available	☐	☐
4.6.1.4	Ensure dtspc is not available	☐	☐
4.6.1.5	Ensure CDE daemons have sgid and suid mode disabled	☐	☐
4.6.1.6	Ensure CDE remote GUI login is disabled	☐	☐
4.6.1.7	Ensure CDE screensaver lock is enabled	☐	☐
4.6.1.8	Ensure CDE login screen hostname is masked	☐	☐
4.6.1.9	Ensure access to /etc/dt/config/Xconfig is configured	☐	☐
4.6.1.10	Ensure the file /etc/dt/config/Xservers is configured	☐	☐
4.6.1.11	Ensure access to Xresources is configured	☐	☐
4.6.2	Configure FTPD		
4.6.2.1	Ensure root access to ftpd is disabled	☐	☐
4.6.2.2	Ensure ftpd login banner is configured	☐	☐
4.6.2.3	Ensure ftpd umask is configured	☐	☐
4.6.3	Configure OpenSSH		
4.6.3.1	Ensure latest version of openssh is installed	☐	☐
4.6.3.2	Ensure /etc/shosts.equiv and /etc/rhosts.equiv are removed	☐	☐
4.6.3.3	Ensure sftp-server arguments are configured	☐	☐
4.6.3.4	Ensure sshd access is configured	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.6.3.5	Ensure sshd Banner is configured	☐	☐
4.6.3.6	Ensure sshd Ciphers are configured	☐	☐
4.6.3.7	Ensure sshd HostbasedAuthentication is disabled	☐	☐
4.6.3.8	Ensure sshd IgnoreRhosts is enabled	☐	☐
4.6.3.9	Ensure sshd KexAlgorithms is configured	☐	☐
4.6.3.10	Ensure sshd LogLevel is configured	☐	☐
4.6.3.11	Ensure sshd MACs are configured	☐	☐
4.6.3.12	Ensure sshd MaxAuthTries is configured	☐	☐
4.6.3.13	Ensure sshd PermitEmptyPasswords is disabled	☐	☐
4.6.3.14	Ensure sshd PermitRootLogin is configured	☐	☐
4.6.3.15	Ensure sshd PermitRootLogin is disabled	☐	☐
4.6.3.16	Ensure sshd PermitUserEnvironment is disabled	☐	☐
4.6.3.17	Ensure sshd ReKeyLimit is configured	☐	☐
4.6.3.18	Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured	☐	☐
4.6.4	Configure Sendmail		
4.6.4.1	Ensure sendmail version information is hidden	☐	☐
4.6.4.2	Ensure sendmail PrivacyOptions is configured	☐	☐
4.6.4.3	Ensure access to /etc/mail/sendmail.cf is configured	☐	☐
4.6.4.4	Ensure access to /var/spool/clientmqueue is configured	☐	☐
4.6.4.5	Ensure access to /var/spool/mqueue is configured	☐	☐
4.7	Configure Login Controls		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.7.1	Ensure herald is configured	☐	☐
4.7.2	Ensure logindelay is configured	☐	☐
4.7.3	Ensure loginretries is configured	☐	☐
4.7.4	Ensure logintimeout is configured	☐	☐
4.7.5	Ensure TMOOUT is configured	☐	☐
4.7.6	Unattended terminal session timeout is 900 seconds (or less) - readonly	☐	☐
4.8	Verify Integrity of Installation Settings		
4.8.1	Ensure root access is controlled	☐	☐
4.8.2	Ensure root user default shell is ksh	☐	☐
4.8.3	Ensure core dumps are disabled	☐	☐
4.8.4	Ensure default path does not include current working directory	☐	☐
4.8.5	Ensure root user path does not include current working directory	☐	☐
4.8.6	Ensure motd is configured	☐	☐
4.9	Configure Memory Options		
4.9.1	Ensure Address space layout randomization is enabled	☐	☐
5	Account Management		
5.1	Configure local accounts		
5.1.1	Ensure all local user accounts have a hashed password	☐	☐
5.1.2	Ensure usernames and UIDs are unique	☐	☐
5.1.3	Ensure group names and GIDs are unique	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.4	Ensure an Inventory of Administrator accounts is established and maintained	☐	☐
5.1.5	Ensure an Inventory of user accounts is established and maintained	☐	☐
5.1.6	Ensure all local user accounts have valid stanzas in /etc/security/passwd	☐	☐
5.2	Password Management and Controls		
5.2.1	Ensure histsize is configured	☐	☐
5.2.2	Ensure minimum password age is configured	☐	☐
5.2.3	Ensure password history expiry is configured	☐	☐
5.2.4	Ensure passwords are controlled by password attributes	☐	☐
5.2.5	Ensure maxexpired is configured	☐	☐
5.2.6	Ensure password expiration is configured	☐	☐
5.2.7	Ensure pwd_algorithm is configured	☐	☐
5.2.8	Ensure a strong password hashing algorithm is configured	☐	☐
5.2.9	Ensure minimum password length is configured	☐	☐
5.2.10	Ensure number of characters changed in new password is configured	☐	☐
5.2.11	Ensure minalpha is configured	☐	☐
5.2.12	Ensure minother is configured	☐	☐
5.2.13	Ensure password maximum repeated characters is configured	☐	☐
5.2.14	Ensure mindigit is configured	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.15	Ensure minloweralpha is configured	☐	☐
5.2.16	Ensure minupperalpha is configured	☐	☐
5.2.17	Ensure minspecialchar is configured	☐	☐
5.3	Configure System Accounts		
5.3.1	Ensure user adm is secured	☐	☐
5.3.2	Ensure user bin is secured	☐	☐
5.3.3	Ensure user daemon is secured	☐	☐
5.3.4	Ensure user guest is secured	☐	☐
5.3.5	Ensure user lpd is secured	☐	☐
5.3.6	Ensure user nobody is secured	☐	☐
5.3.7	Ensure user nuucp is secured	☐	☐
5.3.8	Ensure user sys is secured	☐	☐
5.3.9	Ensure user uucp is secured	☐	☐
5.3.10	Ensure System Accounts cannot access system using ftp.	☐	☐
5.4	User Attributes for Active Processes		
5.5	Disable Dormant Accounts		
6	Access Control Management		
6.1	Configure SUDO managed privilege escalation		
6.1.1	Ensure sudo is installed	☐	☐
6.1.2	Ensure sudo logging is active	☐	☐
6.1.3	Ensure sudo commands use pty	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2	Configure Services Management		
6.2.1	Ensure at is restricted to authorized users	☐	☐
6.2.2	Ensure access to crontab is configured	☐	☐
7	Configure Continuous Vulnerability Management		
7.1	Ensure Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) is regularly checked	☐	☐
7.2	Ensure system firmware updates are installed	☐	☐
8	Logging and Auditing		
8.1	Configure AIX Audit		
8.1.1	Ensure /audit filesystem has been created and configured	☐	☐
8.1.2	Ensure Audit bin(ary) audit event collection is configured	☐	☐
8.1.3	Ensure modification to TE system is audited	☐	☐
8.2	Configure Syslog		
8.2.1	Ensure syslog local logging is configured	☐	☐
8.2.2	Ensure syslog is configured to send logs to a remote log host	☐	☐
8.2.3	Ensure syslog is not configured to receive logs from a remote client	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Version 1.1.0		
ADDED ITEMS:		
6/27/2025	1.1.0	ADDED SECTION: 1.3.3 - AIX 7.2 installation
6/27/2025	1.1.0	ADDED RECOMMENDATION: 1.3.3.2 - Ensure SSH client and server packages are installed on AIX 7.2
6/27/2025	1.1.0	ADDED SECTION: 1.3.4 - AIX 7.3 Installation
6/27/2025	1.1.0	ADDED RECOMMENDATION: 1.3.4.1 - Ensure Secure by Default is selected during the installation
6/27/2025	1.1.0	ADDED RECOMMENDATION: 2.2 - Ensure system Microcode Discovery Service (MDS) is performed regularly
6/27/2025	1.1.0	ADDED RECOMMENDATION: 3.5 - Ensure there are no group staff writable files
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.1.1.1 - Ensure access on root user smit.log is configured
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.2.8 - Ensure snmpd is not installed
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.3.1.6 - Ensure snapp is not installed
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.3.1.7 - Ensure NIM master is not installed
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.3.2.2 - Ensure dhcp client services are not in use
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.4.1.6 - Ensure access by root over nfs is disabled or blocked
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.4.2.2 - Ensure Filesystem Encryption via Encrypted Logical Volume is configured

Date	Version	Changes for this version
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.7.6 - Ensure TMOUT is configured
6/27/2025	1.1.0	ADDED RECOMMENDATION: 4.7.7 - Unattended terminal session timeout is 900 seconds (or less) - readonly
6/27/2025	1.1.0	ADDED SECTION: 4.8 - Verify Integrity of Installation Settings
6/27/2025	1.1.0	ADDED RECOMMENDATION: 5.1.6 - Ensure all local user accounts have valid stanzas in /etc/security/passwd
6/27/2025	1.1.0	ADDED RECOMMENDATION: 5.2.6 - Ensure password expiration is configured
6/27/2025	1.1.0	ADDED RECOMMENDATION: 5.2.10 - Ensure number of characters changed in new password is configured
6/27/2025	1.1.0	ADDED RECOMMENDATION: 7.1.3 - Ensure modification to TE system is audited
DROPPED ITEMS:		
6/27/2025	1.1.0	DROPPED SECTION: 2.1 - Trusted Execution (TE)
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 3.2 - Ensure group write permission are removed from default groups
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 3.6 - Ensure there are no group staff" writable files"
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.1.1.1 - Ensure access on /smit.log is configured
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.2.1 - Ensure sendmail in not in use
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.2.8 - Ensure snmpd is not available
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.3.2.2 - Ensure aixmibd service is removed
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.3.2.3 - Ensure dhcpd is not in use

Date	Version	Changes for this version
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.3.2.6 - Ensure dpid2 is not in use
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.3.2.15 - Ensure snmpmib2 is not in use
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.4.1.6 - Ensure root access is disabled or blocked.
6/27/2025	1.1.0	DROPPED SECTION: 4.6 - Configure Host Based Firewall
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.6.1 - Ensure that IP Security is available
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.6.2 - Ensure loopback traffic is blocked on external interfaces
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.6.3 - Ensure that IPsec filters are active
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 4.8.6 - Ensure session timeout is configured
6/27/2025	1.1.0	DROPPED SECTION: 4.9 - Configure Installation Settings
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 5.2.6 - Ensure maxage is configured
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 5.2.10 - Ensure password number of changed characters is configured
6/27/2025	1.1.0	DROPPED SECTION: 5.4 - User Attributes for Active Processes
6/27/2025	1.1.0	DROPPED SECTION: 5.5 - Disable Dormant Accounts
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 7.1.2 - Ensure Audit configuration defines audit classes
6/27/2025	1.1.0	DROPPED RECOMMENDATION: 7.1.3 - Ensure Audit creates audit processing commands
MOVED ITEMS:		

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED SECTION: 1.3.2 - AIX MKSYSB Installation moved from 1.3.3 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 1.3.3.1 - AIX Secure Profile Installation (Basic AIX Security - BAS) moved from 1.3.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.1 - Ensure system configuration is documented and verified regularly moved from 2.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.3 - Ensure Trusted Execution Path is enabled moved from 2.1.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.4 - Ensure Trusted Execution (TE) policies are locked moved from 2.1.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.5 - Ensure Unauthorized Applications are reported moved from 2.1.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.6 - Ensure Allowlist violations are enabled moved from 2.1.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.7 - Ensure regular scans for unauthorized applications moved from 2.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 2.8 - Ensure unused symbolic links are removed moved from 2.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 3.2 - Ensure world writable directories have the SVTX bit set moved from 3.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 3.3 - Ensure there are no system 'default group' writable files (objects) moved from 3.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 3.4 - Ensure world writable files are secured moved from 3.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 3.6 - Ensure no files or directories without an owner and a group exist moved from 3.7 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.2.1 - Ensure sendmail is not in use moved from 4.3.2.14 in 1.0.0

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.3 - Ensure dhcprd is not in use moved from 4.3.2.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.4 - Ensure dhcpsd is not in use moved from 4.3.2.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.5 - Ensure gated is not in use moved from 4.3.2.7 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.6 - Ensure hostmibd is not in use moved from 4.3.2.8 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.7 - Ensure mrouted is not in use moved from 4.3.2.9 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.8 - Ensure named is not in use moved from 4.3.2.10 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.9 - Ensure portmap is not in use moved from 4.3.2.11 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.10 - Ensure routed is not in use moved from 4.3.2.12 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.11 - Ensure rwhod is not in use moved from 4.3.2.13 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.12 - Ensure sendmail is not in use moved from 4.3.2.14 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.3.2.13 - Ensure timed is not in use moved from 4.3.2.16 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.6 - Standard Services and Applications moved from 4.7 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.6.1 - Configure Common Desktop Environment moved from 4.7.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.1 - Ensure CDE is not installed moved from 4.7.1.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.2 - Ensure the cmsd service is not available moved from 4.7.1.2 in 1.0.0

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.3 - Ensure dtlogin service is not available moved from 4.7.1.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.4 - Ensure dtspc is not available moved from 4.7.1.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.5 - Ensure CDE daemons have sgid and suid mode disabled moved from 4.7.1.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.6 - Ensure CDE remote GUI login is disabled moved from 4.7.1.6 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.7 - Ensure CDE screensaver lock is enabled moved from 4.7.1.7 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.8 - Ensure CDE login screen hostname is masked moved from 4.7.1.8 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.9 - Ensure access to /etc/dt/config/Xconfig is configured moved from 4.7.1.9 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.10 - Ensure the file /etc/dt/config/Xservers is configured moved from 4.7.1.10 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.1.11 - Ensure access to Xresources is configured moved from 4.7.1.11 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.6.2 - Configure FTPD moved from 4.7.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.2.1 - Ensure root access to ftpd is disabled moved from 4.7.2.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.2.2 - Ensure ftpd login banner is configured moved from 4.7.2.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.2.3 - Ensure ftpd umask is configured moved from 4.7.2.3 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.6.3 - Configure OpenSSH moved from 4.7.3 in 1.0.0

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.1 - Ensure latest version of openssh is installed moved from 4.7.3.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.2 - Ensure /etc/shosts.equiv and /etc/rhosts.equiv are removed moved from 4.7.3.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.3 - Ensure sftp-server arguments are configured moved from 4.7.3.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.4 - Ensure sshd access is configured moved from 4.7.3.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.5 - Ensure sshd Banner is configured moved from 4.7.3.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.6 - Ensure sshd Ciphers are configured moved from 4.7.3.6 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.7 - Ensure sshd HostbasedAuthentication is disabled moved from 4.7.3.7 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.8 - Ensure sshd IgnoreRhosts is enabled moved from 4.7.3.8 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.9 - Ensure sshd KexAlgorithms is configured moved from 4.7.3.9 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.10 - Ensure sshd LogLevel is configured moved from 4.7.3.10 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.11 - Ensure sshd MACs are configured moved from 4.7.3.11 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.12 - Ensure sshd MaxAuthTries is configured moved from 4.7.3.12 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.13 - Ensure sshd PermitEmptyPasswords is disabled moved from 4.7.3.13 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.14 - Ensure sshd PermitRootLogin is configured moved from 4.7.3.14 in 1.0.0

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.15 - Ensure sshd PermitRootLogin is disabled moved from 4.7.3.15 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.16 - Ensure sshd PermitUserEnvironment is disabled moved from 4.7.3.16 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.3.17 - Ensure sshd ReKeyLimit is configured moved from 4.7.3.17 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.6.4 - Configure Sendmail moved from 4.7.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.1 - Ensure sendmail version information is hidden moved from 4.7.4.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.2 - Ensure sendmail PrivacyOptions is configured moved from 4.7.4.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.3 - Ensure sendmail DaemonPortOptions is configured moved from 4.7.4.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.4 - Ensure access to /etc/mail/sendmail.cf is configured moved from 4.7.4.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.5 - Ensure access to /var/spool/clientmqueue is configured moved from 4.7.4.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.6.4.6 - Ensure access to /var/spool/mqueue is configured moved from 4.7.4.6 in 1.0.0
6/27/2025	1.1.0	MOVED SECTION: 4.7 - Configure Login Controls moved from 4.8 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.7.1 - Ensure herald is configured moved from 4.8.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.7.2 - Ensure logindelay is configured moved from 4.8.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.7.3 - Ensure loginretries is configured moved from 4.8.3 in 1.0.0

Date	Version	Changes for this version
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.7.4 - Ensure logintimeout is configured moved from 4.8.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.7.5 - Ensure administrative user accounts are locked moved from 4.8.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.1 - Ensure root access is controlled moved from 4.9.1 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.2 - Ensure root user default shell is ksh moved from 4.9.2 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.3 - Ensure core dumps are disabled moved from 4.9.3 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.4 - Ensure default path does not include current working directory moved from 4.9.4 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.5 - Ensure root user path does not include current working directory moved from 4.9.5 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 4.8.6 - Ensure motd is configured moved from 4.9.6 in 1.0.0
6/27/2025	1.1.0	MOVED RECOMMENDATION: 7.1.2 - Ensure Audit bin(ary) audit event collection is configured moved from 7.1.4 in 1.0.0
UPDATED ITEMS:		
6/27/2025	1.1.0	UPDATED SECTION: 1 - Benchmark Organization - Sections Modified: Description
6/27/2025	1.1.0	UPDATED SECTION: 1.1 - Benchmark Principles, Conventions and Assumptions - Sections Modified: Description
6/27/2025	1.1.0	UPDATED SECTION: 1.3 - AIX - Installation methods - Sections Modified: Description
6/27/2025	1.1.0	UPDATED SECTION: 1.3.3.1 - AIX Secure Profile Installation (Basic AIX Security - BAS) - Sections Modified: Description
6/27/2025	1.1.0	UPDATED SECTION: 1.5 - Summary - Sections Modified: Description

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED SECTION: 2 - Inventory and Control of Assets - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 2.5 - Ensure Unauthorized Applications are reported - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 2.7 - Ensure regular scans for unauthorized applications - Sections Modified: Rationale Statement
6/27/2025	1.1.0	UPDATED SECTION: 3 - Configure Data Protection - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 3.2 - Ensure world writable directories have the SVTX bit set - Sections Modified: Assessment Status; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 3.3 - Ensure there are no system 'default group' writable files (objects) - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 3.4 - Ensure world writable files are secured - Sections Modified: Assessment Status; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED SECTION: 4 - Secure Configuration of Enterprise Assets and Software - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.7 - Ensure access to /etc/ssh/ssh_banner is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.8 - Ensure access on /etc/ssh/ssh_config is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.9 - Ensure access on /etc/ssh/sshd_config is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.12 - Ensure access on /var/adm/cron/log is configured - Sections Modified: Remediation Procedure

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.13 - Ensure access on /var/ct/RMstart.log is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.14 - Ensure access on /var/tmp/dpid2.log is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.15 - Ensure access on /var/tmp/hostmibd.log is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.1.16 - Ensure access on /var/tmp/snmpd.log is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.2.4 - Ensure access on /audit and /etc/security/audit is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.2.5 - Ensure access to /etc/security is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.1.2.8 - Ensure access on /var/spool/cron/crontabs is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.2.1 - Ensure sendmail is not in use - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.2.6 - Ensure that host based authentication files are not present - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.2.7 - Ensure legacy remote daemon support is not available - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.1.1 - Ensure writesrv service is not in use - Sections Modified: Audit Procedure

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.1.2 - Ensure dt service is not in use - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.1.5 - Ensure rcnfs service is not in use - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.1 - Ensure inetd daemon is disabled when no additional services are required - Sections Modified: Impact Statement
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.3 - Ensure dhcprd is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.4 - Ensure dhcpsd is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.5 - Ensure gated is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.6 - Ensure hostmibd is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.8 - Ensure named is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.11 - Ensure rwhod is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.12 - Ensure sendmail is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.2.13 - Ensure timed is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.3.1 - Ensure autoconf6 is not in use - Sections Modified: Profile
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.3.2 - Ensure ndpd-host is not in use - Sections Modified: Profile
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.3.3 - Ensure ndpd-router is not in use - Sections Modified: Profile

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.4.14 - Ensure rlogin daemon is not in use - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.3.4.15 - Ensure netstat daemon is not in use - Sections Modified: Description
6/27/2025	1.1.0	UPDATED SECTION: 4.4.1 - Configure Network Filesystem (NFS) - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.4.1.1 - Ensure NFS client mounts are disabled in /etc/filesystems - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.4.1.3 - Ensure NFS client mounts include nosuid and nodev options - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.4.1.7 - Ensure secure RPC authentication is enabled - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.4.3.1 - Ensure only / permits device files. - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.1 - Ensure sockthresh is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.2 - Ensure bcastping is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.3 - Ensure clean_partial_conns is enabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.4 - Ensure directed_broadcast is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.5 - Ensure icmpaddressmask is disabled - Sections Modified: Remediation Procedure

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.6 - Ensure ipforwarding is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.7 - Ensure ip6forwarding is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.8 - Ensure ipignoreredirects is enabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.9 - Ensure ipsendredirects is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.10 - Ensure ipsrcrouteforward is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.11 - Ensure ipsrcrouterrecv is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.12 - Ensure ipsrcroutesend is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.13 - Ensure ip6srcrouteforward is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.14 - Ensure nfs_use_reserved_ports is enabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.15 - Ensure nonlocsrcroute is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.16 - Ensure tcp_pmtu_discover is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.17 - Ensure tcp_tcpsecure is configured - Sections Modified: Remediation Procedure

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.5.18 - Ensure udp_pmtu_discover is disabled - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.1.2 - Ensure the cmsd service is not available - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.1.3 - Ensure dtlogin service is not available - Sections Modified: Rationale Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.1.7 - Ensure CDE screensaver lock is enabled - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.1.8 - Ensure CDE login screen hostname is masked - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.1.10 - Ensure the file /etc/dt/config/Xservers is configured - Sections Modified: Audit Procedure
6/27/2025	1.1.0	UPDATED SECTION: 4.6.2 - Configure FTPD - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.3.1 - Ensure latest version of openssh is installed - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.3.11 - Ensure sshd MACs are configured - Sections Modified: Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.3.17 - Ensure sshd ReKeyLimit is configured - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.6.4.2 - Ensure sendmail PrivacyOptions is configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 4.7.1 - Ensure herald is configured - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
6/27/2025	1.1.0	UPDATED SECTION: 5 - Account Management - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 5.1.1 - Ensure all local user accounts have a hashed password - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 5.1.3 - Ensure group names and GIDs are unique - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED SECTION: 5.2 - Password Management and Controls - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 5.2.8 - Ensure a strong password hashing algorithm is configured - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 5.3.4 - Ensure user guest is secured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 5.3.10 - Ensure System Accounts cannot access system using ftp. - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED SECTION: 6 - Access Control Management - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 6.1.2 - Ensure sudo logging is active - Sections Modified: Remediation Procedure; Audit Procedure
6/27/2025	1.1.0	UPDATED SECTION: 6.2 - Configure Services Management - Sections Modified: Description
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 7.1.1 - Ensure /audit filesystem has been created and configured - Sections Modified: Remediation Procedure
6/27/2025	1.1.0	UPDATED RECOMMENDATION: 7.2.2 - Ensure syslog is configured to send logs to a remote log host - Sections Modified: Remediation Procedure
		Version 1.1.0 Published 7/27/2025

Date	Version	Changes for this version
Version 1.2.0		
ADDED ITEMS:		
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.1.17 - Ensure access is configured for commands referenced by crontab entries
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.1.18 - Ensure local interactive user dot files access is configured
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.1.20 - Ensure access on /var/tmp/snmpdv3.log is configured
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.2.2 - Ensure HOME directories are owned by root or the UID specified in /etc/passwd
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.2.9 - Ensure access on /var/spool/cron/atjobs is configured
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.1.2.10 - Ensure all directories in root PATH access are configured
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.3.2.3 - Ensure dhcp relay services are not in use
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.3.2.4 - Ensure dhcp server services are not in use
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.3.2.7 - Ensure multicast routing is not in use
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.3.2.8 - Ensure dns server services are not in use
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.3.4.22 - Ensure rsync daemon is not in use
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.5.19 - Ensure icmptimestamp is disabled
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.6.3.18 - Ensure sshd ClientAliveInterval and ClientAliveCountMax are configured
3/9/2026	1.2.0	ADDED SECTION: 4.9 - Configure Memory Options

Date	Version	Changes for this version
3/9/2026	1.2.0	ADDED RECOMMENDATION: 4.9.1 - Ensure Address space layout randomization is enabled
3/9/2026	1.2.0	ADDED SECTION: 5.4 - User Attributes for Active Processes
3/9/2026	1.2.0	ADDED SECTION: 5.5 - Disable Dormant Accounts
3/9/2026	1.2.0	ADDED RECOMMENDATION: 6.2.2 - Ensure access to crontab is configured
3/9/2026	1.2.0	ADDED SECTION: 7 - Configure Continuous Vulnerability Management
3/9/2026	1.2.0	ADDED RECOMMENDATION: 7.1 - Ensure Fix Level Recommendation Tool Vulnerability Checker Script (FLRTVC) is regularly checked
3/9/2026	1.2.0	ADDED RECOMMENDATION: 7.2 - Ensure system firmware updates are installed
DROPPED ITEMS:		
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 2.2 - Ensure system Microcode Discovery Service (MDS) is performed regularly
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.1.1.17 - Ensure crontab is restricted to authorized users
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.1.1.18 - Ensure Home directory configuration file access is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.1.2.2 - Ensure Home directories access is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.1.2.9 - Ensure all directories in root PATH access is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.3.2.3 - Ensure dhcprd is not in use
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.3.2.4 - Ensure dhcpsd is not in use
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.3.2.7 - Ensure mrouted is not in use

Date	Version	Changes for this version
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.3.2.8 - Ensure named is not in use
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.3.2.12 - Ensure sendmail is not in use
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.4.2.2 - Ensure Filesystem Encryption via Encrypted Logical Volume is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.6.4.3 - Ensure sendmail DaemonPortOptions is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 4.7.5 - Ensure administrative user accounts are locked
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 6.2.2 - Ensure at.allow is configured
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 6.2.3 - Ensure crontab is restricted authorized users
3/9/2026	1.2.0	DROPPED RECOMMENDATION: 6.2.4 - Ensure cron.allow is configured
MOVED ITEMS:		
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.2 - Ensure Trusted Execution Path is enabled moved from 2.3 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.3 - Ensure Trusted Execution (TE) policies are locked moved from 2.4 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.4 - Ensure Unauthorized Applications are reported moved from 2.5 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.5 - Ensure Allowlist violations are enabled moved from 2.6 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.6 - Ensure regular scans for unauthorized applications moved from 2.7 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 2.7 - Ensure unused symbolic links are removed moved from 2.8 in 1.1.0

Date	Version	Changes for this version
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.1.2.11 - Ensure root user has a dedicated home directory moved from 4.1.2.10 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.1 - Ensure NIS client is not installed moved from 4.2.2 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.2 - Ensure NIS server services are not in use moved from 4.2.3 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.3 - Ensure legacy NIS markers are removed moved from 4.2.4 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.4 - Ensure all entries in /etc/hosts.equiv are removed moved from 4.2.5 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.5 - Ensure that host based authentication files are not present moved from 4.2.6 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.6 - Ensure legacy remote daemon support is not available moved from 4.2.7 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.2.7 - Ensure snmpd is not installed moved from 4.2.8 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.2.12 - Ensure sendmail is not in use moved from 4.2.1 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.14 - Ensure netstat daemon is not in use moved from 4.3.4.15 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.15 - Ensure ntalk daemon is not in use moved from 4.3.4.16 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.16 - Ensure pcnfsd daemon is not in use moved from 4.3.4.17 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.17 - Ensure pop3 daemon is not in use moved from 4.3.4.18 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.18 - Ensure rexd daemon is not in use moved from 4.3.4.19 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.19 - Ensure rlogin daemon is not in use moved from 4.3.4.14 in 1.1.0

Date	Version	Changes for this version
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.23 - Ensure rusersd daemon is not in use moved from 4.3.4.22 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.24 - Ensure rwalld daemon is not in use moved from 4.3.4.23 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.25 - Ensure shell daemon is not in use moved from 4.3.4.24 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.26 - Ensure sprayd daemon is not in use moved from 4.3.4.25 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.3.4.32 - Ensure xmquery daemon is not in use moved from 4.3.4.26 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.6.4.3 - Ensure access to /etc/mail/sendmail.cf is configured moved from 4.6.4.4 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.6.4.4 - Ensure access to /var/spool/clientmqueue is configured moved from 4.6.4.5 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.6.4.5 - Ensure access to /var/spool/mqueue is configured moved from 4.6.4.6 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.7.5 - Ensure TMOUT is configured moved from 4.7.6 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 4.7.6 - Unattended terminal session timeout is 900 seconds (or less) - readonly moved from 4.7.7 in 1.1.0
3/9/2026	1.2.0	MOVED SECTION: 8 - Logging and Auditing moved from 7 in 1.1.0
3/9/2026	1.2.0	MOVED SECTION: 8.1 - Configure AIX Audit moved from 7.1 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.1.1 - Ensure /audit filesystem has been created and configured moved from 7.1.1 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.1.2 - Ensure Audit bin(ary) audit event collection is configured moved from 7.1.2 in 1.1.0

Date	Version	Changes for this version
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.1.3 - Ensure modification to TE system is audited moved from 7.1.3 in 1.1.0
3/9/2026	1.2.0	MOVED SECTION: 8.2 - Configure Syslog moved from 7.2 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.2.1 - Ensure syslog local logging is configured moved from 7.2.1 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.2.2 - Ensure syslog is configured to send logs to a remote log host moved from 7.2.2 in 1.1.0
3/9/2026	1.2.0	MOVED RECOMMENDATION: 8.2.3 - Ensure syslog is not configured to receive logs from a remote client moved from 7.2.3 in 1.1.0
UPDATED ITEMS:		
3/9/2026	1.2.0	UPDATED SECTION: 1 - Benchmark Organization - Sections Modified: Description
3/9/2026	1.2.0	UPDATED SECTION: 1.1 - Benchmark Principles, Conventions and Assumptions - Sections Modified: Description
3/9/2026	1.2.0	UPDATED SECTION: 1.2 - HOWTO use this benchmark - Sections Modified: Description
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 2.1 - Ensure system configuration is documented and verified regularly - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 2.4 - Ensure Unauthorized Applications are reported - Sections Modified: Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 2.7 - Ensure unused symbolic links are removed - Sections Modified: Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 3.1 - Ensure default user umask is configured - Sections Modified: Rationale Statement; Audit Procedure

Date	Version	Changes for this version
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 3.6 - Ensure no files or directories without an owner and a group exist - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.1.13 - Ensure access on /var/ct/RMstart.log is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.1.14 - Ensure access on /var/tmp/dpid2.log is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.1.15 - Ensure access on /var/tmp/hostmibd.log is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.1.16 - Ensure access on /var/tmp/snmpd.log is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED SECTION: 4.1.2 - Configure Trusted Directories - Sections Modified: Description
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.2.4 - Ensure access on /audit and /etc/security/audit is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.2.6 - Ensure access on /var/adm/ras is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.1.2.8 - Ensure access on /var/spool/cron/crontabs is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.2.1 - Ensure NIS client is not installed - Sections Modified: Description; Rationale Statement; Impact Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.2.6 - Ensure legacy remote daemon support is not available - Sections Modified: Remediation Procedure

Date	Version	Changes for this version
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.1.1 - Ensure writesrv service is not in use - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.1.2 - Ensure dt service is not in use - Sections Modified: Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.1.3 - Ensure piobe service is not in use - Sections Modified: Rationale Statement; Impact Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.1.4 - Ensure qdaemon service is not in use - Sections Modified: Rationale Statement; Impact Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.1.7 - Ensure NIM master is not installed - Sections Modified: Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.2 - Ensure dhcp client services are not in use - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.5 - Ensure gated is not in use - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.6 - Ensure hostmibd is not in use - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.10 - Ensure routed is not in use - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.11 - Ensure rwhod is not in use - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.12 - Ensure sendmail is not in use - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.2.13 - Ensure timed is not in use - Sections Modified: Description; Rationale Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.3.3 - Ensure ndpd-router is not in use - Sections Modified: Impact Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.3.4.19 - Ensure rlogin daemon is not in use - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.5.16 - Ensure tcp_pmtu_discover is disabled - Sections Modified: Rationale Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.5.18 - Ensure udp_pmtu_discover is disabled - Sections Modified: Rationale Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.6.3.3 - Ensure sftp-server arguments are configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 4.8.5 - Ensure root user path does not include current working directory - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 6.1.1 - Ensure sudo is installed - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 6.1.2 - Ensure sudo logging is active - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 6.1.3 - Ensure sudo commands use pty - Sections Modified: Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 6.2.1 - Ensure at is restricted to authorized users - Sections Modified: Profile; Description; Rationale Statement; Impact Statement; Remediation Procedure; Audit Procedure

Date	Version	Changes for this version
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 8.1.2 - Ensure Audit bin(ary) audit event collection is configured - Sections Modified: Rationale Statement
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 8.1.3 - Ensure modification to TE system is audited - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 8.2.1 - Ensure syslog local logging is configured - Sections Modified: Remediation Procedure; Audit Procedure
3/9/2026	1.2.0	UPDATED RECOMMENDATION: 8.2.3 - Ensure syslog is not configured to receive logs from a remote client - Sections Modified: Profile; Description; Rationale Statement; Remediation Procedure; Audit Procedure