the CENTER for
INTERNET SECURITY

Security Configuration Benchmark For

IBM AIX 5.3 and AIX 6.1

Version 1.0.0
December 21st, 2010

http://cisecurity.org
feedback@cisecurity.org

Terms of Use Agreement

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere (“**Products**”) as a public service to Internet users worldwide. Recommendations contained in the Products (“**Recommendations**”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization (“**we**”) agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;

We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, Security Configuration Benchmark for AIX 5.3 and AIX 6.1, provides prescriptive guidance for establishing a secure configuration posture for AIX versions 5.3 and 6.1 running on the Power Systems platform. This guide was tested against AIX 5.3 TL-05 / TL-07 and AIX 6.1 TL-01, installed from IBM base installation media. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

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

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to 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 5.3 and AIX 6.1 on the Power Systems platform.

A working knowledge of `vi` is assumed in order to implement some of the configuration changes.

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:

Authors
Paul Sharpe

Contributors and Reviewers
Shailesh Athalye, *Symantec Inc.*
Christiane Cuculo, *CPqD*
Blake Frantz, *Center for Internet Security*
Huibert Kivits
Boris Kleiman, *Lightening International*
Nikhil Mittal
Steve Parham, *IBM*

Typographic Conventions

The following typographical conventions are used throughout this guide:

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

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

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

Level-II Benchmark settings/actions

Level-II 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

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Introduction

Scope

This guide provides security configuration guidance for use during the configuration of AIX 5.3 and 6.1 Operating Systems. There is a particular emphasis on the configuration of AIX 6.1, but as there is common affinity between the two releases much of the guide is relevant regardless of version specifics. Where function is not available for AIX 5.3, this will be clearly highlighted and where there is a different approach, this will be clearly defined.

The scope of the guide is applicable to AIX 5.3 TL-05+ and AIX 6.1. The reason for the minimum version requirement of AIX 5.3 TL-05 is because the AIX Security Expert tool will be used to automate a large proportion of the best practice and recommendations and this is the AIX 5.3 Technology Level in which the tool was first released.

Approach

The suggested approach in terms of implementing this guide would be to install a vanilla AIX image, via NIM or the AIX product CD/DVD's, followed by the recommendations detailed in this guide and any other corporate standardization i.e. software installation and filesystem and user creation. Once completed, a `mksysb` backup of the system could then be taken and this image could be deployed via NIM for any subsequent operating system builds. This would provide a standard build mechanism, ensuring 100% compliance to all company standards and the best practice recommendations detailed in this benchmark.

Within the AIX Base Operating System Installation Menus it is recommended that the following options are selected:

- 64-bit kernel

- JFS2 filesystems
- All devices and kernels are installed = yes *
- Trusted Computing Base Install = yes **

* This is to ensure that all device drivers are contained within the standard build image for deploying to different server hardware configurations.

** For AIX 5.3 systems only, it is recommended that Trusted Computing Base (TCB) is installed. This is an install time only option.

Maintenance Cadence

Considerations

Before entering into the recommendation section of this paper it is important to put into context the relevance of an AIX software maintenance strategy. It is imperative that regular Technology Level (TL) and Service Pack (SP) updates are applied to an AIX estate, to ensure that all known security vulnerabilities are addressed and to remain within a supported TL stream.

The current IBM software maintenance strategy revolves around the release of Technology Levels and Service Packs. Technology Levels are released twice per year, one in the spring and the other in fall. They introduce support for new hardware, new functionality, and new features and contain cumulative fixes since the release of the previous TL. The fix support window for a given TL is two years from its release date.

Service Packs are released throughout the lifecycle of the TL and address security vulnerabilities and other critical fixes. They are typically released every 12 weeks; obviously this timeframe is dependant on the number and criticality of the issues found.

It is recommended that full TL's or SP's are applied rather than individual fixes, due to the far more rigorous certification and testing process. The large and complex matrix of possible fix combinations are not subjected to the same degree of testing and therefore installing individual fixes is not recommended.

A security fix will be initially released as an interim fix, which is installed and maintained via the `emgr` framework. It is recommended that, unless it is an extremely critical security issue, to wait and apply the fix as part of a full SP release to ensure maximum system stability.

Summary

The recommended maintenance strategy is as follows:-

- Stay current and refresh the TL of each system at least once a year – For maximum system stability wait until SP3 is released on the newer TL and then migrate.

- Review the Service Packs for any security or critical fixes – apply these regularly throughout the life cycle of a TL.

- Do not apply interim fixes or individual fixes unless there is an urgent requirement to do so. Instead apply full TL's and SP's for maximum stability.

- There should be a monthly review of the security advisory bulletins to remain apprised of all known security issues. These can currently be viewed at the following URL:

  http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd

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

  ftp://aix.software.ibm.com/aix/efixes/security

- 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:

  http://www-933.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:

  http://www14.software.ibm.com/webapp/set2/sas/f/best/home.html

AIX Security Expert Introduction

This section will focus on the AIX Security Expert framework. The tool has been introduced to standardize and simplify the security hardening process in AIX, with over 300 settings and commands within its scope. It can be used to replace in-house security scripts and procedures.

Security Levels

There are three standard security levels, other than default, and the ability to create a customized hybrid policy.

Low Level Security

This policy implements common non-disruptive security enhancements.

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

Medium Level Security

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

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

High Level Security

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

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

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

Custom Level Security

The approach of this benchmark is to implement a hybrid policy, which contains a combination of recommended settings from both the Medium and High Level default policies. A customized XML file provides the ultimate flexibility in terms of being able to choose whether or not to implement every recommended AIX Security Expert controlled setting in this benchmark e.g. whether clear text password protocols are allowed. This policy can be easily modified depending on the environmental requirements. A simple edit of the customized XML file, prior to it being implemented, is all that is required. This flexibility is not present within the default Low, Medium and High Level policies which provide a pre-defined rigid level of security hardening standards.

Implementing the Custom Level Policy

There are two tar files provided with this benchmark, one for each AIX release, as there are XML format differences between the two operating system versions. Both files are in tar format, have an absolute path and can be extracted via the following commands:-

AIX 5.3:

```
tar -xvf <PATH to tar file>/CIS_IBM_AIX_5.3-6.1_Benchmark_v1.0.0_AIXPERT_5.3.tar
```

AIX 6.1:

```
tar -xvf <PATH to tar file>/CIS_IBM_AIX_5.3-6.1_Benchmark_v1.0.0_AIXPERT_6.1.tar
```

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

For AIX 5.3:

```
/etc/security/aixpert/custom/custom_5.3.xml
```

For AIX 6.1:

```
/etc/security/aixpert/custom/custom_6.1.xml
```

Prior to implementing the AIX Security Expert customized settings, please review the benchmark recommendations in the next section. If there are any settings that need to be changed from a recommended value, based on environmental requirements, edit the XML file using the `vi` command. All AIX Security Expert managed Level 2 recommendations have a procedure detailing which applicable setting to change for reversion, if required.

As much of the guide as possible has been automated within the AIX Security Expert customized XML file. This includes a number of recommendations normally outside the remit of the tool. In these instances the `execmds` functionality has been used to execute the appropriate commands and implement the recommendations.

One of the recommendations within this benchmark is to setup and configure AIX auditing (1.7.11). In the introductory section of this document, it was recommended that the Operating System be installed utilizing `jfs2` filesystems. The default AIX Security Expert scripts (AIX 5.3 TL-07) created a `jfs` based `/audit` filesystem during testing, so to ensure that a `jfs2` audit filesystem is utilized, it can be manually created.

If the system was installed utilizing `jfs` filesystems, or if auditing is not to be implemented, the commands below can be ignored:

```
mklv -y auditlv -t jfs2 -u 2 -c 1 rootvg 1 hdisk0
crfs -v jfs2 -d auditlv -m /audit -A yes -t no
mount /audit
chfs –a size=256M /audit
```

NOTE: The `chfs` resizing is only valid when the physical partition size of `rootvg` is less than 256MB. The logical volume name can be changed from the example to reflect any internal standards.

Once the recommendations have been reviewed, implementation of the customized XML file should be performed in the following way:

AIX 5.3:

```
aixpert -f /etc/security/aixpert/custom/custom_5.3.xml
```

AIX 6.1:

```
aixpert -f /etc/security/aixpert/custom/custom_6.1.xml
```

Once the XML has been successfully implemented, the applied settings are placed in the following file:

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

The values set by the customized XML file can be validated via:

```
aixpert –c
```

This compares the settings, defined in the `appliedaixpert.xml` file, to those currently set on the system. If there is deviation from these standards i.e. a setting has been changed, it will be reported in the following log file:

```
cat /etc/security/aixpert/check_report.txt
```

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

During the customized XML implementation, the following files are copied prior to being changed:

```
cp –p /etc/inittab /etc/inittab.orig.$date
cp -p /etc/rc.tcpip /etc/rc.tcpip.orig.$date
cp –p /etc/inetd.conf /etc/inetd.conf.orig.$date
```

1. AIX Security Expert Recommendations

This section provides details of the recommended settings controlled within the AIX Security Expert framework. The settings within this section can all be automatically applied, utilizing the `aixpert` command to implement the customized XML file.

1.1 AIX Security Expert – Password Policy

This section provides guidance on the configuration of the password policy. This includes recommended length, complexity, re-use and expiration.

The recommendations in this section affect the parameters of the default user stanza. The values set are only applicable if specific values are not defined during the creation of a user. It is therefore recommended to not set any of these values explicitly, unless there is a specific requirement to do so when a user is created.

1.1.1 /etc/security/user - mindiff (Level 1, Scorable)

Description:
Defines the minimum number of characters that are required in a new password which were not in the old password.

Rationale:
In setting the `mindiff` attribute, it ensures that users are not able to reuse the same or similar passwords.

Remediation:
In `/etc/security/user`, set the default user stanza `mindiff` attribute to be greater than or equal to `4`.

This means that when a user password is set it needs to comprise of at least `4` characters not present in the previous password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a mindiff=4
```

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default mindiff=4
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	mindiff=4
Medium Level policy	mindiff =3
Low Level policy	No effect

1.1.2 /etc/security/user - minage (Level 1, Scorable)

Description:
Defines the minimum number of weeks before a password can be changed.

Rationale:
In setting the `minage` attribute, it prohibits users changing their password until a set number of weeks have passed.

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

This means that a user cannot change their password until at least a week after being set.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a minage=1
```

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
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	minage=1
Medium Level policy	minage =4
Low Level policy	No effect

1.1.3 /etc/security/user - maxage (Level 1, Scorable)

Description:
Defines the maximum number of weeks that a password is valid.

Rationale:
In setting the `maxage` attribute, it enforces regular password changes.

Remediation:
In `/etc/security/user`, set the default user stanza `maxage` attribute to be less than or equal to `13`.

This means that a user password must be changed `13` weeks after being set.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a maxage=13
```

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default maxage=13
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	maxage =13
Medium Level policy	maxage = 13
Low Level policy	maxage = 52

1.1.4 /etc/security/user - minlen (Level 1, Scorable)

Description:
Defines the minimum length of a password.

Rationale:
In setting the `minlen` attribute, it ensures that passwords meet the required length criteria.

Remediation:
In `/etc/security/user`, set the default user stanza `minlen` attribute to be greater than or equal to `8`.

This means that all user passwords must be at least `8` characters in length.

NOTE: If a password length greater than `8` is required, an enhanced password hashing algorithm must be selected as detailed in section 1.1.11. The default crypt algorithm only supports `8` character passwords.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a minlen=8
```

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minlen=8
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	minlen = 8
Medium Level policy	minlen = 8
Low Level policy	minlen = 8

1.1.5 /etc/security/user - minalpha (Level 1, Scorable)

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.

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

This means that there must be at least `2` alphabetic characters within an `8` character user password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minalpha=2
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	minalpha = 2
Medium Level policy	minalpha = 1
Low Level policy	No effect

1.1.6 /etc/security/user- minother (Level 1, Scorable)

Description:
Defines the number of characters within a password which must be non-alphabetic.

Rationale:
In setting the `minother` attribute, it limits the number of weeks after password expiry when it may be changed by the user.

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

This means that there must be at least `2` non-alphabetic characters within an `8` character user password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default minother=2
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	minother = 2
Medium Level policy	minother = 1
Low Level policy	no effect

1.1.7 /etc/security/user - maxrepeats (Level 1, Scorable)

Description:
Defines the maximum number of times a character may appear in a password.

Rationale:
In setting the `maxrepeats` attribute, it enforces a maximum number of character repeats within a password

Remediation:
In `/etc/security/user`, set the default user stanza `maxrepeats` attribute to `2`.

This means that a user may not use the same character more than twice in a password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

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=2
```

Default Value: 8

Default AIX Security Expert policy values:

High Level policy	maxrepeats = 2
Medium Level policy	no effect
Low Level policy	no effect

1.1.8 /etc/security/user - histexpire (Level 1, Scorable)

Description:
Defines the period of time in weeks that a user will not be able to reuse a password.

Rationale:
In setting the `histexpire` attribute, it ensures that a user cannot reuse a password within a set period of time.

Remediation:
In `/etc/security/user`, set the default user stanza `histexpire` attribute to be less than or equal to `13`.

This means that a user will not be able to re-use any password set in the last 13 weeks.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a histexpire=13
```

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=13
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	histexpire = 13
Medium Level policy	histexpire = 13
Low Level policy	histexpire = 26

1.1.9 /etc/security/user - histsize (Level 1, Scorable)

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.

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

This means that a user many not re-use any of the previous 20 passwords.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default histsize=20
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	histsize = 20
Medium Level policy	histsize = 4
Low Level policy	histsize = 4

1.1.10 /etc/security/user - maxexpired (Level 1, Scorable)

Description:
Defines the number of weeks after `maxage`, that a password can be reset by the user

Rationale:
In setting the `maxexpired` attribute, it limits the number of weeks after password expiry when it may be changed by the user.

Remediation:
In `/etc/security/user`, set the default user stanza `maxexpired` attribute to `2`.

This means that a user can only reset their password up to `2` weeks after it has expired. After this an administrative user would need to reset the password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

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=2
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	maxexpired = 2

Medium Level policy maxexpired = 4
Low Level policy   maxexpired = 8

1.1.11 /etc/security/login.cfg – pwd_algorithm (AIX 5.3 TL-07 +) (Level 2, Scorable)

Description:
Defines the loadable password algorithm used when storing user passwords.

The management of the password encryption algorithm is not performed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

Rationale:
A development of AIX 6.1 was the ability to use different password algorithms as defined in `/etc/security/pwdalg.cfg`. This functionality has been back ported into AIX 5.3 TL-07 and above. 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 `ssha256`. 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 remain supported, but there can only one system password algorithm active at any one time.

Remediation:
In `/etc/security/login.cfg`, set the `usw` user stanza `pwd_algorithm` attribute to `ssha256`.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s usw -a pwd_algorithm=ssha256
```

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
usw pwd_algorithm=ssha256
```

Reversion:
If there is a requirement to continue to use the `crypt` algorithm or the system is running on a level older than AIX 5.3 TL-07, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chsec -f /etc/security/login.cfg -s usw -a
pwd_algorithm=ssha256"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chsec -f /etc/security/login.cfg -s usw -a
pwd_algorithm=ssha256"</AIXPertArgs> -->
```

Default Value: crypt

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.2 AIX Security Expert – Login Policy

This section provides guidance on the configuration of the system login policy. This includes login timeouts, delays and remote root access.

The recommendations in this section affect the general login policy of the system for all users. Every user should have a dedicated account, to ensure accountability and audit trailing. Any generic accounts should be disabled from direct login, where possible. All remote logons as root should also be prohibited, instead elevation to root should only be allowed once a user has authenticated locally through their individual user account.

1.2.1 /etc/security/login.cfg - logininterval (Level 1, Scorable)

Description:

Defines the time interval, in seconds, when the unsuccessful logins must occur to disable a port. This parameter is applicable to all `tty` connections and the system console.

Rationale:

In setting the `logininterval` attribute, a port will be disabled if the incorrect password is entered a pre-defined number of times, set via `logindisable`, within this interval.

Remediation:

In `/etc/security/login.cfg`, set the default stanza `logininterval` attribute to be less than or equal to `300`.

This means that the port will be disabled if the incorrect password is typed the appropriate number of times, within a `300` second interval.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s default -a logininterval=300
```

Audit:
From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logininterval
```

The above command should yield the following output:

```
default logininterval=300
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	logininterval = 300
Medium Level policy	logininterval = 60
Low Level policy	no effect

1.2.2 /etc/security/login.cfg - logindisable (Level 1, Scorable)

Description:
Defines the number of unsuccessful login attempts required before a port will be locked. This parameter is applicable to all `tty` connections and the system console.

Rationale:
In setting the `logindisable` attribute, a port will be disabled if the incorrect password is entered a set number of times within a specified interval, set via `logininterval`.

Remediation:
In `/etc/security/login.cfg`, set the default stanza `logindisable` attribute to be less than or equal to `10`.

This means that the port will be disabled if the incorrect password is typed `10` times within a `300` second interval.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s default -a logindisable=10
```

Audit:
From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a logindisable
```

The above command should yield the following output:

```
default logindisable=10
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	logindisable = 10
Medium Level policy	logindisable = 10
Low Level policy	no effect

1.2.3 /etc/security/login.cfg - loginreenable (Level 1, Scorable)

Description:
Defines the number of seconds after a port is locked that it will be automatically un-locked. This parameter is applicable to all `tty` connections and the system console.

Rationale:
In setting the `loginreenable` attribute, a locked port will be automatically re-enabled once a given number of seconds have passed.

Remediation:
In `/etc/security/login.cfg`, set the default stanza `loginreenable` attribute to be greater than or equal to `360`.

This means that a locked port will be automatically re-enabled `360` seconds after being locked.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s default -a loginreenable=360
```

Audit:
From the command prompt, execute the following command:

```
lssec -f /etc/security/login.cfg -s default -a loginreenable
```

The above command should yield the following output:

```
default loginreenable=360
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	loginreenable = 360
Medium Level policy	loginreenable = 30
Low Level policy	no effect

1.2.4 /etc/security/login.cfg - logintimeout (Level 1, Scorable)

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.

Remediation:
In `/etc/security/login.cfg`, set the usw stanza `logintimeout` attribute to be less than or equal to `30`.

This means that a user will have `30` seconds, from prompting, in which to type in their password.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s usw -a logintimeout=30
```

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
```

Default Value: 60

Default AIX Security Expert policy values:

High Level policy	logintimeout = 30
Medium Level policy	logintimeout = 60
Low Level policy	logintimeout = 60

1.2.5 /etc/security/login.cfg - logindelay (Level 1, Scorable)

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.

Remediation:
In `/etc/security/login.cfg`, set the default stanza `logindelay` attribute to be greater than or equal to `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`)

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s default -a logindelay=10
```

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
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	logindelay = 10
Medium Level policy	logindelay = 5
Low Level policy	logindelay = 5

1.2.6 /etc/security/user - loginretries (Level 1, Scorable)

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.

Remediation:
In `/etc/security/user`, set the default stanza `loginretries` attribute to `3`.

This means that a user will have `3` attempts to enter the correct password. This does not apply to the root user, which has its own stanza entry disabling this feature.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s default -a loginretries=3
```

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=3
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	loginretries = 3
Medium Level policy	loginretries = 4
Low Level policy	AIX 5.3 =No effect AIX 6.1 = 5

1.2.7 /etc/security/user - rlogin (Level 1, Scorable)

Description:
Defines whether or not the root user can login remotely.

Rationale:
In setting the `rlogin` attribute to false, this ensures that the root user cannot remotely log into the system. All remote logins as root should be prohibited, instead elevation to root should only be allowed once a user has authenticated locally through their individual user account.

Remediation:
In `/etc/security/user`, set the root stanza `rlogin` attribute to `false`.

This means that the root user will not be able to log in the system directly.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/user -s root -a rlogin=false
```

Audit:
From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s root -a rlogin
```

The above command should yield the following output:

```
root rlogin=false
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	rlogin = false
Medium Level policy	rlogin = false
Low Level policy	rlogin = true

1.2.8 /etc/security/user - sugroups (Level 1, Scorable)

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

Rationale:
In setting the `sugroups` attribute to `system`, this ensures that only members of the system group are able to `su` root. This makes it difficult for an attacker to use a stolen root password as the attacker first has to get access to a system user ID.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chuser su=true sugroups=system root
```

Audit:
From the command prompt, execute the following command:

```
lssec -f /etc/security/user -s root -a sugroups -a su
```

The above command should yield the following output:

```
root sugroups=ALL su=true
```

Default Value: N/A

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.2.9 System account lockdown (Level 2, Scorable)

Description:
This change disables direct login access for the generic system accounts i.e. `daemon, bin, sys, adm, uucp, nobody and lpd.`

The lockdown of the non-interactive system users is not a managed process within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

Rationale:
This change disables direct local and remote login to the generic system accounts i.e. `daemon, bin, sys, adm, uucp, nobody and lpd`. It is recommended that a password is not set on these accounts to ensure that the only access is via `su` from the root account.

There should not be a requirement to log in as any of these users directly. All users should be given specific logon ids to ensure traceability and accountability.

Remediation:
Change the login and remote login user flags to disable access.

Please note the commands below are for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chuser login=false rlogin=false daemon
chuser login=false rlogin=false bin
chuser login=false rlogin=false sys
chuser login=false rlogin=false adm
chuser login=false rlogin=false uucp
chuser login=false rlogin=false nobody
chuser login=false rlogin=false lpd
```

Audit:

```
lsuser -a login rlogin <user>
```

The above command should yield the following output:

```
<user> login=false rlogin=false
```

Reversion:
If there is a requirement to enable generic account remote access, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
 <AIXPertArgs>"chuser login=false rlogin=false daemon; chuser login=false
rlogin=false bin; chuser login=false rlogin=false sys; chuser login=false
```

```
rlogin=false adm; chuser login=false rlogin=false uucp; chuser login=false
rlogin=false nobody; chuser login=false rlogin=false lpd"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chuser login=false rlogin=false daemon; chuser login=false
rlogin=false bin; chuser login=false rlogin=false sys; chuser login=false
rlogin=false adm; chuser login=false rlogin=false uucp; chuser login=false
rlogin=false nobody; chuser login=false rlogin=false lpd"</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3 AIX Security Expert – System Services Management

The objective of this section is to reduce the number of running services down to those which are core to the common functions of a UNIX server. When a superfluous service is not running, the system will not be subject to any latent vulnerability later discovered with that service and not require any subsequent remediation.

This section provides guidance on the startup of system services in `/etc/inittab`, `/etc/rc.tcpip` and `/etc/inetd.conf`. The majority of services within these files are disabled in AIX by default, so this section will focus on those services which are enabled, which if possible, should be disabled.

1.3.1 /etc/inittab - qdaemon (Level 2, Scorable)

Description:

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

Rationale:

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

Remediation:

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmitab qdaemon
```

Audit:

From the command prompt, execute the following command:

```
lsitab qdaemon
```

The above command should yield not yield output

Reversion:
If there is a requirement to implement print queues on the system, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>qdaemon: /etc/inittab : d disqdaemonhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>qdaemon: /etc/inittab : d disqdaemonhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>qdaemon: /etc/inittab : d hls_disqdaemon</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>qdaemon: /etc/inittab : d hls_disqdaemon</AIXPertArgs> -->
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	Entry removed
Medium Level policy	Entry removed
Low Level policy	No effect

1.3.2 /etc/inittab - lpd (Level 2, Scorable)

Description:
The `lpd` daemon accepts remote print jobs from other systems.

Rationale:
If there is not a requirement for the system to act as a remote print server for other servers, remove the `lpd` entry.

Remediation:
In `/etc/inittab`, remove the `lpd` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmitab lpd
```

Audit:
From the command prompt, execute the following command:

```
lsitab lpd
```

The above command should not yield output

Reversion:
If there is a requirement to allow remote print queues on the system, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>lpd: /etc/inittab : d dislpdhls </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>lpd: /etc/inittab : d dislpdhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs> lpd: /etc/inittab : d hls_dislpd</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> lpd: /etc/inittab : d hls_dislpd</AIXPertArgs> -->
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	Entry removed
Medium Level policy	Entry removed
Low Level policy	No effect

1.3.3 /etc/inittab - piobe (Level 2, Scorable)

Description:
This daemon is the I/O back end for the printing process, handling the job scheduling and spooling.

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmitab piobe
```

Audit:
From the command prompt, execute the following command:

```
lsitab piobe
```

The above command should yield not yield output

Reversion:
If there is a requirement to implement print queues on the system, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>piobe: /etc/inittab : d dispiobehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>piobe: /etc/inittab : d dispiobehls</AIXPertArgs -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>piobe: /etc/inittab : d hls_dispiobe</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>piobe: /etc/inittab : d hls_dispiobe</AIXPertArgs -->
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	Entry removed
Medium Level policy	Entry removed
Low Level policy	No effect

1.3.4 /etc/inittab – dt (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmitab dt
```

Audit:
From the command prompt, execute the following command:

```
lsitab dt
```

The above command should yield not yield output

Reversion:
No reversion is required if an `lft` is attached, it will not be disabled.

If there is a requirement to run CDE, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>"dt:" "/etc/inittab" ":" d discdehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"dt:" "/etc/inittab" ":" d discdehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs> >"dt:" "/etc/inittab" ":" d hls_discde</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"dt:" "/etc/inittab" ":" d hls_discde</AIXPertArgs> -->
```

Default Value: Uncommented (if an `lft` is present)

Default AIX Security Expert policy values:

High Level policy	Entry removed (if an `lft` is not present)
Medium Level policy	Entry removed (if an `lft` is not present)
Low Level policy	No effect

1.3.5 /etc/inittab - rcnfs (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmitab rcnfs
```

Audit:
From the command prompt, execute the following command:

```
lsitab rcnfs
```

The above command should yield not yield output

Reversion:
If there is a requirement to run NFS, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>d disablenfshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d disablenfshls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>d hls_disablenfs</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d hls_disablenfs</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	NFS disabled
Medium Level policy	No effect
Low Level policy	No effect

1.3.6 /etc/rc.tcpip – sendmail (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d sendmail
```

Audit:

From the command prompt, execute the following command:

```
grep "start /usr/lib/sendmail" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `sendmail`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>sendmail d dismaildmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>sendmail d dismaildmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>sendmail d hls_dismaildmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>sendmail d hls_dismaildmn</AIXPertArgs> -->
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.7 /etc/rc.tcpip – snmpd (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d snmpd
```

Audit:
From the command prompt, execute the following command:

```
grep "start /usr/sbin/snmpd "$src_running"" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `snmpd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>snmpd d dissnmpdmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>snmpd d dissnmpdmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>snmpd d hls_dissnmpdmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>snmpd d hls_dissnmpdmn</AIXPertArgs> -->
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.8 /etc/rc.tcpip – dhcpcd (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d dhcpcd
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/dhcpcd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `dhcpcd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>dhcpcd d disdhcpclienthls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcpcd d disdhcpclienthls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>dhcpcd d hls_disdhcpclient</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcpcd d hls_disdhcpclient</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.9 /etc/rc.tcpip – dhcprd (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d dhcprd
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/dhcprd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `dhcprd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>dhcprd d disdhcpagenthls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcprd d disdhcpagenthls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>dhcprd d hls_disdhcpagent</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcprd d hls_disdhcpagent</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.10 /etc/rc.tcpip – dhcpsd (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d dhcpsd
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/dhcpsd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `dhcpsd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>dhcpsd d disdhcpservhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcpsd d disdhcpservhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>dhcpsd d hls_disdhcpserv</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dhcpsd d hls_disdhcpserv</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.11 /etc/rc.tcpip – autoconf6 (Level 2, Scorable)

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

Rationale:
`authoconf6` 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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d autoconf6
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/autoconf6" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `autoconf6`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>autoconf6 d disautoconf6hls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>autoconf6 d disautoconf6hls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>autoconf6 d hls_disautoconf6</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>autoconf6 d hls_disautoconf6</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.12 /etc/rc.tcpip – gated (Level 2, Scorable)

Description:
This entry starts the `gated` daemon system startup. This daemon provides gateway routing functions for protocols such as RIP and SNMP.

Rationale:

The `gated` daemon provides gateway routing functions for protocols such as RIP and SNMP. It is recommended that this daemon is disabled, unless the server is functioning as a network router.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d gated
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/gated" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `gated`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>gated d disgateddmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>gated d disgateddmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>gated d hls_disgateddmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>gated d hls_disgateddmn</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	Commented out

1.3.13 /etc/rc.tcpip – mrouted (Level 2, Scorable)

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

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d mrouted
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/mrouted" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `mrouted`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>mrouted d dismrouteddmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>mrouted d dismrouteddmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>mrouted d hls_dismrouteddmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>mrouted d hls_dismrouteddmn</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.14 /etc/rc.tcpip – named (Level 2, Scorable)

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

Rationale:
The `named` daemon is the server for the DNS protocol and controls domain name resolution for its clients. It is recommended that this daemon is disabled, unless the server is functioning as a DNS server.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d named
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/named" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `named`, edit the customized XML file prior to implementing:

AIX 5.3

Replace:

```
<AIXPertArgs>named d disdnsdmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>named d disdnsdmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>named d hls_disdnsdmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>named d hls_disdnsdmn</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.15 /etc/rc.tcpip – routed (Level 2, Scorable)

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

Rationale:
The `routed` daemon manages the network routing tables in the kernel. It is recommended that this daemon is disabled, unless the server is functioning as a network router.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d routed
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/routed" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `routed`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>routed d disrtngdmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>routed d disrtngdmnhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>mrouted d hls_dismrouteddmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>mrouted d hls_dismrouteddmn</AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.16 /etc/rc.tcpip – rwhod (Level 2, Scorable)

Description:
This entry starts the `rwhod` daemon at system startup. This is the remote WHO service.

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d rwhod
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/rwhod" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `rwhod`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>rwhod d disrwhoddmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rwhod d disrwhoddmnhls</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a rwhod
```

AIX 6.1

Replace:

```
<AIXPertArgs>rwhod d hls_disrwhoddmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rwhod d hls_disrwhoddmn</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a rwhod
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out

Medium Level policy	No effect
Low Level policy	No effect

1.3.17 /etc/rc.tcpip – timed (Level 2, Scorable)

Description:
This entry starts the `timed` daemon at system startup. This is old UNIX time service.

Rationale:
The `timed` daemon is the old UNIX time service. You must disable this service and use `xntp`, if time synchronization is required in your environment.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d timed
```

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/timed" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `timed`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>timed d distimedmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>timed d distimedmnhls</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a timed
```

AIX 6.1

Replace:

```
<AIXPertArgs>timed d hls_distimedmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>timed d hls_distimedmn</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a timed
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	Commented out

1.3.18 /etc/rc.tcpip – dpid2 (Level 2, Scorable)

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

Rationale:
The `dpid2` deamon acts as a protocol converter, which enables DPI (SNMP v2) sub-agents, such as `hostmibd`, to talk to a SNMP v1 agent that follows SNMP MUX protocol. Unless the server hosts an SNMP agent, it is recommended that `dpid2` is disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d dpid2
```

Audit:
From the command prompt, execute the following command:

```
grep "dpid2" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `dpid2`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>dipid2 d disdpid2dmnhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dipid2 d disdpid2dmnhls</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a dpid2
```

AIX 6.1

Replace:

```
<AIXPertArgs>dpid2 d hls_disdpid2dmn</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>dpid2 d hls_disdpid2dmn</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a dpid2
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.19 /etc/rc.tcpip – hostmibd (Level 2, Scorable)

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

The `hostmibd` daemon is not managed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

Rationale:

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

The specific MIB variables which are managed by `hostmibd` are defined by RFC 2790. Further details relating to these MIBS can be found in the URL below:

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds2/hostmibd.htm

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d hostmibd
```

Audit:
From the command prompt, execute the following command:

```
grep "hostmibd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `hostmibd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chrctcp -d hostmibd"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chrctcp -d hostmibd"</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a hostmibd
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A

Low Level policy N/A

1.3.20 /etc/rc.tcpip – snmpmibd (Level 2, Scorable)

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

The snmpmibd daemon is not managed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

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

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

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds5/snmpmibd.htm

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d snmpmibd
```

Audit:
From the command prompt, execute the following command:

```
grep "snmpmibd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run snmpmibd, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chrctcp -d snmpmibd"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chrctcp -d snmpmibd"</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a snmpmibd
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.21 /etc/rc.tcpip – aixmibd (Level 2, Scorable)

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

The aixmibd daemon is not a managed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

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

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

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds1/aixmibd.htm

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chrctcp -d aixmibd
```

Audit:
From the command prompt, execute the following command:

```
grep "aixmibd" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `aixmibd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chrctcp -d aixmibd"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chrctcp -d aixmibd"</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a aixmibd
```

Default Value: Uncommented

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.22 /etc/rc.tcpip – ndpd-host (Level 2, Scorable)

Description:
This entry starts `ndpd-host` on system startup. This is the Neighbor Discovery Protocol (NDP) daemon, required in IPv6.

The `ndpd-host` entry is not managed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

Rationale:
The `ndpd-host` is the NDP deamon for the server. Unless the server utilizes IPv6, this is not required and should be disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/ndpd-host" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `ndpd-host`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chrctcp -d ndpd-host"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chrctcp -d ndpd-host"</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a ndpd-host
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.23 /etc/rc.tcpip – ndpd-router (Level 2, Scorable)

Description:
This entry starts `ndpd-router` on system startup. This manages the Neighbor Discovery Protocol (NDP) for non kernel activities, required in IPv6.

The `ndpd-router` entry is not managed within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "/sbin/ndpd-router" /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `ndpd-router`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chrctcp -d ndpd-router"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chrctcp –d ndpd-router"</AIXPertArgs> -->
```

Enable the daemon:

```
chrctcp -a ndpd-router
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.24 /etc/inetd.conf – telnet (Level 2, Scorable)

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

Rationale:
This `telnet` service is used to service remote user connections. This is historically the most commonly used remote access method for UNIX servers. The username and passwords are

passed over the network in clear text and therefore insecurely. Unless required the `telnetd` daemon will be disabled.

Many older legacy systems do not support SSH and still require `telnet` as a protocol for access. If this is not required, it is recommended that telnet is disabled and SSH is used as a replacement authentication mechanism.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "telnet" /etc/inetd.conf
```

The above command should yield the following output:

```
#telnet stream  tcp6    nowait  root    /usr/sbin/telnetd       telnetd -a
```

Reversion:
If there is a requirement to run `telnet`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>telnet tcp d telnethls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>telnet tcp d telnethls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>telnet tcp d hls_telnet</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>telnet tcp d hls_telnet</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.25 /etc/inetd.conf – exec (Level 2, Scorable)

Description:
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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "rexecd" /etc/inetd.conf
```

The above command should yield the following output:

```
#exec    stream  tcp6    nowait  root    /usr/sbin/rexecd        rexecd
```

Reversion:
If there is a requirement to run `exec`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>exec tcp d rexecdhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>exec tcp d rexecdhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>exec tcp d hls_rexecd</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>exec tcp d hls_rexecd</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.26 /etc/inetd.conf – daytime (Level 2, Scorable)

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

Remediation:
In `/etc/inetd.conf`, comment out the `daytime` entries.

Please note the commands below are for information only, as the settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "daytime" /etc/inetd.conf
```

The above command should yield the following output:

```
#daytime         stream  tcp     nowait  root    internal
#daytime         dgram   udp     wait    root    internal
```

Reversion:
If there is a requirement to run `daytime`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>daytime tcp d tcpdaytimehls</AIXPertArgs>
<AIXPertArgs>daytime udp d udpdaytimehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>daytime tcp d tcpdaytimehls</AIXPertArgs> -->
<!-- <AIXPertArgs>daytime udp d udpdaytimehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>daytime tcp d hls_tcpdaytime</</AIXPertArgs>
<AIXPertArgs>daytime udp d hls_udpdaytime</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>daytime tcp d hls_tcpdaytime</</AIXPertArgs> -->
<!-- <AIXPertArgs>daytime udp d hls_udpdaytime</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.27 /etc/inetd.conf – shell (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#shell" /etc/inetd.conf
```

The above command should yield the following output:

```
#shell  stream  tcp6    nowait  root    /usr/sbin/rshd  rshd
```

Reversion:
If there is a requirement to run `shell`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>shell tcp d shellhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>shell tcp d shellhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>shell tcp d hls_shell</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>shell tcp d hls_shell</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	Commented out

1.3.28 /etc/inetd.conf – cmsd (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'cmsd' -p 'sunrpc_udp'
```

Audit:
From the command prompt, execute the following command:

```
grep "cmsd" /etc/inetd.conf
```

The above command should yield the following output:

```
#cmsd   sunrpc_udp      udp     wait    root    /usr/dt/bin/rpc.cmsd cmsd 100068
2-5
```

Reversion:
If there is a requirement to run `cmsd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>cmsd udp d cmsdhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>cmsd udp d cmsdhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>cmsd udp d hls_cmsd</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>cmsd udp d hls_cmsd</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.29 /etc/inetd.conf – ttdbserver (Level 2, Scorable)

Description:
This entry starts the `ttdbserver` service when required. It is not a pre-requisite service for CDE, which is fully functional when it is disabled.

Rationale:
The `ttdbserver` service is the tool-talk database service for CDE. This service runs as root and should be disabled. Unless required the `ttdbserver` service will be disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ttdbserver' -p 'sunrpc_tcp'
```

Audit:
From the command prompt, execute the following command:

```
grep "ttdbserver" /etc/inetd.conf
```

The above command should yield the following output:

```
#ttdbserver     sunrpc_tcp      tcp     wait    root
/usr/dt/bin/rpc.ttdbserver rpc.ttdbserver 100083 1
```

Reversion:
If there is a requirement to run `ttdbserver`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>ttdbserver tcp d ttdbserverhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ttdbserver tcp d ttdbserverhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>ttdbserver tcp d hls_ttdbserver</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ttdbserver tcp d hls_ttdbserver</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.30 /etc/inetd.conf – uucp (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "uucp" /etc/inetd.conf
```

The above command should yield the following output:

```
#uucp    stream  tcp     nowait  root    /usr/sbin/uucpd uucpd
```

Reversion:
If there is a requirement to run `uucp`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>uucp tcp d uucphls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>uucp tcp d uucphls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>uucp tcp d hls_uucp</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>uucp tcp d hls_uucp</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.31 /etc/inetd.conf – time (Level 2, Scorable)

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 use if time synchronization is necessary. Unless required the `time` service will be disabled.

Remediation:

In `/etc/inetd.conf`, comment out the `time` entries.

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#time" /etc/inetd.conf
```

The above command should yield the following output:

```
#time   stream  tcp     nowait  root    internal
#time   dgram   udp     wait    root    internal
```

Reversion:
If there is a requirement to run `time`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>time tcp d tcptimehls</AIXPertArgs>
<AIXPertArgs>time udp d udptimehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>time tcp d tcptimehls</AIXPertArgs> -->
<!-- <AIXPertArgs>time udp d udptimehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>time tcp d hls_tcptime</AIXPertArgs>
<AIXPertArgs>time udp d hls_udptime</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>time tcp d hls_tcptime</AIXPertArgs> -->
<!-- <AIXPertArgs>time udp d hls_udptime</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:
High Level policy Commented out

Medium Level policy	No effect
Low Level policy	No effect

1.3.32 /etc/inetd.conf – login (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'login' -p 'tcp'
```

Audit:
From the command prompt, execute the following command:

```
grep "^#login" /etc/inetd.conf
```

The above command should yield the following output:

```
#login   stream   tcp6    nowait   root    /usr/sbin/rlogind       rlogind
```

Reversion:
If there is a requirement to run `login`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>login tcp d rloginhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>login tcp d rloginhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>login tcp d hls_rlogin</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>login tcp d hls_rlogin</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	No effect

1.3.33 /etc/inetd.conf – talk (Level 2, Scorable)

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#talk" /etc/inetd.conf
```

The above command should yield the following output:

```
#talk    dgram    udp     wait     root     /usr/sbin/talkd talkd
```

Reversion:
If there is a requirement to run `talk`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>talk udp d talkhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>talk udp d talkhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>talk udp d hls_talk</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>talk udp d hls_talk</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	Commented out
Low Level policy	Commented out

1.3.34 /etc/inetd.conf – ntalk (Level 2, Scorable)

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

The `ntalk` service is not a managed parameter within the default AIX Security Expert framework. This parameter is managed as a customized entry in the XML files.

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 `ntalk` service will be disabled

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#ntalk" /etc/inetd.conf
```

The above command should yield the following output:

```
#ntalk  dgram   udp     wait    root    /usr/sbin/talkd talkd
```

Reversion:
If there is a requirement to run `ntalk`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ntalk' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'ntalk' -p 'udp'" -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.35 /etc/inetd.conf – ftp (Level 2, Scorable)

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

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 will be disabled.

Many older legacy systems do not support SSH and still required `ftp` as a service for data copying. If this is not required it is recommended that `ftp` is disabled and `sftp` is used as a replacement file and directory copying mechanism.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#ftp" /etc/inetd.conf
```

The above command should yield the following output:

```
#ftp    stream  tcp6    nowait  root    /usr/sbin/ftpd  ftpd
```

Reversion:
If there is a requirement to run `ftp`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>ftp tcp d ftphls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ftp tcp d ftphls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>ftp tcp d hls_ftp</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ftp tcp d hls_ftp</AIXPertArgs> -->
```

Default Value: Commented in

Default AIX Security Expert policy values:

High Level policy	Commented out
Medium Level policy	No effect
Low Level policy	No effect

1.3.36 /etc/inetd.conf – chargen (Level 2, Scorable)

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.

Remediation:
In `/etc/inetd.conf`, comment out the `chargen` entries.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#chargen" /etc/inetd.conf
```

The above command should yield the following output:

```
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
```

Reversion:
If there is a requirement to run `chargen`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p
'udp'" </AIXPertArgs>
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p
'tcp'" </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p
'udp'" </AIXPertArgs> -->
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'chargen' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.37 /etc/inetd.conf – discard (Level 2, Scorable)

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.

Remediation:
In `/etc/inetd.conf`, comment out the `discard` entries.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#discard" /etc/inetd.conf
```

The above command should yield the following output:

```
#discard        stream  tcp     nowait  root    internal
#discard        dgram   udp     wait    root    internal
```

Reversion:
If there is a requirement to run `discard`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p
'udp'" </AIXPertArgs>
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p
'tcp'" </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p
'udp'" </AIXPertArgs> -->
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'discard' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.38 /etc/inetd.conf – dtspc (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'dtspc' -p 'tcp'
```

Audit:
From the command prompt, execute the following command:

```
grep "^#dtspc" /etc/inetd.conf
```

The above command should yield the following output:

```
#dtspcd stream   tcp     nowait   root    /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
```

Reversion:
If there is a requirement to run `dtspc`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'dtspc' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'dtspc' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.39 /etc/inetd.conf – echo (Level 2, Scorable)

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.

Remediation:
In `/etc/inetd.conf`, comment out the `echo` entries.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#echo" /etc/inetd.conf
```

The above command should yield the following output:

```
#echo   stream  tcp     nowait  root    internal
#echo   dgram   udp     wait    root    internal
```

Reversion:
If there is a requirement to run `discard`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p 'udp'"
</AIXPertArgs>
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p
'udp'" </AIXPertArgs> -->
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'echo' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.40 /etc/inetd.conf – pcnfs (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:

From the command prompt, execute the following command:

```
grep "^#pcnfsd" /etc/inetd.conf
```

The above command should yield the following output:

```
#pcnfsd sunrpc_udp      udp     wait    root    /usr/sbin/rpc.pcnfsd    pcnfsd
150001 1-2
```

Reversion:
If there is a requirement to run `pcnfsd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pcnfsd' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pcnfsd' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.41 /etc/inetd.conf – rstatd (Level 2, Scorable)

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

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. This service should be disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#rstatd" /etc/inetd.conf
```

The above command should yield the following output:

```
#rstatd sunrpc_udp      udp     wait    root    /usr/sbin/rpc.rstatd    rstatd
100001 1-3
```

Reversion:
If there is a requirement to run `rstatd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rstatd' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rstatd' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:
High Level policy N/A
Medium Level policy N/A
Low Level policy N/A

1.3.42 /etc/inetd.conf – rusersd (Level 2, Scorable)

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

Rationale:
The `rusersd` service runs as root and provides a list of current users active on a system. An attacker may use this information in a DoS attack. This is not an essential service and should be disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#rusersd" /etc/inetd.conf
```

The above command should yield the following output:

```
#rusersd        sunrpc_udp      udp     wait    root
/usr/lib/netsvc/rusers/rpc.rusersd      rusersd 100002 1-2
```

Reversion:
If there is a requirement to run `rusersd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rusersd' -p
'udp'" </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rusersd' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.43 /etc/inetd.conf – rwalld (Level 2, Scorable)

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 must be disabled unless absolutely necessary. Attackers may use this service to launch DoS attacks.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#rwalld" /etc/inetd.conf
```

The above command should yield the following output:

```
#rwalld sunrpc_udp      udp     wait    root    /usr/lib/netsvc/rwall/rpc.rwalld
rwalld 100008 1
```

Reversion:
If there is a requirement to run `rwalld`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rwalld' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rwalld' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:
High Level policy	N/A
Medium Level policy N/A
Low Level policy	N/A

1.3.44 /etc/inetd.conf – sprayd (Level 2, Scorable)

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 you are not running NFS, as it can be used by attackers in a Distributed Denial of Service (DDoS) attack.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#sprayd" /etc/inetd.conf
```

The above command should yield the following output:

```
#sprayd sunrpc_udp      udp     wait    root    /usr/lib/netsvc/spray/rpc.sprayd
sprayd 100012 1
```

Reversion:
If there is a requirement to run `sprayd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'sprayd' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'sprayd' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.45 /etc/inetd.conf – klogin (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#klogin" /etc/inetd.conf
```

The above command should yield the following output:

```
#klogin stream  tcp     nowait  root    /usr/sbin/krlogind      krlogind
```

Reversion:
If there is a requirement to run `klogin`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'klogin' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'klogin' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.46 /etc/inetd.conf – kshell (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#kshell" /etc/inetd.conf
```

The above command should yield the following output:

```
#kshell stream  tcp     nowait  root    /usr/sbin/krshd krshd
```

Reversion:
If there is a requirement to run `klogin`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'kshell' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'kshell' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.47 /etc/inetd.conf – rquotad (Level 2, Scorable)

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.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#rquotad" /etc/inetd.conf
```

The above command should yield the following output:

```
#rquotad        sunrpc_udp      udp     wait    root    /usr/sbin/rpc.rquotad
rquotad 100011 1
```

Reversion:
If there is a requirement to run `rquotad`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rquotad' -p
'udp'" </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'rquotad' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.48 /etc/inetd.conf – tftp (Level 2, Scorable)

Description:
This entry starts the `tftp` service when required.

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

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsubserver -r inetd -C /etc/inetd.conf -d  -v 'tftp' -p 'udp'
```

Audit:
From the command prompt, execute the following command:

```
grep "^#tftp" /etc/inetd.conf
```

The above command should yield the following output:

```
#tftp   dgram   udp6    SRC     nobody  /usr/sbin/tftpd tftpd -n
```

Reversion:
If there is a requirement to run `tftp`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'tftp' -p 'udp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'tftp' -p
'udp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:
High Level policy N/A
Medium Level policy N/A
Low Level policy N/A

1.3.49 /etc/inetd.conf – imap (Level 2, Scorable)

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.

Remediation:
In `/etc/inetd.conf`, comment out the `imap2` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#imap2" /etc/inetd.conf
```

The above command should yield the following output:

```
#imap2   stream   tcp      nowait   root    /usr/sbin/imapd imapd
```

Reversion:
If there is a requirement to run `imap2`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'imap2' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'imap2' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.50 /etc/inetd.conf – pop3 (Level 2, Scorable)

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.

Remediation:
In `/etc/inetd.conf`, comment out the `pop3` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#pop3" /etc/inetd.conf
```

The above command should yield the following output:

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

Reversion:
If there is a requirement to run `pop3`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pop3' -p 'tcp"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'pop3' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.51 /etc/inetd.conf – fingerd (Level 2, Scorable)

Description:
This entry starts the `fingerd` daemon when required.

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 if it is not required.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#finger" /etc/inetd.conf
```

The above command should yield the following output:

```
#finger stream  tcp     nowait  nobody  /usr/sbin/fingerd     fingerd
```

Reversion:
If there is a requirement to run `fingerd`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'finger' -p 'tcp'"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'finger' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:
High Level policy N/A
Medium Level policy N/A
Low Level policy N/A

1.3.52 /etc/inetd.conf – instsrv (Level 2, Scorable)

Description:
This entry starts the `instsrv` service when required.

Rationale:
The `instsrv` service is part of the Network Installation Tools, used for servicing servers running AIX 3.2. This service should be disabled.

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

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

Audit:
From the command prompt, execute the following command:

```
grep "^#instsrv" /etc/inetd.conf
```

The above command should yield the following output:

```
#instsrv stream tcp     nowait  netinst /u/netinst/bin/instsrv instsrv -r
/tmp/netinstalllog /u/netinst/scripts
```

Reversion:
If there is a requirement to run `instsrv`, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'instsrv' -p
'tcp'" </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chsubserver -r inetd -C /etc/inetd.conf -d  -v 'instsrv' -p
'tcp'" </AIXPertArgs> -->
```

Default Value: Commented out

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.3.53 /etc/inetd.conf – permissions and ownership (Level 1, Scorable)

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.

Remediation:
Set the recommended permissions and ownership to `/etc/inetd.conf`.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chmod u=rw,go=r /etc/inetd.conf
chown root:system /etc/inetd.conf
```

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
```

If there is a requirement to leave the current ownership and permissions in place, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs> "chmod 644 /etc/inetd.conf; chown root:system /etc/inetd.conf"
</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> "chmod 644 /etc/inetd.conf; chown root:system
/etc/inetd.conf" </AIXPertArgs> -->
```

Default Value: 644, root:system

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.4 AIX Security Expert – Disabling Remote Services

This section provides guidance on the local disablement of remote system services. In the previous section, recommendations were made to disable the remote services in `/etc/inetd.conf`. This stops the server from accepting connections, but the binaries to initiate remote connections from the server to another host should also be restricted along with the daemons themselves being fully disabled. There are also many known security vulnerabilities that relate to these services, they are a primary target for any DoS attack.

It is recommended that, unless otherwise required, that the following services and daemons will have their execute permissions removed:

```
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/sbin/rlogind
/usr/sbin/rshd
```

1.4.1 Remote command lockdown (Level 2, Scorable)

Description:

Removes all permissions from the remote service commands: `rsh`, `rlogin` and `rcp`.

Rationale:

This effectively disables the following commands, for all users:

```
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
```

These remote services send usernames and passwords in clear text and should not be used. Unless required these binaries will be disabled for all users. The SSH suite of commands should be utilized to provide equivalent functionality.

Remediation:
Use the `chmod` command to remove all permissions on the remote services.

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chmod ugo= /usr/bin/rcp
chmod ugo= /usr/bin/rlogin
chmod ugo= /usr/bin/rsh
```

Audit:
From the command prompt, execute the following commands:

```
ls –l /usr/bin/rcp | awk '{print $1}'
ls –l /usr/bin/rlogin | awk '{print $1}'
ls -l /usr/bin/rsh | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
----------
```

Reversion:
If there is a requirement to run any of these services, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>d disrmtcmdshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d disrmtcmdshls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>d hls_disrmtcmds</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d hls_disrmtcmds</AIXPertArgs> -->
```

If there is a requirement to just revert one or more services, implement the customized AIX Security Expert XML file and execute the relevant command/s:

```
chmod ugo=rx,u+s /usr/bin/rcp
chmod ugo=rx,u+s /usr/bin/rlogin
chmod ugo=rx,u+s /usr/bin/rsh
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	Permissions removed
Medium Level policy	No effect
Low Level policy	No effect

1.4.2 Remote daemon lockdown (Level 2, Scorable)

Description:
Removes all permissions from the remote service daemons: `rshd`, and `rlogind`.

Rationale:
This effectively disables the following daemons, for all users:

```
/usr/sbin/rlogind
/usr/sbin/rshd
/usr/sbin/tftpd
```

These remote services both send and receive usernames and passwords in clear text and should not be used. Unless required these daemons will be disabled for all users.

Remediation:
Use the `chmod` command to remove all permissions on the remote daemons.

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chmod ugo= /usr/sbin/rlogind
chmod ugo= /usr/sbin/rshd
chmod ugo= /usr/sbin/tftpd
```

Audit:
From the command prompt, execute the following commands:

```
ls -l /usr/sbin/rlogind | awk '{print $1}'
ls -l /usr/sbin/rshd | awk '{print $1}'
ls -l /usr/sbin/tftpd | awk '{print $1}'
```

Each of the above commands should return with the following permissions:

```
----------
```

Reversion:
If there is a requirement to run any of these services, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>d disrmtdmnshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d disrmtdmnshls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>d hls_disrmtdmns</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>d hls_disrmtdmns</AIXPertArgs> -->
```

If there is a requirement to just revert one or more daemons, implement the customized AIX Security Expert XML file and execute the relevant command/s:

```
chmod ug=rx,o=r /usr/sbin/rlogind
chmod ug=rx,o=r /usr/sbin/rshd
chmod ug=rx,o=r /usr/sbin/tftpd
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	Permissions removed
Medium Level policy	No effect
Low Level policy	No effect

1.5 AIX Security Expert – Automated Authentication

This section provides guidance on the removal of `.nertrc, .rhosts` files and `/etc/hosts.equiv` entries. The existence of these files could allow remote access to the system without user or password authentication. It is recommended, that unless otherwise required, any such files are removed from all home directories on the system.

1.5.1 Removal of .rhosts and .netrc files (Level 2, Scorable)

Description:
This process removes all instances of `.rhosts` and `.netrc` files.

Rationale:
The `.rhosts` and `.netrc` files can be used to circumvent normal login or change control procedures. The existence of such files, with the relevant entries, can allow remote user access to a system bypassing local user and password authentication. Unless required these files will be removed from all user home directories.

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

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
find / -name ".netrc" -exec rm {} \;
find / -name ".rhosts" -exec rm {} \;
```

Audit:
From the command prompt, execute the following commands:

```
find / -name ".netrc" -print
find / -name ".rhosts" -print
```

The above commands should not yield output

Reversion:
If there is a requirement to implement `.nertrc` and `.rhosts` files, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>h rmrhostsnetrchls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h rmrhostsnetrchls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>h hls_rmrhostsnetrc</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h hls_rmrhostsnetrc</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	All files removed from all home directories
Medium Level policy	All files removed from all home directories
Low Level policy	All files removed from root home directory only

1.5.2 Removal of entries from /etc/hosts.equiv (Level 2, Scorable)

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.

Remediation:
Remove all entries from the `/etc/hosts.equiv` file.

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
sed -i '/^\s*$/d; s/^\(\s*[^#].*\)/#\1/' /etc/hosts.equiv
```

Note: the above command removes blank lines and comments out any non comments entries.

Audit:
From the command prompt, execute the following command:

```
grep -v "^\s*#" /etc/hosts.equiv
```

The above command should not yield output

Reversion:
If there is a requirement to have entries in this file, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>rmetchostsequivhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rmetchostsequivhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>hls_rmetchostsequiv</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>hls_rmetchostsequiv</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	Remove all entries from `/etc/hosts.equiv`
Medium Level policy	Remove all entries from `/etc/hosts.equiv`
Low Level policy	Remove all entries from `/etc/hosts.equiv`

1.6 AIX Security Expert – TCP/IP Hardening

This section of the benchmark will focus on the hardening of standard TCP/IP tuning parameters. This is particularly important for the security of the system as the risk of SYN, source routing and smurf attacks can all be significantly reduced or eliminated by following the recommendations in this section. It is anticipated that any firewalls will also be configured to safeguard against these types of attack.

1.6.1 TCP/IP Tuning - ipsrcrouteforward (Level 2, Scorable)

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.

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcrouteforward` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipsrcrouteforward=0
```

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

Audit:

```
grep "ipsrcrouteforward" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipsrcrouteforward = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>ipsrcrouteforward=0 s ipsrcrouteforwardhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcrouteforward=0 s ipsrcrouteforwardhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>ipsrcrouteforward=0 s hls_ipsrcrouteforward</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcrouteforward=0 s hls_ipsrcrouteforward</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	No effect

1.6.2 TCP/IP Tuning - ipignoreredirects (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `ipignoreredirects` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipignoreredirects=1
```

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

Audit:

```
grep "ipignoreredirects" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipignoreredirects = "1"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>ipignoreredirects=1 s ipignoreredirectshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipignoreredirects=1 s ipignoreredirectshls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>ipignoreredirects=1 s hls_ipignoreredirects</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipignoreredirects=1 s hls_ipignoreredirects</AIXPertArgs> -->
```

Default Value: 0

Default AIX Security Expert policy values:

High Level policy	1
Medium Level policy	0
Low Level policy	No effect

1.6.3 TCP/IP Tuning - clean_partial_conns (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `clean_partial_conns` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o clean_partial_conns=1
```

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

Audit:

```
grep "clean_partial_conns" /etc/tunables/nextboot
```

The above command should yield the following output:

```
clean_partial_conns = "1"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>clean_partial_conns=1 s clean_partial_connshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>clean_partial_conns=1 s clean_partial_connshls </AIXPertArgs>
-->
```

AIX 6.1

Replace:

```
<AIXPertArgs>clean_partial_conns=1 s hls_clean_partial_conns</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>clean_partial_conns=1 s hls_clean_partial_conns</AIXPertArgs>
-->
```

Default Value: 0

Default AIX Security Expert policy values:

High Level policy	1
Medium Level policy	1
Low Level policy	1

1.6.4 TCP/IP Tuning - ipsrcroutesend (Level 2, Scorable)

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.

Remediation:

In `/etc/tunables/nextboot`, add the `ipsrcroutesend` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipsrcroutesend=0
```

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

Audit:

```
grep "ipsrcroutesend" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipsrcroutesend = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>ipsrcroutesend=0 s ipsrcroutesendhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcroutesend=0 s ipsrcroutesendhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>ipsrcroutesend=0 s hls_ipsrcroutesend</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcroutesend=0 s hls_ipsrcroutesend</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	1
Low Level policy	1

1.6.5 TCP/IP Tuning - ipforwarding (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `ipforwarding` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipforwarding=0
```

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

Audit:

```
grep "ipforwarding" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipforwarding = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>ipforwarding=0 s ipforwardinghls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipforwarding=0 s ipforwardinghls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>ipforwarding=0 s hls_ipforwarding</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipforwarding=0 s hls_ipforwarding</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:
High Level policy 0

Medium Level policy	1
Low Level policy	1

1.6.6 TCP/IP Tuning - ipsendredirects (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `ipsendredirects` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipsendredirects=0
```

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

Audit:

```
grep "ipsendredirects" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipsendredirects = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>ipsendredirects=0 s ipsendredirectshls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsendredirects=0 s ipsendredirectshls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>ipsendredirects=0 s hls_ipsendredirects</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsendredirects=0 s hls_ipsendredirects</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	1
Low Level policy	1

References:

1. CCE-ID TBC

1.6.7 TCP/IP Tuning - ip6srcrouteforward (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `ip6srcrouteforward` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ip6srcrouteforward=0
```

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

Audit:

```
grep "ip6srcrouteforward" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ip6srcrouteforward = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>ip6srcrouteforward=0 s ip6srcrouteforwardhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ip6srcrouteforward=0 s ip6srcrouteforwardhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>ip6srcrouteforward=0 s hls_ip6srcrouteforward </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ip6srcrouteforward=0 s hls_ip6srcrouteforward</AIXPertArgs> --
>
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	1
Low Level policy	1

1.6.8 TCP/IP Tuning – directed_broadcast (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `directed_broadcast` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o directed_broadcast=0
```

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

Audit:

```
grep "directed_broadcast" /etc/tunables/nextboot
```

The above command should yield the following output:

```
directed_broadcast = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>directed_broadcast=0 s directed_broadcasthls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>directed_broadcast=0 s directed_broadcasthls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>directed_broadcast=0 s hls_directed_broadcast</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>directed_broadcast=0 s hls_directed_broadcast</AIXPertArgs> --
>
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	0

1.6.9 TCP/IP Tuning – tcp_pmtu_discover (Level 2, Scorable)

Description:
The tcp_pmtu_discover parameter controls whether TCP MTU discovery is enabled.

Rationale:
The tcp_pmtu_discover parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When tcp_pmtu_discover is enabled, it leaves the system vulnerable to source routing attacks.

Remediation:
In /etc/tunables/nextboot, add the tcp_pmtu_discover entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o tcp_pmtu_discover=0
```

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

Audit:

```
grep "tcp_pmtu_discover" /etc/tunables/nextboot
```

The above command should yield the following output:

```
tcp_pmtu_discover = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>tcp_pmtu_discover=0 s tcp_pmtu_discoverhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_pmtu_discover=0 s tcp_pmtu_discoverhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>tcp_pmtu_discover=0 s hls_tcp_pmtu_discover</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_pmtu_discover=0 s hls_tcp_pmtu_discover</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	0

1.6.10 TCP/IP Tuning – bcastping (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `bcastping` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o bcastping=0
```

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

Audit:

```
grep "bcastping" /etc/tunables/nextboot
```

The above command should yield the following output:

```
bcastping = "0"
```

Reversion:

If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>bcastping=0 s bcastpinghls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>bcastping=0 s bcastpinghls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>bcastping=0 s hls_bcastping</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>bcastping=0 s hls_bcastping</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	0

1.6.11 TCP/IP Tuning – icmpaddressmask (Level 2, Scorable)

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.

Remediation:

In `/etc/tunables/nextboot`, add the `icmpaddressmask` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o icmpaddressmask=0
```

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

Audit:

```
grep "icmpaddressmask" /etc/tunables/nextboot
```

The above command should yield the following output:

```
icmpaddressmask = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>icmpaddressmask=0 s icmpaddressmaskhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>icmpaddressmask=0 s icmpaddressmaskhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>icmpaddressmask=0 s hls_icmpaddressmask</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>icmpaddressmask=0 s hls_icmpaddressmask</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	0

1.6.12 TCP/IP Tuning – udp_pmtu_discover (Level 2, Scorable)

Description:
The `udp_pmtu_discover` parameter controls whether MTU discovery is enabled.

Rationale:
The udp_pmtu_discover parameter will be set to 0. The idea of MTU discovery is to avoid packet fragmentation between remote networks. This is achieved by discovering the network route and utilizing the smallest MTU size within that path when transmitting packets. When udp_pmtu_discover is enabled, it leaves the system vulnerable to source routing attacks.

Remediation:
In /etc/tunables/nextboot, add the udp_pmtu_discover entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o udp_pmtu_discover=0
```

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

Audit:

```
grep "udp_pmtu_discover" /etc/tunables/nextboot
```

The above command should yield the following output:

```
udp_pmtu_discover = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>udp_pmtu_discover=0 s udp_pmtu_discoverhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>udp_pmtu_discover=0 s udp_pmtu_discoverhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>udp_pmtu_discover=0 s hls_udp_pmtu_discover</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>udp_pmtu_discover=0 s hls_udp_pmtu_discover</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	0
Low Level policy	0

1.6.13 TCP/IP Tuning – ipsrcrouterecv (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `ipsrcrouterecv` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o ipsrcrouterecv=0
```

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

Audit:

```
grep "ipsrcrouterecv" /etc/tunables/nextboot
```

The above command should yield the following output:

```
ipsrcrouterecv = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>ipsrcrouterecv=0 s ipsrcrouterecvhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcrouterecv=0 s ipsrcrouterecvhls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>ipsrcrouterecv=0 s hls_ipsrcrouterecv</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>ipsrcrouterecv=0 s hls_ipsrcrouterecv</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	No effect
Low Level policy	No effect

1.6.14 TCP/IP Tuning – nonlocsrcroute (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `nonlocsrcroute` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o nonlocsrcroute=0
```

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

Audit:

```
grep "nonlocsrcroute" /etc/tunables/nextboot
```

The above command should yield the following output:

```
nonlocsrcroute = "0"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>nonlocsrcroute=0 s nonlocsrcroutehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>nonlocsrcroute=0 s nonlocsrcroutehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>nonlocsrcroute=0 s hls_nonlocsrcroute</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>nonlocsrcroute=0 s hls_nonlocsrcroute</AIXPertArgs> -->
```

Default Value: 1

Default AIX Security Expert policy values:

High Level policy	0
Medium Level policy	No effect
Low Level policy	No effect

1.6.15 TCP/IP Tuning –tcp_tcpsecure (Level 2, Scorable)

Description:
The `tcp_tcpsecure` parameter value determines if the system is protected from three specific vulnerabilities:

Fake SYN – This is used to terminate an established connection. A `tcp_tcpsecure` value of `1` protects the system from this vulnerability.

Fake RST – As above, this is used to terminate an established connection. A `tcp_tcpsecure` value of `2` protects the system from this vulnerability.

Fake data – A hacker may inject fake data into an established connection. A `tcp_tcpsecure` value of `4` protects the system from this vulnerability.

The `tcp_tcpsecure` parameter is, by default, only managed within the AIX 6.1 Security Expert framework. The parameter will also be set for AIX 5.3 as it has been added as a customized entry in the XML file.

Rationale:
The `tcp_tcpsecure` parameter will be set to `7`. This means that the system will be protected from any connection reset and data integrity attacks.

Remediation:
In `/etc/tunables/nextboot`, add the `tcp_tcpsecure` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o tcp_tcpsecure=7
```

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

Audit:

```
grep "tcp_tcpsecure" /etc/tunables/nextboot
```

The above command should yield the following output:

```
tcp_tcpsecure = "7"
```

Reversion:
If there is a requirement have this parameter set to the default, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>"no -p -o tcp_tcpsecure=7"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"no -p -o tcp_tcpsecure=7"</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs> tcp_tcpsecure=7 s hls_tcp_tcpsecure </AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_tcpsecure=7 s hls_tcp_tcpsecure</AIXPertArgs> -->
```

Default Value: 0

Default AIX Security Expert policy values:

High Level policy	7
Medium Level policy	7
Low Level policy	5

1.6.16 TCP/IP Tuning – sockthresh (Level 2, Scorable)

Description:
The `sockthresh` parameter value determines what percentage of the total memory allocated to networking, set via `thewall`, can be used for sockets.

`The sockthresh` parameter is, by default, only managed within the AIX 6.1 Security Expert framework. The parameter will also be set for AIX 5.3 as it has been added as a customized entry in the XML file.

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.

Remediation:
In `/etc/tunables/nextboot`, add the `sockthresh` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o sockthresh=60
```

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

Audit:

```
grep "sockthresh" /etc/tunables/nextboot
```

The above command should yield the following output:

```
sockthresh = "60"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>"no -p -o sockthresh=60"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"no -p -o sockthresh=60"</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>sockthresh=60 s hls_sockthresh</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>sockthresh=60 s hls_sockthresh</AIXPertArgs> -->
```

Default Value: No limit

Default AIX Security Expert policy values:

High Level policy	60
Medium Level policy	70
Low Level policy	85

1.6.17 TCP/IP Tuning – rfc1323 (Level 2, Scorable)

Description:
The `rfc1323` parameter determines whether the TCP window sizes (`tcp_sendspace` and `tcp_recvspace`) can be greater than 64KB.

Rationale:
The `rfc1323` parameter will be set to 1. This means that the system will allow the TCP windows sizes to exceed 64KB. This is a requirement for high performance networks, particularly those which utilize large MTU sizes.

Remediation:
In `/etc/tunables/nextboot`, add the `rfc1323` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o rfc1323=1
```

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

Audit:

```
grep "rfc1323" /etc/tunables/nextboot
```

The above command should yield the following output:

```
rfc1323 = "1"
```

Reversion:
If there is a requirement have this parameter enabled, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>rfc1323=1 s rfc1323hls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rfc1323=1 s rfc1323hls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>rfc1323=1 s hls_rfc1323</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rfc1323=1 s hls_rfc1323</AIXPertArgs> -->
```

Default Value: 0

Default AIX Security Expert policy values:

High Level policy	1
Medium Level policy	1
Low Level policy	1

1.6.18 TCP/IP Tuning – tcp_sendspace (Level 2, Scorable)

Description:
The `tcp_sendspace` parameter sets the socket buffer size for sending data. This recommendation changes the default size, but many adapters have specific buffer sizes implemented within the device driver. These are typically 64KB or greater.

Rationale:
The `tcp_sendspace` parameter will be set to 262144. This means that the system default socket buffer size for sending data will be 262KB. This is the minimum recommendation for modern high performance networks.

Remediation:
In `/etc/tunables/nextboot`, add the `tcp_sendspace` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o tcp_sendspace=262144
```

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

Audit:

```
grep "tcp_sendspace" /etc/tunables/nextboot
```

The above command should yield the following output:

```
tcp_sendspace = "262144"
```

Reversion:
If there is a requirement to leave this parameter at the default value, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>tcp_sendspace=262144 s tcp_sendspacehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_sendspace=262144 s tcp_sendspacehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>tcp_sendspace=262144 s hls_tcp_sendspace</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_sendspace=262144 s hls_tcp_sendspace</AIXPertArgs> -->
```

Default Value: 16384

Default AIX Security Expert policy values:

High Level policy	262144
Medium Level policy	262144
Low Level policy	262144

1.6.19 TCP/IP Tuning – tcp_recvspace (Level 2, Scorable)

Description:

The `tcp_recvspace` parameter sets the socket buffer size for receiving data. This recommendation changes the default size, but many adapters have specific buffer sizes implemented within the device driver. These are typically 64KB or greater.

Rationale:

The `tcp_recvspace` parameter will be set to 262144. This means that the system default socket buffer size for receiving data will be 262KB. This is the minimum recommendation for modern high performance networks.

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_recvspace` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o tcp_recvspace=262144
```

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

Audit:

```
grep "tcp_recvspace" /etc/tunables/nextboot
```

The above command should yield the following output:

```
tcp_recvspace = "262144"
```

Reversion:

If there is a requirement to leave this parameter at the default value, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>tcp_recvspace=262144 s tcp_recvspacehls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_recvspace=262144 s tcp_recvspacehls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>tcp_recvspace=262144 s hls_tcp_recvspace</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_recvspace=262144 s hls_tcp_recvspace</AIXPertArgs> -->
```

Default Value: 16384

Default AIX Security Expert policy values:

High Level policy	262144
Medium Level policy	262144
Low Level policy	262144

1.6.20 TCP/IP Tuning – tcp_mssdflt (Level 2, Scorable)

Description:

The `tcp_mssdflt` parameter sets the maximum segment size for communication to a remote network. This parameter is only relevant if MTU discovery is disabled, which is recommended in this benchmark.

Rationale:

The `tcp_mssdflt` parameter will be set to 1448 . This value reflects the packet size minus the TCP/IP headers.

Remediation:

In `/etc/tunables/nextboot`, add the `tcp_mssdflt` entry.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
no -p -o tcp_mssdflt=1448
```

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

Audit:

```
grep "tcp_mssdflt" /etc/tunables/nextboot
```

The above command should yield the following output:

```
tcp_mssdflt = "1448"
```

Reversion:
If there is a requirement to leave this parameter at the default value, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>tcp_mssdflt=1448 s tcp_mssdflthls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_mssdflt=1448 s tcp_mssdflthls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>tcp_mssdflt=1448 s hls_tcp_mssdflt</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>tcp_mssdflt=1448 s hls_tcp_mssdflt</AIXPertArgs> -->
```

Default Value: 1460

Default AIX Security Expert policy values:

High Level policy	1448
Medium Level policy	1448
Low Level policy	1448

1.6.21 TCP/IP Tuning – nfs_use_reserved_ports (Level 2, Scorable)

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.

Remediation:
In `/etc/tunables/nextboot`, add the `portcheck and nfs_use_reserved_ports` entries.

Please note the command below is for information only, as this setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
nfso -p -o portcheck=1
nfso -p -o nfs_use_reserved_ports=1
```

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

Audit:

```
egrep "portcheck|nfs_use_reserved_ports" /etc/tunables/nextboot
```

The above command should yield the following output:

```
portcheck = "1"
nfs_use_reserved_ports = "1"
```

Reversion:
If there is a requirement to leave this parameter at the default value, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"nfso -p -o portcheck=1; nfso -p -o
nfs_use_reserved_ports=1"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"nfso -p -o portcheck=1; nfso -p -o
nfs_use_reserved_ports=1"<AIXPertArgs> -->
```

Default Value: 0

Default AIX Security Expert policy values:
High Level policy N/A
Medium Level policy N/A
Low Level policy N/A

1.7 AIX Security Expert – Miscellaneous Enhancements

This section will detail some of the more generic changes made during the implementation of the customized XML file i.e. those which may not warrant a dedicated section.

These recommendations are the final automated AIX Security Expert changes in this benchmark.

1.7.1 Miscellaneous Enhancements – /.profile PATH (Level 1, Scorable)

Description:
This change removes any "." entries from the root PATH environment variable. This determines whether or not the current working directory is included in the search path.

Rationale:
The "." will be removed from the root `PATH` variable in the relevant files, dependant on the root users shell definition in `/etc/passwd`. This means that any harmful programs, placed in common locations, would never be automatically executed. All directories must be explicitly defined within the PATH variable.

Remediation:
Edit the PATH variable in the `/.profile` (assumes root is using `/bin/ksh` in this example)

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
grep "PATH=" ~root/.profile | egrep ":\.:|:\.$"
```

If the command above yields output, remove the "." entries:

```
vi ~root/.profile
```

Audit:

```
grep "PATH=" ~root/.profile | egrep ":\.:|:\.$"
```

The above command should yield no output.

Reversion:
If there is a requirement to leave the variable at the default level, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>rmdotfrmpathroothls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>rmdotfrmpathroothls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>hls_rmdotfrmpathroot</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>hls_rmdotfrmpathroot</AIXPertArgs> -->
```

Default Value: dot present

Default AIX Security Expert policy values:

High Level policy	dot removed
Medium Level policy	dot removed
Low Level policy	dot removed

1.7.2 Miscellaneous Enhancements – /etc/environment PATH (AIX 5.3 only) (Level 1, Scorable)

Description:
This change removes any "." entries from the PATH environment variable in `/etc/environment`. This determines whether or not the current working directory is included in the search path.

Rationale:
The "." will be removed from the PATH variable in `/etc/environment`. All directories must be explicitly defined within the PATH variable. This removes current working directory searching for all users.

NOTE: This automated functionality is not available in AIX 6.1 `aixpert` implementation.

Remediation:
Edit the PATH variable in `/etc/environment`

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
grep "PATH=" /etc/environment | egrep ":\.:|:\.$"
```

If the command above yields output, remove the "." entries:

```
vi /etc/environment
```

Audit:

```
grep "PATH=" /etc/environment | egrep ":\.:|:\.$"
```

The above command should yield no output.

Reversion:
If there is a requirement to leave the variable at the default level, edit the customized XML file prior to implementing:

AIX 5.3

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
 <AIXPertArgs>r rmdotfrmpathetcenvhls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>r rmdotfrmpathetcenvhls</AIXPertArgs> -->
```

Default Value: dot present

Default AIX Security Expert policy values:

High Level policy	dot removed
Medium Level policy	dot removed
Low Level policy	dot removed

1.7.3 Miscellaneous Enhancements – crontab access (Level 2, Scorable)

Description:
This change creates a `cron.allow` file with a root user entry and removes the `cron.deny` file, if it exists.

Rationale:
This ensures that only the root user has the ability to create a `crontab`. A hacker may exploit use of the `crontab` to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

NOTE: The adm user may also be added, particularly if system accounting is to be implemented.

Remediation:

Create the `/var/adm/cron/cron.allow` file

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
echo "root" > /var/adm/cron/cron.allow
echo "adm" >> /var/adm/cron/cron.allow
```

Audit:

```
grep "root" /var/adm/cron/cron.allow
grep "adm" /var/adm/cron/cron.allow
```

The above command should yield the following output:

```
root
adm
```

Reversion:
If there is a requirement to leave `cron` access at the default level, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
 <AIXPertArgs>h limitsysacchls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h limitsysacchls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
 <AIXPertArgs>h hls_limitsysacc</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h hls_limitsysacc</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	File created
Medium Level policy	No effect

Low Level policy	No effect

1.7.4 Miscellaneous Enhancements – at access (Level 2, Scorable)

Description:
This change creates an `at.allow` file with a root user entry and removes the `at.deny` file, if it exists.

Controlling `at` access is not a managed process within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

Rationale:
This ensures that only the root user has the ability to schedule jobs through the `at` command. A hacker may exploit use of `at` to execute programs or processes automatically. Limiting access to the root account only reduces this risk.

Remediation:
Create the `/var/adm/cron/at.allow` file

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
echo "root" > /var/adm/cron/at.allow
```

Audit:

```
grep "root" /var/adm/cron/at.allow
```

The above command should yield the following output:

```
root
```

Reversion:
If there is a requirement to leave `at` access at the default level, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
 <AIXPertArgs>"echo root > /var/adm/cron/at.allow; rm
/var/adm/cron/at.deny"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"echo root > /var/adm/cron/at.allow; rm
/var/adm/cron/at.deny"</AIXPertArgs> -->
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.7.5 Miscellaneous Enhancements – /etc/ftpusers (Level 1, Scorable)

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.

Remediation:
Add root to the `/etc/ftpusers` file

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
echo "root" >> /etc/ftpusers
```

Audit:

```
grep "root" /etc/ftpusers
```

The above command should yield the following output:

```
root
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	Entry added
Medium Level policy	Entry added
Low Level policy	No effect

1.7.6 Miscellaneous Enhancements – login herald (Level 1, Scorable)

Description:
This change adds a default herald to `/etc/security/login.cfg`.

Rationale:
This change puts into place a suggested login herald to replace the default entry. As the herald is presented to a user prior to logon, it should not provide any information about the operating system or version. Instead, it should detail a company standard acceptable use policy. This herald can be subsequently tailored to reflect a corporate standard policy.

Remediation:
Add a default login herald to `/etc/security/login.cfg`

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/login.cfg -s default -a herald="Unauthorized use of\
 this system is prohibited.\nlogin:"
```

Audit:

```
lssec -f /etc/security/login.cfg -s default -a herald
```

The above command should yield the following output:

```
default herald="Unauthorized use of this system is prohibited.\nlogin:"
```

Default AIX Security Expert policy values:

High Level policy	Herald configured
Medium Level policy	Herald configured
Low Level policy	Herald configured

1.7.7 Miscellaneous Enhancements – guest account removal (Level 1, Scorable)

Description:
This change removes the `guest` user and home directory from the system.

Rationale:
This change removes the `guest` user. If a user logs in with a generic username, audit trails are of limited value as it is not necessarily possible to identify who has accessed an account. The `guest` account should be removed and all users should be given specific logon ids to ensure traceability and accountability.

Remediation:
Remove the `guest` user

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
rmuser -p guest
```

```
rm -r /home/guest
```

Audit:

```
lsuser guest
```

The above command should yield the following output:

```
3004-687 User "guest" does not exist.
```

Default Value: Account exists

Default AIX Security Expert policy values:

High Level policy	Account removed
Medium Level policy	Account removed
Low Level policy	Account removed

1.7.8 Miscellaneous Enhancements – crontab permissions (Level 1, Scorable)

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.

Remediation:
Ensure that all root `crontab` entries are owned and writable by root only.

Please note the commands below are for information only, as these settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
crontab -l |awk '{print $6}' |grep "/"

For each entry:

chown root <PATH to file>
chmod g-w,o-w <PATH to file>
```

Audit:

```
ls -l <PATH to file>
```

Default Value: No effect

Default AIX Security Expert policy values:

High Level policy	Permissions checked
Medium Level policy	Permissions checked
Low Level policy	Permissions checked

1.7.9 Miscellaneous Enhancements – default umask (Level 2, Scorable)

Description:
This changes the default user `umask` in `/etc/security/user`.

Rationale:
The default user `umask` will be set to 027. This means that the default file creation permissions give read and write access to the user, read access to the group and no access to other. The default directory creation permissions give read, write and execute access to the user, read and execute to the group and no access to other. This is the recommended `umask` setting, as world access should be explicitly defined and not added during default creation. Where possible, access to files and directories should be managed via group membership and ACL's, rather than opening up directory structures for world access. In particular, world write access should be avoided.

Consideration should be given to further securing the default user `umask` by implementing 077. This means that only the user has read/write access to the files and directories they create. Group and/or world access would need to be explicitly defined.

As part of this change all explicitly defined `umask` user settings are removed.

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

Please note the command below is for information only, as the setting will be automatically applied when the customized AIX Security Expert XML file is implemented.

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

If a `umask` of 077 is required, reflect the following changes in the AIX Security Expert XML files:

AIX 5.3

Replace:

```
<AIXPertArgs>umask=27 ALL umaskmls</AIXPertArgs>
```

With:

```
<AIXPertArgs>umask=77 ALL umaskmls</AIXPertArgs>
```

AIX 6.1

Replace:

```
<AIXPertArgs> umask=27 ALL hls_umask</AIXPertArgs>
```

With:

```
<AIXPertArgs> umask=77 ALL hls_umask</AIXPertArgs>
```

Audit:
From the command prompt, execute the following command:

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

The above command should yield the following output:

```
default umask=27
```

Reversion:
If there is a requirement to not change the default umask value, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>umask=27 ALL umaskmls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>umask=27 ALL umaskmls</AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs> umask=27 ALL hls_umask</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs> umask=27 ALL hls_umask</AIXPertArgs> -->
```

Default Value: 022

Default AIX Security Expert policy values:

High Level policy	077
Medium Level policy	027
Low Level policy	022

1.7.10 Miscellaneous Enhancements – disabling core dumps (Level 2, Scorable)

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.

Disabling core dumps is not a managed process within the default AIX Security Expert framework. This change is managed as a customized entry in the XML files.

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`.

Remediation:
Change the default user stanza attributes `core` and `core_hard` in `/etc/security/limits` and the set the `fullcore` kernel parameter to `false`.

Please note the commands below are for information only, as the settings will be automatically applied when the customized AIX Security Expert XML file is implemented.

```
chsec -f /etc/security/limits -s default -a core=0 –a core_hard=0
chdev -l sys0 -a fullcore=false
```

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
```

Reversion:

If there is a requirement to enable core dumps, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

Replace:

```
<AIXPertArgs>"chsec -f /etc/security/limits -s default -a core=0 -a core_hard=0;
chdev -l sys0 -a fullcore=false"</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>"chsec -f /etc/security/limits -s default -a core=0 -a
core_hard=0; chdev -l sys0 -a fullcore=false"</AIXPertArgs> -->
```

Default Value: Core dumps enabled

Default AIX Security Expert policy values:

High Level policy	N/A
Medium Level policy	N/A
Low Level policy	N/A

1.7.11 Miscellaneous Enhancements – AIX Auditing (Level 2, Scorable)

Description:
This change configures AIX auditing in bin mode. If auditing is already configured, this enhancement is not implemented.

Rationale:
AIX auditing provides a framework within which to capture pertinent system and security related information, such as failed login attempts, `cron` usage etc. It is recommended that auditing is enabled as part of a group of measures designed to provide enhanced logging of system and security changes.

Further information regarding the setup and management of accounting and auditing can be found in the “Accounting and Auditing for AIX 5L Redbook”:

http://www.redbooks.ibm.com/redbooks/pdfs/sg246396.pdf

Remediation:
Configure AIX auditing in-line with the High Level AIX Security Expert policy.

Please note the commands below are for information only, as the commands will be automatically executed when the customized AIX Security Expert XML file is implemented.

Create a `/audit` filesystem, at least 100 MB in size. The script always creates a standard `jfs` filesystem. If the `/audit` filesystem exists, this step is skipped:

```
mklv -y <LV name> -t jfs -u 1 -c 1 rootvg 1 hdisk0
```

```
crfs -v jfs -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"
```

Audit:
Ensure that the `/audit` filesystem has been created and mounted:

```
df -k /audit
```

The above command should yield the following output:

```
/dev/auditlv        262144    261776    1%         4     1% /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
```

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 echo:

```
audit:2:boot:audit start > /dev/console 2>&1 # Start audit
```

Reversion:
If there is a requirement to not implement auditing, edit the customized XML file prior to implementing:

```
vi /etc/security/aixpert/custom/custom_aix<OS>.xml
```

AIX 5.3

Replace:

```
<AIXPertArgs>h hls_binaudit</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h hls_binaudit/AIXPertArgs> -->
```

AIX 6.1

Replace:

```
<AIXPertArgs>h binaudithls</AIXPertArgs>
```

With:

```
<!-- <AIXPertArgs>h binaudithls</AIXPertArgs> -->
```

Default Value: Auditing not configured

Default AIX Security Expert policy values:

High Level policy	Auditing configured
Medium Level policy	Auditing configured
Low Level policy	Auditing configured

2. Non AIX Security Expert Managed Recommendations

This section of the benchmark will focus on the recommendations which are not automatically applied during the implementation of the AIX Security Expert customized XML file. A number of these recommendations are not scorable, in that the implementation needs to be tailored to suit the needs of a given environment, which also makes compliance checking impossible.

The following recommendations are detailed in this section:

- Configuring syslog
- Secure remote access
- Configuring sendmail
- Configuring CDE
- Configuring NFS
- Configuring SNMP
- TCP Wrappers
- File and directory permissions and ownership
- Privileged command management – Enhanced RBAC and sudo
- Encrypted Filesystem (EFS)
- Trusted Execution
- File Permissions Manager (FPM)

2.1 Configuring 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.

2.1.1 Configuring syslog - local logging (Level 2, Scorable)

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.

Remediation:
Explicitly define a log file for the `auth.info` output in `/etc/syslog.conf`:

```
printf "auth.info\t\t/var/adm/authlog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

NOTE: This ensures that remote login, `sudo` or `su` attempts are logged separately

Create the `authlog` file and make it readable by root only:

```
touch /var/adm/authlog
chown root:system /var/adm/authlog
chmod u=rw,go= /var/adm/authlog
```

Create an entry in `/etc/syslog.conf` to capture all other output of level info or higher, excluding authentication information, as this is to be captured within `/var/adm/authlog`:

```
printf "*.info;auth.none\t/var/adm/syslog rotate time 1w files 4\n" >>
/etc/syslog.conf
```

Create the `syslog` file:

```
touch /var/adm/syslog
chmod u=rw,g=r,o= /var/adm/syslog
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf:`

```
refresh -s syslogd
```

Audit:
Ensure that the log entries have been added successfully:

```
tail -2 /etc/syslog.conf
```

The above command should yield the following output:

```
auth.info                /var/adm/authlog rotate time 1w files 4
*.info;auth.none         /var/adm/syslog rotate time 1w files 4
```

Check that the `authlog` and `syslog` files have been created:

```
ls -l /var/adm/authlog /var/adm/syslog
```

Reversion:
Edit the `/etc/syslog.conf` and the 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
```

Default Value: Not Configured

2.1.2 Configuring syslog – remote logging (Level 2, Scorable)

Description:
This recommendation implements a remote `syslog` configuration.

Rationale:
To further enhance the local `syslog` logging process, it is recommended 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.

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>\n" >> \
/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:

```
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
```

Audit:
Ensure that the log entries have been added successfully:

```
tail -2 /etc/syslog.conf
```

The above command should yield the following output:

```
auth.info               @<IP address of remote syslog server>
*.info;auth.none        @<IP address of remote syslog server>
```

Reversion:
Edit the `/etc/syslog.conf` and the remove the remote `syslog` entries:

```
vi /etc/syslog.conf
```

Remove:

```
auth.info               @<IP address of remote syslog server>
```

```
*.info;auth.none        @<IP address of remote syslog server>
```

Refresh `syslogd` to force the daemon to read the edited `/etc/syslog.conf:`

```
refresh -s syslogd
```

Default Value: Not Configured

2.1.3 Configuring syslog - remote messages (Level 2, Scorable)

Description:
This recommendation prevents the local `syslogd` daemon from accepting messages from other hosts on the network.

Rationale:
Apart from a central `syslog` server, all other hosts should not accept remote `syslog` messages. By default the `syslogd` daemon accepts all remote `syslog` messages as no authentication is required. This means that a hacker could flood a server with `syslog` messages and potentially fill up the `/var` filesystem.

Remediation:
If the server does not act as a central `syslog` server, suppress the logging of messages originating from remote servers:

```
chssys -s syslogd -a "-r"
```

Re-cycle `syslogd` to activate the configuration change`:`

```
stopsrc -s syslogd
startsrc -s syslogd
```

Audit:
Ensure that daemon is running with the newly updated configuration:

```
ps -ef |grep "syslogd"
```

The above command should yield the following output:

```
  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.

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
```

Default Value: Not Configured

2.2 Secure Remote Access

The use of SSH provides a secure and encrypted mechanism for connecting to a UNIX server. The recommendations in this benchmark disable clear text password access methods, such as telnet and rlogin. There are many legacy scenarios where telnet and ftp may still be required, but SSH should not be ignored in these situations and used where ever possible alongside the non-encrypted services. The preferred scenario is that SSH is the only available remote access service.

One of the historical issues relating to the use of OpenSSH was the lack of vendor support for the software. This has now been addressed as it has the full support, and is in fact packaged, by IBM for AIX based on the Open source libraries.

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

2.2.1 Configuring SSH – installation (Level 2, Scorable)

Description:
The recommendation is to install OpenSSH and OpenSSL libraries from the expansion pack media, or the IBM supported packages downloaded from the internet.

Rationale:
This is the preferred mechanism for remote client access as it provides socket level encryption, via OpenSSL. If any clear text password service is required for legacy connections the two services may sit side by side, with SSH utilized wherever possible. Ideally, SSH should be the only available remote access mechanism.

If the software is not available from the expansion pack media, download from the following locations.

OpenSSH:

http://sourceforge.net/projects/openssh-aix/

OpenSSL:

https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=aixbp

NOTE: A login is required to download OpenSSL.

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

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f
openssl,openssh.license,openssh.base,openssh.man.en_US,openssh.msg.en_US -c -N -
g -X -G -Y
```

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

Audit:
Validate the installation of the software:

```
lslpp -L |egrep "openssh|ssl"
```

The above command should yield the following output:

```
  openssh.base.client      4.3.0.5300    C      F    Open Secure Shell Commands
  openssh.base.server      4.3.0.5300    C      F    Open Secure Shell Server
  openssh.license          4.3.0.5300    C      F    Open Secure Shell License
  openssh.msg.en_US        4.3.0.5300    C      F    Open Secure Shell Messages
  openssl.base              0.9.8.601    C      F    Open Secure Socket Layer
  openssl.license           0.9.8.601    C      F    Open Secure Socket License
  openssl.man.en_US         0.9.8.601    C      F    Open Secure Socket Layer
  openssl                    0.9.7g-1    C      R    Secure Sockets Layer and
```

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

Ensure that the SSH daemon is set to automatically start during system IPL:

```
ls -l /etc/rc.d/rc2.d/Ssshd | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r-xr-xr-x   root     system          Ssshd
```

Reversion:
De-install the OpenSSL and OpenSSH software:

```
installp -u openssh* openssl
```

Default Value: Not Installed

2.2.2 Configuring SSH – disabling direct root access (Level 1, Scorable)

Description:

The recommendation is to edit the `/etc/ssh/sshd_config` file to disable direct root login. By default direct root login via SSH is enabled.

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 is extremely insecure and offers little in the way of audit trailing for accountability.

Remediation:
Edit the /`etc/ssh/sshd_config` file and disable direct root login for SSH:

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

Replace:

```
#PermitRootLogin yes
```

With:

```
PermitRootLogin no
```

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

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

Audit:
Ensure that the `PermitRootLogin` parameter has been changed:

```
grep "PermitRootLogin" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitRootLogin no
```

Default Value: PermitRootLogin yes

References:

1. CCE-ID TBC

2.2.3 Configuring SSH – server protocol 2 (Level 1, Scorable)

Description:
The recommendation is to edit the `/etc/ssh/sshd_config` file and allow the SSH2 protocol only. By default the SSH1 protocol is also available. This is the SSH server configuration file.

Rationale:

There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the `/etc/ssh/sshd_config` file and allow the SSH2 protocol only.

Remediation:
Edit the /`etc/ssh/sshd_config` file and explicitly define the SSH2 protocol:

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

Replace:

```
#Protocol 2,1
```

With:

```
Protocol 2
```

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

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

Audit:
Ensure that the `Protocol` parameter has been changed:

```
grep "Protocol" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
Protocol 2
```

Default Value: Both SSH2 and SSH1 protocols are available

2.2.4 Configuring SSH – client protocol 2 (Level 1, Scorable)

Description:
The recommendation is to edit the `/etc/ssh/ssh_config` file and allow the SSH2 protocol only. By default the SSH1 protocol is also available. This is the SSH client configuration file.

Rationale:
There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security

features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the /etc/ssh/ssh_config file and allow the SSH2 protocol only.

Remediation:
Edit the /etc/ssh/ssh_config file and explicitly define the SSH2 protocol:

```
vi /etc/ssh/ssh_config
```

Replace:

```
# Protocol 2,1
```

With:

```
Protocol 2
```

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

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

Audit:
Ensure that the Protocol parameter has been changed:

```
grep "Protocol" /etc/ssh/ssh_config
```

The above command should yield the following output:

```
Protocol 2
```

Default Value: Both SSH2 and SSH1 protocols are available

2.2.5 Configuring SSH – banner configuration (Level 1, Scorable)

Description:
The recommendation is to edit the /etc/ssh/sshd_config file and configure a path to a login herald message.

Rationale:
The login herald configured previously is not displayed during the initiation of a new SSH connection. Prior to a password being entered the user should accept the terms and conditions of the corporate acceptable usage policy.

Remediation:
Create an SSH banner file:

```
printf "Unauthorized use of this system is prohibited.\n" > /etc/ssh/ssh_banner
```

NOTE: The content of the banner file can reflect any internal acceptable usage policy standards

Edit the /`etc/ssh/sshd_config` file and customize the `Banner` parameter:

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

Replace:

```
#Banner /some/path
```

With:

```
Banner /etc/ssh/ssh_banner
```

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

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

Audit:
Ensure that the `Banner` parameter has been changed:

```
grep "Banner" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
Banner /etc/ssh/ssh_banner
```

Default Value: No banner is configured

2.2.6 Configuring SSH – ignore .shosts and .rhosts (Level 1, Scorable)

Description:
The recommendation is to edit the `/etc/ssh/sshd_config` file and set the `IgnoreRhosts` parameter to ignore `.shosts` and `.rhosts` files

Rationale:
A user can logon to a remote system without authenticating themselves if `.rhosts` or `.shosts` files exist in the remote home directory and if the client machine name and user name are present in these files. This method is fundamentally insecure as the local system can be exploited by IP, DNS (Domain Name Server) and routing spoofing attacks. Additionally, this authentication method relies on the integrity of the client machine. These weaknesses have

been known and exploited for a long time. Since this authentication method is not secure, it must be disabled.

Remediation:
Edit the /etc/ssh/sshd_config file to disable the .shosts and .rhosts authentication parameter:

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

Replace:

```
#IgnoreRhosts yes
```

With:

```
IgnoreRhosts yes
```

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

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

Audit:
Ensure that the IgnoreRhosts parameter has been changed:

```
grep "IgnoreRhosts" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
IgnoreRhosts yes
```

Default Value: IgnoreRhosts yes

2.2.7 Configuring SSH – disable null passwords (Level 1, Scorable)

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.

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
```

Audit:
Ensure that the PermitEmptyPasswords parameter has been changed:

```
grep "PermitEmptyPasswords" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
PermitEmptyPasswords no
```

Default Value: PermitEmptyPasswords no

2.2.9 Configuring SSH – disallow host based authentication (Level 2, Scorable)

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

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

Remediation:
Edit the /etc/ssh/sshd_config file to ensure that host based authentication is disallowed:

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

Replace:

```
#HostbasedAuthentication no
```

With:

```
HostbasedAuthentication no
```

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

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

Audit:
Ensure that the `HostbasedAuthentication` parameter has been changed :

```
grep "HostbasedAuthentication" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
HostbasedAuthentication no
```

Reversion:
Revert to the default setting for the `HostBasedAuthentication` parameter:

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

Replace:

```
HostbasedAuthentication no
```

With:

```
# HostbasedAuthentication no
```

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

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

Default Value: HostbasedAuthentication no

2.2.10 Configuring SSH – set privilege separation (Level 1, Scorable)

Description:
The recommendation is to edit the `/etc/ssh/sshd_config` file to ensure that privilege separation is enabled.

Rationale:
Setting privilege separation helps to secure remote `ssh` access. Once a user is authenticated the `sshd` daemon creates a child process which has the privileges of the authenticated user

and this then handles incoming network traffic. The aim of this is to prevent privilege escalation through the initial root process.

Remediation:
Edit the /etc/ssh/sshd_config file to ensure that privilege separation is enabled:

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

Replace:

```
#UsePrivilegeSeparation yes
```

With:

```
UsePrivilegeSeparation yes
```

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

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

Audit:
Ensure that the UsePrivilegeSeparation parameter has been changed:

```
grep "UsePrivilegeSeparation" /etc/ssh/sshd_config
```

The above command should yield the following output:

```
UsePrivilegeSeparation yes
```

Default Value: UsePrivilegeSeparation yes

2.2.11 Configuring SSH – sshd_config permissions lockdown (Level 1, Scorable)

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. The recommended value is not to provide any access rights for any user, other than the owner of the file.

Remediation:
Change the permissions of the /etc/ssh/sshd_config file to ensure that only the owner can read and write to the file:

```
chmod u=rw,go= /etc/ssh/sshd_config
```

Audit:
Ensure that the /`etc/ssh/sshd_config` permissions have been successfully changed:

```
ls -l /etc/ssh/sshd_config | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-------    root      system         /etc/ssh/sshd_config
```

Default Value: 640

2.2.12 Configuring SSH – ssh_config permissions lockdown (Level 1, Scorable)

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 access rights for any user, other than the owner of the file.

Remediation:
Change the permissions of the /`etc/ssh/ssh_config` file to ensure that only the owner can read and write to the file:

```
chmod u=rw,go= /etc/ssh/ssh_config
```

Audit:
Ensure that the /`etc/ssh/ssh_config` permissions have been successfully changed:

```
ls -l /etc/ssh/ssh_config | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-------    root      system         /etc/ssh/ssh_config
```

Default Value: 640

2.2.13 Configuring SSH – removal of .shosts files (Level 2, Scorable)

Description:
The recommendation is to remove any existing `.shosts` files from all user home directories.

Rationale:

The existence of `.shosts` files in a user home directory, combined with the correct SSH parameter can allow passwordless authentication between servers. As previous recommendations in this section disable this authentication method, these files, if they exist, should be removed.

Remediation:
List out all of the existing `.shost` files:

```
find / -name ".shosts" -print
```

Review the list of `.shost` files and remove them individually, or all at once:

Individually:

```
rm (full pathname)
```

All at once:

```
find / -name ".shosts" -exec rm {} \;
```

Audit:
Ensure that the all of the .shost files have been successfully removed:

```
find / -name ".shosts" -print
```

The above command should yield no output.

Reversion:
Any deleted files would need to be restored from a backup.

Default Value: N/A

2.2.14 Configuring SSH – removal of /etc/shosts.equiv (Level 2, Scorable)

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

Rationale:
The existence of `a /etc/shosts.equiv` file, combined with the correct SSH parameter can allow passwordless authentication between servers. As previous recommendations in this section disable this authentication method these files, if they exist, should be removed.

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

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

If the file exists:

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

Audit:
Ensure that the /etc/shosts.equiv file has been successfully removed:

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

The above command should yield no output.

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

Default Value: N/A

2.3 Sendmail Configuration

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

2.3.1 /etc/mail/sendmail.cf – SmtpGreetingMessage (Level 1, Scorable)

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

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

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
```

Change:

```
O SmtpGreetingMessage=$j Sendmail $b
```

To:

```
O SmtpGreetingMessage=mailerready
```

Audit:
Validate the installation of the software：

```
grep -i "SmtpGreetingMessage" /etc/mail/sendmail.cf
```

The above command should yield the following output:

```
O SmtpGreetingMessage=mailerready
```

Reversion:
Copy back the original `/etc/sendmail.cf` file:

```
cp -p /etc/mail/sendmail.cf.pre_cis /etc/mail/sendmail.cf
```

Default Value: SmtpGreetingMessage=$j Sendmail $b

2.3.2 /etc/mail/sendmail.cf – permissions and ownership (Level 1, Scorable)

Description:
The recommended permissions and ownership for `/etc/mail/sendmail.cf` are applied.

Rationale:
The `/etc/mail/sendmail.cf` file is used by the `sendmail` daemon to determine its default configuration. This file must be protected from unauthorized access and modifications.

Remediation:
Set the recommended permissions and ownership to `/etc/mail/sendmail.cf`:

```
chmod u=rw,g=r,o= /etc/mail/sendmail.cf
chown root /etc/mail/sendmail.cf
```

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
```

Default Value: 644, root:system

2.3.3 /var/spool/mqueue – permissions and ownership (Level 1, Scorable)

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

Rationale:
The `sendmail` daemon generally stores its queued mail in the /`var/spool/mqueue` directory. Queued messages are the messages that have not yet reached their final destination. To ensure the integrity of the messages during storage, the mail queue directory must be secured from unauthorized access.

NOTE: It is possible to specify an alternate spool directory in the `/etc/mail/sendmail.cf` file via the `QueueDirectory` parameter.

Remediation:
Set the recommended permissions and ownership to `/var/spool/mqueue`:

```
chmod u=rwx,go= /var/spool/mqueue
chown root /var/spool/mqueue
```

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
```

Default Value: 770, root:system

2.4 Common Desktop Environment (CDE)

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

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

2.4.1 CDE – de-installing CDE (Level 2, Scorable)

Description:

The recommendation is to de-install CDE from the system, assuming that it is not required and is already installed.

Rationale:
The 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.

Remediation:
Identity if CDE is already installed:

```
lslpp -l |grep -i CDE
```

If there are CDE filesets installed – de-install them if CDE is not required.

For each fileset preview the de-installation:

```
installp -up <fileset name>
```

Review the fileset removal preview output, paying particular attention to the other pre-requisites that will also be removed. Typically only `X11.Dt` filesets should be de-installed as pre-requisites.

Once reviewed, de-install the fileset and pre-requisites:

```
installp -ug <fileset name>
```

NOTE: Repeat until all CDE filesets are de-installed

Audit:
Validate the de-installation of the software :

```
lslpp -l |grep -i CDE
```

The above command should yield no output.

Reversion:
Re-install the CDE software from the AIX media.

Default Value: N/A

2.4.2 CDE – disabling dtlogin (Level 2, Scorable)

Description:
Do not start CDE automatically on system boot.

Rationale:
The implementation of the customized aixpert XML file disables CDE if there is not a graphical console attached to the system. If there is a graphical console consider disabling CDE anyway.

Remediation:
Disable CDE start up:

```
/usr/dt/bin/dtconfig -d
```

NOTE: If CDE is not installed the command will not be found

Audit:
Validate the de-installation of the software:

```
lsitab dt
```

The above command should yield no output.

Reversion:
To re-configure the auto-start of the CDE software:

```
/usr/dt/bin/dtconfig -e
```

Default Value: N/A

2.4.3 CDE – sgid/suid binary lockdown (Level 1, Scorable)

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.

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
```

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
```

Default Value: N/A

2.4.4 CDE – remote GUI login disabled (Level 2, Scorable)

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.

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
```

Audit:

Validate the change:

```
grep "Dtlogin.request" Xconfig
```

The command above should yield the following output:

```
Dtlogin.requestPort:        0
```

Reversion:
Comment out the option:

```
vi /etc/dt/config/Xconfig
```

Reflect:

```
#  Dtlogin.requestPort:        0
```

Default Value: Enabled

2.4.5 CDE – screensaver lock (Level 1, Scorable)

Description:
The default timeout is 30 minutes of keyboard and mouse inactivity before a password protected screensaver is invoked by the CDE session manager.

Rationale:
The default timeout of 30 minutes prior to a password protected screensaver being invoked is too long. The recommendation is to set this to 10 minutes to protect from unauthorized access on unattended systems.

Individual users are able to over ride this default setting.

Remediation:
Set the default timeout parameters `dtsession*saverTimeout:` and `dtsession*lockTimeout`:

```
for file in /usr/dt/config/*/sys.resources; do
   dir=`dirname $file | sed -e s/usr/etc/`
   mkdir -p $dir
   echo 'dtsession*saverTimeout: 10' >> $dir/sys.resources
   echo 'dtsession*lockTimeout: 10' >> $dir/sys.resources
done
```

Audit:
Validate the changes to the `sys.resources` files:

```
egrep "dtsession\*saverTimeout:|dtsession\*lockTimeout:"
/etc/dt/config/*/sys.resources
```

The above command should yield a similar output to the following:

```
/usr/dt/config/en_US/sys.resources:dtsession*saverTimeout:  10
/usr/dt/config/en_US/sys.resources:dtsession*lockTimeout:   10
```

Default Value: N/A

2.4.6 CDE – /etc/dt/config/Xconfig permissions and ownership (Level 1, Scorable)

Description:
The `/etc/dt/config/Xconfig` file is used to customize CDE DT login attributes.

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.

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 ugo=r /etc/dt/config/Xconfig
```

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
```

Default Value: N/A

2.4.7 CDE – /etc/dt/config/Xservers permissions and ownership (Level 1, Scorable)

Description:
The `/etc/dt/config/Xservers` contains entries to start the Xserver on the local display.

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.

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 ugo=r /etc/dt/config/Xservers
```

Audit:
Validate the ownership and permissions:

```
ls -l /etc/dt/config/Xservers | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-r--r--r--  root      bin            /etc/dt/config/Xservers
```

Default Value: N/A

2.4.8 CDE – login screen hostname masking (Level 1, Scorable)

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.

Remediation:
Copy the files from `/usr/dt/config/*/Xresources` to `/etc/dt/config/*/Xresources` and add the `Dtlogin*greeting.labelString` and `Dtlogin*greeting.persLabelString` parameters to all copied `Xresources` files:

```
for file in /usr/dt/config/*/Xresources; do
dir=`dirname $file | sed s/usr/etc/`
mkdir -p $dir
if [ ! -f $dir/Xresources ]; then
cp $file $dir/Xresources
fi
WARN="Authorized uses only. All activity may be monitored and
reported."
echo "Dtlogin*greeting.labelString: $WARN" >>$dir/Xresources
echo "Dtlogin*greeting.persLabelString: $WARN" >>$dir/Xresources
done
```

Audit:
Validate the changes to the `Xresources` files:

```
egrep "Dtlogin\*greeting.labelString|Dtlogin\*greeting.persLabelString:"
/etc/dt/config/*/Xresources
```

The above command should yield a similar output to the folllowing:

```
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.labelString: Authorized uses
only. All activity may be monitored and reported.
/usr/dt/config/en_US/Xresources:!! Dtlogin*greeting.persLabelString: Authorized
uses only. All activity may be monitored and reported.
```

Default Value: N/A

2.4.9 CDE – /etc/dt/config//Xresources permissions and ownership (Level 1, Scorable)*

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.

Remediation:
Set the appropriate permissions and ownership on all Xresources files:

```
chown root:sys /etc/dt/config/*/Xresources
chmod u=rw,go=r /etc/dt/config/*/Xresources
```

Audit:
Validate the ownership and permissions:

```
ls -l /etc/dt/config/*/Xresources | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield a similar output to the folllowing:

```
-r--r--r--    root      sys            /etc/dt/config/en_GB/Xresources
-r--r--r--    root      sys            /etc/dt/config/en_US/Xresources
```

Default Value: N/A

2.5 NFS

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

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

2.5.1 NFS – de-install NFS (Level 2, Scorable)

Description:
Remove /etc/exports and de-install NFS.

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.

Remediation:
Ensure that there are no current NFS client mounts:

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

The above commands should yield no output.

De-install the NFS client software:

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

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
```

Audit:
Ensure that the software has been successfully de-installed :

```
lslpp –l |grep -i nfs
```

The above command should yield no output.

Reversion:
Re-install the software from the product DVD's

Default Value: N/A

2.5.2 NFS – nosuid on NFS client mounts (Level 1, Scorable)

Description:
Disable `suid/sgid` program execution within any mounted NFS filesystem.

Rationale:
Setting the `nosuid` option means that on the NFS server the root user cannot make an `suid`-root program within an exported filesystem. Then log onto an NFS client as a standard user and use the `suid`-root program to effectively become root on that client.

Remediation:
For each NFS mount, disable `suid` programs.

List the current NFS mounts:

```
mount |grep "nfs"
```

For each NFS filesystem add the nosuid option, this change should be made via an edit to the `/etc/filesystems` file.

Create a copy of `/etc/filesystems`:

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

For each NFS mount edit the options line to reflect the `nosuid` option:

```
vi /etc/filesystems
```

Reflect in each NFS options line:

```
options          = rw,bg,hard,intr,nosuid,sec=sys
```

NOTE: The above options line is an example, the `nosuid` should be added to the existing options

The NFS mount needs to be re-mounted to reflect this change

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

```
mount |grep "nfs" |wc -l
mount |grep "nfs" |grep "nosuid" |wc -l
```

Both commands should yield the same output.

Default Value: N/A

2.5.3 NFS – localhost removal (Level 1, Scorable)

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 filesytems 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.

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
```

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

```
cat /etc/exports
```

Default Value: N/A

2.5.4 NFS – restrict NFS access (Level 2, Scorable)

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.

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:

```
cat /etc/exports
```

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

```
/usr/spool/mail -access=symmachine
```

If the file is updated, to reflect client access changes, update the current NFS export options:

```
exportfs -a
```

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

```
cat /etc/exports
```

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

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

Default Value: N/A

2.5.5 NFS – no_root_squash option (Level 1, Scorable)

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

Rationale:
Each NFS export on the server should have the `anon=-2` option set. Without this, an NFS export could be at risk, where the remote root user effectively has root access on the NFS mount. By setting the export option `anon=-2` , when the client attempts to access (read, write, or delete) the NFS mount, the server substitutes the UID to the server's nobody account, which is `-2`. This means that the root user on the client cannot access or change files that only root on the server can access or change. It is therefore recommended that `root_squash` is set on all exported filesystems.

The default value of any exported filesystem or directory is `-2,` another value has to be explicitly set.

As a more secure option you can set the option to `anon=-1`, which 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 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.

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

```
smitty chnfsexp
```

For each filesystem, as defined in the F4 list, set the following option:

```
Anonymous UID                                      [-2]
```

NOTE: Press enter to accept the change

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

```
exportfs -a
```

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

```
cat /etc/exports |grep "anon="
```

The above should command should yield no output.

Default Value: -2

2.5.6 NFS – secure NFS (Level 2, Scorable)

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

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

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

```
smitty chnfsexp
```

For each filesystem, as defined in the F4 list. There are five security methods which can be used to define different security access methods for different clients:

```
Security method 1                                    [sys,krb5p,krb5i,krb5,d> +
*     Mode to export directory                          read-write             +
      Hostname list. If exported read-mostly          []
      Hosts & netgroups allowed client access         []
      Hosts allowed root access                       []
```

The 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
```

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

```
cat /etc/exports |grep "sec="
```

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

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

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

Default Value: N/A

2.6 NIS

Network Information Service (NIS) or Yellow Pages (YP), is a client/server directory service protocol used for distributing system configuration data, such as: users, groups, passwords and hosts between computers in a network. This is typically done in larger environments to centralize the management of this data. If the NIS software is installed but not configured, an attacker can cripple a machine by starting NIS. In environments where NIS is utilized, tools like `ypsnarf` allow an attacker to grab the contents of your NIS maps, providing large amounts of information about your site.

The first recommendation in this section is to de-install NIS, if it is installed, to lockdown this service. However, if NIS is used in the environment it is recommended that NIS+ is used instead. NIS+ is structured differently from NIS and supports secure and encrypted RPC, which resolves many of the security issues.

The configuration of NIS+ is not within the scope of this benchmark; however the links below can be used for initial reference:

AIX 5.3:
NIS+ transition

AIX 6.1:
NIS+ transition

2.6.1 NIS – disable NIS client (Level 2, Scorable)

Description:
If NIS is not used in the environment, disable the NIS client and de-install the software.

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

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
```

Audit:
Ensure that the software has been successfully de-installed :

```
lslpp -L bos.net.nis.client
```

The above should command should return a “not found” error.

Reversion:
Re-install the software from the product DVD’s:

Default Value: N/A

2.6.2 NIS – disable NIS server (Level 2, Scorable)

Description:
If NIS is not used in the environment, disable the NIS server and de-install the software.

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

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
```

Audit:
Ensure that the software has been successfully de-installed:

```
lslpp -L bos.net.nis.server
```

The above should command should return a “not found” error.

Reversion:
Re-install the software from the product DVD’s:

Default Value: N/A

2.6.3 NIS – remove NIS markers from password and group files (Level 2, Scorable)

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.

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
```

Audit:
Re-run the command:

```
grep ^+: /etc/passwd /etc/group
```

The command above should yield no output.

Reversion:
Add the + line back to the same point in the file/s:

```
vi /etc/passwd
vi /etc/group
```

Default Value: N/A

2.6.4 NIS – restrict NIS server communication (Level 2, Scorable)

Description:
If NIS must be used in the environment, limit access to the NIS data to specific subnets.

Rationale:
By default the NIS server will authenticate all IP addresses if the `/var/yp/securenets` file does not exist, or exists without any subnets defined. The `/var/yp/securenets` file contains a list of subnets that are considered trusted and are allowed to access NIS data using the `ypserv` and `ypxfrd` daemons. This is a user-created file that resides on a NIS master server and any slave servers. Without configuring this file, anyone with knowledge of the NIS server address and the domain name, can obtain NIS served data, including the contents of the `/etc/passwd` file. Hence, it is recommended that the `/var/yp/securenets` file is configured to restrict access.

Remediation:
Create and secure the `/var/yp/securenets` file (if it does not already exist):

```
touch /var/yp/securenets
chmod u=rw,go= /var/yp/securenets
```

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
```

Audit:
Review the content of the `/var/yp/securenets` file:

```
cat /var/yp/securenets
```

NOTE: A test should be performed from an allowed client and non-allowed subnet to validate the securenets configuration

Reversion:
Remove the `/var/yp/securenets` file:

```
rm /var/yp/securenets
```

Default Value: N/A

2.7 SNMP

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

The Simple Network Management Protocol (SNMP) is a commonly used service that provides network management and monitoring capabilities. SNMP offers the capability to poll networked devices and monitor data such as utilization and errors from various subsystems on the host. SNMP is also capable of changing the configurations on the host, allowing remote management of the system. The protocol uses a community string for authentication from the SNMP client to the SNMP agent on the managed device.

In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but only allow access from `localhost` connections. Nevertheless, a local user may install an SNMP client and modify sensitive variables. If SNMP is required, the community strings must be greater than six characters and include a combination of letters, numbers, and special characters to avoid a brute force attack.

2.7.1 SNMP – disable private community (Level 2, Scorable)

Description:
If `snmpd` is required within the environment, disable the `private` community.

Rationale:
In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from `localhost` connections. As these SNMP names are the default, they must not be used. Any SNMP community name strings should be a combination of letters, numbers and special characters to enhance security.

Remediation:
Create a backup of `/etc/snmpd.conf`:

```
cp -p /etc/snmpd.conf /etc/snmpd.conf.pre_cis
```

Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `private` entry:

```
#community       private 127.0.0.1 255.255.255.255 readWrite
```

Audit:
Ensure the `private` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community" /etc/snmpd.conf.
```

The above command should yield the following output:

```
#community       private 127.0.0.1 255.255.255.255 readWrite
```

Reversion:
Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

Default Value: Commented in

2.7.2 SNMP – disable system community (Level 2, Scorable)

Description:
If `snmpd` is required within the environment, disable the `system` community.

Rationale:
In AIX, two SNMP community names, `private` and `system`, are enabled with read/write privileges, but are allowed access only from `localhost` connections. As these SNMP names are the default, they must not be used. Any SNMP community name strings should be a combination of letters, numbers and special characters to enhance security.

Remediation:
Edit the file:

```
vi /etc/snmpd.conf
```

Comment out the `system` entry:

```
#community       system  127.0.0.1 255.255.255.255 readWrite 1.17.2
```

Audit:
Ensure the `system` entry has been commented out from `/etc/snmpd.conf`:

```
grep "^#community" /etc/snmpd.conf
```

The above command should yield the following output:

```
#community       system  127.0.0.1 255.255.255.255 readWrite 1.17.2
```

Reversion:
Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

Default Value: Commented in

2.7.3 SNMP – restrict public community access (Level 2, Scorable)

Description:
If `snmpd` is required within the environment, implement IP access restrictions to the `public` community.

Rationale:
If SNMP is required, the default `public` community name should be renamed to a more secure combination of letters, numbers and special characters. However, if the public community is required then IP access restrictions should be put into place.

Remediation:
Edit the file:

```
vi /etc/snmpd.conf
```

Implement IP access restrictions to ALL of the available community names:

```
community       public  192.132.10.0 255.255.255.0 readOnly
```

The format of each line should reflect:

```
community community <community name> <IP addresses> <netmask> [ <permissions>
<view>]
```

Audit:
Review the available community IP access control:

```
grep "^community" /etc/snmpd.conf.
```

NOTE: validate the allowed IP address and netmasks

Reversion:
Copy back the original `/etc/snmpd.conf` file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

Default Value: N/A

2.7.4 SNMP – disable Readwrite community (Level 2, Scorable)

Description:
If `snmpd` is required within the environment, disable `readWrite` permissions for all active `community` names.

Rationale:
If SNMP is required, none of the available community names should have `readWrite` permissions defined. This would allow a remote client to query and to set system configuration parameters. SNMP `readWrite` communities must be disabled unless absolutely necessary. If a `readWrite` community is enabled, then access must be granted to only trusted machines in your network. As SNMP uses community names as part of authentication, you must ensure that all community names are greater than six characters and is a mix of characters, numbers, and special characters.

Remediation:
Edit the file:

```
vi /etc/snmpd.conf
```

Replace all instances of:

```
community community <community name> <IP addresses> <netmask> [ readWrite
<view>]
```

With:

```
community community <community name> <IP addresses> <netmask> [ readOnly <view>]
```

Audit:

Review the community lines in /etc/snmpd.conf:

```
grep "^community" /etc/snmpd.conf.
```

NOTE: ensure that there is no readWrite access.

Reversion:
Copy back the original /etc/snmpd.conf file:

```
cp -p /etc/snmpd.conf.pre_cis /etc/snmpd.conf
```

Default Value: N/A

2.8 Securing inetd

During the implementation of the default customized aixpert XML file, the services within /etc/inetd.conf will have been disabled. If all services have been disabled and are not required, the inetd daemon itself can be disabled to further enhance security.

2.8.1 inetd - disabling inetd (Level 2, Scorable)

Description:
If all of services run and managed by inetd are disabled, disable the inetd daemon itself.

Rationale:
If all inetd services are disabled, then there is no need to start the daemon at boot time. An administrator can manually start the inetd service post-IPL, if any of the inetd controlled services are required.

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
```

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

```
grep /usr/sbin/inetd /etc/rc.tcpip
```

The above command should yield the following output:

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

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

```
chrctcp -a inetd
```

Default Value: Commented in

2.9 Portmap Lockdown

The `portmap` deamon 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:

- An NFS client or server
- A NIS (YP) or NIS+ client or server
- Running the CDE GUI
- Running a third-party software application, which is dependent on RPC support

2.9.1 /etc/rc.tcpip - portmap (Level 2, Scorable)

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

Rationale:
If all RPC services are disabled, then there is no need to start the `portmap` daemon at boot time. An administrator can manually start `portmap` post-IPL, if any of the RPC services are required.

Remediation:
Review any active RPC services:

```
rpcinfo -p localhost
```

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

Disable `portmap` if there are no active RPC services:

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

Audit:
Ensure that `portmap` startup has been commented out of `/etc/rc.tcpip`:

```
grep /usr/sbin/portmap /etc/rc.tcpip
```

The above command should yield the following output:

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

Reversion:
Comment in `portmap` startup in `/etc/rc.tcpip`:

```
chrctcp -a portmap
```

Default Value: Commented in

2.10 TCP Wrappers

During the implementation of the default customized aixpert XML file, the services within `/etc/inetd.conf` will have been disabled. However, if some of the services are required, then it is recommended that TCP Wrappers are installed and configured to limit access to these active services.

TCP Wrappers allow the administrator to control who has access to various `inetd` network services via source IP address controls. TCP Wrappers also provide logging information via `syslog` about both successful and unsuccessful connections.

TCP Wrappers are generally triggered via `/etc/inetd.conf`, but other options exist for "wrappering" non-inetd based software.

The configuration of TCP Wrappers to suit a particular environment is outside the scope of this benchmark; however the following links will provide the necessary documentation to plan an appropriate implementation:

TCP Wrappers Home Page

The website contains source code for both IPv4 and IPv6 versions.

2.10.1 TCP Wrappers – installing TCP Wrappers (Level 2, Scorable)

Description:
The recommendation is to install and configure TCP Wrappers if there are active `inetd` controlled services on the system.

Rationale:
TCP Wrappers is a freely available IP packet filtering facility. It provides for greater and more specific control over local network services and the hosts that are allowed to access them. It also makes use of the standard `syslog` facility to track local network use.

Remediation:
Identity any active `inetd` services:

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

If there are any active services, download and install the TCP Wrappers software:

TCP Wrappers is bundled on the AIX media expansion cdrom.

Alternatively, the source code may be downloaded and compiled from:

TCP Wrappers Source Code

NOTE: Ensure that the latest version is downloaded.

The installation example below assumes that the AIX media expansion pack cdrom has been used as the source of the software.

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

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f
netsec.options.tcpwrapper,netsec.options.idprotocol -c -N -g -X -G -Y
```

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

Audit:
Validate the installation of the software :

```
lslpp -L |grep "netsec.options"
```

The above command should yield the following output:

```
netsec.options.idprotocol  1.1.0.0    C     F    Authentication daemon(RFC1413)
netsec.options.tcpwrapper.base
netsec.options.tcpwrapper.license
netsec.options.tcpwrapper.man.en_US
netsec.options.tcpwrapper.msg.en_US
```

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

Reversion:
De-install the TCP Wrappers software:

```
installp -u netsec.options*
```

Default Value: N/A

2.10.2 TCP Wrappers – creating a hosts.deny file (Level 1, Scorable)

Description:
Once TCP Wrappers are installed a `/etc/hosts.deny` file should be created and be configured.

Rationale:
The `/etc/hosts.deny` file describes the names of the hosts which are not allowed to access the local `inetd` services, as decided by the `/usr/sbin/tcpd` server. All access should be denied by default unless explicitly authorized.

Access is granted when a (daemon,client) pair matches an entry in the `/etc/hosts.allow` file. Access is denied when a (daemon,client) pair matches an entry in the `/etc/hosts.deny` file. However, access is granted if matching entry does not exist in both the files. This is why, by default, all access must be denied.

Remediation:
Create a `/etc/hosts.deny` file:

```
touch /etc/hosts.deny
chown root:system /etc/hosts.deny
chmod u=rw,go= /etc/hosts.deny
```

Deny all traffic by default, explicit access will be defined in the `/etc/hosts.allow` file:

```
vi /etc/hosts.deny
```

Add:

```
ALL: ALL
```

Audit:
Validate the content of the `/etc/hosts.deny` file`:`

```
cat /etc/hosts.deny
```

The above command should yield the following output:

```
ALL: ALL
```

Default Value: N/A

2.10.3 TCP Wrappers – creating a hosts.allow file (Level 1, Scorable)

Description:
Once TCP Wrappers are installed a `/etc/hosts.allow` file should be created and be configured.

Rationale:

This file describes the names of the hosts which are allowed to access the local `inetd` services as decided by the `/usr/sbin/tcpd` server. Access is granted when a (daemon,client) pair matches an entry in the `/etc/hosts.allow` file. Access is denied when a (daemon,client) pair matches an entry in the `/etc/hosts.deny` file. However, access is granted if matching entry does not exist in both the files.

Remediation:
Create a `/etc/hosts.allow` file:

```
touch /etc/hosts.allow
chown root:system /etc/hosts.allow
chmod u=rw,go= /etc/hosts.allow
```

Define explicit access to the local `inetd` services:

```
vi /etc/hosts.allow
```

An example configuration:

```
ALL: LOCAL @some_netgroup
ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
```

Audit:
Validate the content of the `/etc/hosts.allow` file`:`

```
cat /etc/hosts.allow
```

The above command should reflect the defined configuration file.

NOTE:- Since the `/etc/hosts.allow` file is processed before `/etc/hosts.deny`, ensure that there are no entries in `/etc/hosts.allow` that may accidentally grant access to a system which are then subsequently denied in `/etc/hosts.deny`.

Default Value: N/A

2.10.4 TCP Wrappers – wrapping inetd services (Level 2, Scorable)

Description:
If TCP Wrappers have been installed because there are active `inetd` services, these services must utilize TCP Wrappers to restrict host access.

Rationale:
By limiting access to the server, you reduce your exposure to threats from attackers on remote systems. Therefore any active `inetd` controlled service which cannot be disabled should be restricted so that it can only be used by trusted hosts.

Remediation:

Prior to implementing this recommendation it is important that hosts.deny and hosts.allow files have been created.

For each active inetd service, change the entry in /etc/inetd.conf, so that tcpd is executed.

Copy the current /etc/inetd.conf file for reversion purposes:

```
cp -p /etc/inetd.conf /etc/inetd.conf.pre_tcp_wrappers
```

For example, to utilize TCP Wrappers on the telnet service:

Edit:

```
vi /etc/inetd.conf
```

Change:

```
telnet stream tcp6 nowait root /usr/sbin/telnetd telnetd
```

To:

```
telnet stream tcp nowait root /usr/sbin/tcpd telnetd
```

Repeat the change for other services.

Audit:
Ensure that the amended service line reflects the tcpd path:

```
grep "service" /etc/inetd.conf |grep "tcpd"
```

The above command should yield output.

Reversion:
Copy back the original /etc/inetd.conf file:

```
cp -p /etc/inetd.conf.pre_tcp_wrappers /etc/inetd.conf
```

Default Value: N/A

2.11 Permissions and Ownership

This section will 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.

2.11.1 Permissions and Ownership – /etc/security (Level 1, Scorable)

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

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

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

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

Audit:
Validate the permissions of `/etc/security`:

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

The above command should yield the following output:

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

Default Value: N/A

2.11.2 Permissions and Ownership – /etc/group (Level 1, Scorable)

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.

Remediation:
Ensure correct ownership and permissions are in place for `/etc/group`:

```
chown root:security /etc/group
chmod u=rw,go=r /etc/group
```

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
```

Default Value: 644

2.11.3 Permissions and Ownership – /etc/passwd (Level 1, Scorable)

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.

Remediation:
Ensure correct ownership and permissions are in place for `/etc/passwd` :

```
chown root:security /etc/passwd
chmod u=rw,go=r /etc/passwd
```

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
```

Default Value: 644

2.11.4 Permissions and Ownership – /etc/security audit (Level 1, Scorable)

Description:
The `/etc/security/audit` directory contains the system audit configuration files.

Rationale:
The `/etc/security/audit` directory stores the audit configuration files. This directory must have adequate access controls to prevent unauthorized access.

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

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

Audit:
Validate the permissions of `/etc/security/audit`:

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

The above command should yield the following output:

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

Default Value: N/A

2.11.5 Permissions and Ownership – /audit (Level 1, Scorable)

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

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

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

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

Audit:
Validate the permissions of `/audit`:

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

The above command should yield the following output:

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

Default Value: N/A

2.11.6 Permissions and Ownership – /smit.log (Level 1, Scorable)

Description:
The`/smit.log` file maintains a history of all `smit` commands run as `root`.

Rationale:
The /smit.log file may contain sensitive information regarding system configuration, which may be of interest to an attacker. This log file must be secured from unauthorized access and modifications.

Remediation:
Remove world read and write access to /smit.log :

```
chmod o-rw /smit.log
```

Audit:
Validate the permissions of /smit.log :

```
ls -l /smit.log | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
-rw-r-----    root     system        /smit.log
```

Default Value: 644

2.11.7 Permissions and Ownership – /var/adm/cron/log (Level 1, Scorable)

Description:
The /var/adm/cron 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.

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

```
chmod o-rw /var/adm/cron/log
```

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----    root     cron         /var/adm/cron/log
```

Default Value: 664

2.11.8 Permissions and Ownership – /var/spool/cron/crontabs (Level 1, Scorable)

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.

Remediation:
Apply the appropriate permissions to `/var/spool/cron/crontabs`:

```
chmod -R o= /var/spool/cron/crontabs
chmod ug=rwx,o= /var/spool/cron/crontabs
chgrp -R cron /var/spool/cron/crontabs
```

Audit:
Validate the permissions of `/var/spool/cron/crontabs`:

```
ls -ld /var/spool/cron/crontabs | awk '{print $1 " " $3 " " $4 " " $9}'
```

The above command should yield the following output:

```
drwxrwx---    root     cron         /var/spool/cron/crontabs
```

Default Value: N/A

2.11.9 Permissions and Ownership – /var/adm/cron/at.allow (Level 1, Scorable)

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.

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
```

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
```

Default Value: N/A

2.11.10 Permissions and Ownership – /var/adm/cron/cron.allow (Level 1, Scorable)

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.

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
```

Audit:
Validate the permissions of `/var/adm/cron/cron.allow:`

```
ls -l /var/adm/cron/cron.allow | awk '{print $1 " " $3 " " $4 " " $9}' theone
```

The above command should yield the following output:

```
-r--------    root     sys         /var/adm/cron/cron.allow
```

Default Value: N/A

2.11.11 Permissions and Ownership – /etc/motd (Level 1, Scorable)

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.

Remediation:
Apply the appropriate permissions to `/etc/motd`:

```
chown bin:bin /etc/motd
chmod u=rw,go=r /etc/motd
```

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
```

Reversion:
Revert to the previous permissions

Default Value: 644

2.11.12 Permissions and Ownership – /var/adm/ras (Level 1, Scorable)

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.

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

```
chmod o-rw /var/adm/ras/*
```

Audit:
Validate the permissions of the files in `/var/adm/ras`:

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

NOTE: The output from the command above will contain numerous files. No files should have read or write permission for other

Default Value: N/A

2.11.13 Permissions and Ownership – /var/ct/RMstart.log (Level 1, Scorable)

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.

Remediation:
Remove world read and write from `/var/ct/RMstart.log`:

```
chmod o-rw /var/ct/RMstart.log
```

Audit:
Validate the permissions of `/var/ct/RMstart.log:`

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

The above command should yield the following output:

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

Default Value: 644

2.11.14 Permissions and Ownership – /var/tmp/dpid2.log (Level 1, Scorable)

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.

As part of the default implementation of the customized XML file, `dpid2` will have been disabled.

Remediation:
Remove world read and write from `/var/tmp/dpid2.log`:

```
chmod o-rw /var/tmp/dpid2.log
```

Audit:
Validate the permissions of `/var/tmp/dpid2.log:`

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

The above command should yield the following output:

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

Default Value: 644

2.11.15 Permissions and Ownership – /var/tmp/hostmibd.log (Level 1, Scorable)

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` logfile can contain network and machine related statistics logged by the daemon. This file must be secured from unauthorized access and modifications.

As part of the default implementation of the customized XML file, `hostmibd` will have been disabled.

Remediation:
Remove world read and write from `/var/tmp/hostmibd.log`:

```
chmod o-rw /var/tmp/hostmibd.log
```

Audit:
Validate the permissions of `/var/tmp/hostmibd.log:`

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

The above command should yield the following output:

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

Default Value: 644

2.11.16 Permissions and Ownership –/var/tmp/snmpd.log (Level 1, Scorable)

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.

As part of the default implementation of the customized XML file, `snmpd` will have been disabled.

Remediation:
Remove world read and write from `/var/tmp/snmpd.log`:

```
chmod o-rw /var/tmp/snmpd.log
```

Audit:
Validate the permissions of `/var/tmp/snmpd.log:`

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

The above command should yield the following output:

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

Default Value: 644

2.11.17 Permissions and Ownership –/var/adm/sa (Level 1, Scorable)

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.

Remediation:
Set the recommended ownership and permissions on `/var/adm/sa`:

```
chown adm:adm /var/adm/sa
chmod u=rwx,go=rx /var/adm/sa
```

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
```

Default Value: N/A

2.11.18 Permissions and Ownership – world writable directory in root PATH (Level 1, Scorable)

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.

Remediation:
Search and report on group or world writable directories in root's PATH. The command must be run as the root user:

```
find `echo $PATH | tr ':' ' '` -type d \( -perm -002 -o -perm -020 \) -ls
```

NOTE: Review the output and manually change the directories, if possible.

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 automate the directory permission changes:

```
find `echo $PATH | tr ':' ' '` -type d  \( -perm -002 -o -perm -020 \) -exec
chmod go-w {} \;
```

Once completed validate the permissions for the main parent directories i.e. `/` and `/usr`

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

This command above should yield the following output:

```
drwxr-xr-x   bin      bin            /usr
drwxr-xr-x   root     system         /
```

Audit:
Re-execute the original `find` command:

```
find `echo $PATH | tr ':' ' '` -type d \( -perm -002 -o -perm -020 \) -ls
```

The above command should yield no output

Default Value: N/A

2.11.19 Permissions and Ownership – home directory configuration files (Level 1, Scorable)

Description:
The user configuration files in each home directory e.g. `$HOME/.profile`, must not be group or world writable.

Rationale:
Group or world-writable user configuration files may enable malicious users to steal or modify other user's data, or to gain elevated privileges.

Remediation:
Search and remediate any user configuration files which have group or world writable access:

```
lsuser -a home ALL |cut -f2 -d= | while read HOMEDIR; do
echo "Examining $HOMEDIR"
if [ -d $HOMEDIR ]; then
ls -a $HOMEDIR | grep -Ev "^.$|^..$" | \
while read FILE; do
if [ -f $FILE ]; then
ls -l $FILE
chmod go-w $FILE
fi
done
else
echo "No home dir for $HOMEDIR"
fi
done
```

NOTE: The permission change is automatically applied

Audit:
Re-execute the remediation script and all listed files in each user directory, should not have group or world writable permissions.

Default Value: N/A

2.11.20 Permissions and Ownership – home directory permissions (Level 1, Scorable)

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

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

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

```
NEW_PERMS=750
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -ge 200 ]; then
HOME=`lsuser -a home $NAME | cut -f 2 -d =`
echo "Changing $NAME homedir $HOME"
chmod $NEW_PERMS $HOME
fi
done
```

NOTE: The permission change is automatically applied to all user directories with a user ID over 200.

Modify `/usr/lib/security/mkuser.sys` to ensure that all new user home directories will be created with a default permission of 750:

```
vi /usr/lib/security/mkuser.sys
```

Replace:

```
mkdir $1
```

With:

```
mkdir $1 && chmod u=rwx,g=rx,g= $1
```

Audit:
Validate the permissions of all of the directories changed:

```
lsuser -c ALL | grep -v ^#name | cut -f1 -d: | while read NAME; do
if [ `lsuser -f $NAME | grep id | cut -f2 -d=` -ge 200 ]; then
HOME=`lsuser -a home $NAME | cut -f 2 -d =`
ls -ld $HOME
fi
done
```

NOTE: All listed directories should have drwxr-x--- permissions

Ensure that the change has been made to /usr/lib/security/mkuser.sys to reflect permissions setting:

```
grep -c 'mkdir $1 && chmod u=rwx,g=rx,g= $1' /usr/lib/security/mkuser.sys
```

NOTE: The output from the command above should be 1

Default Value: N/A

2.12 Miscellaneous Configuration Changes

This section of the benchmark will focus on miscellaneous configuration changes. These are general changes which do not warrant a dedicated section.

2.12.1 Miscellaneous Config – serial port restriction (Level 2, Scorable)

Description:
The recommendation is to disable the login capability of all connected tty devices.

Rationale:
It is recommended that the login capability for all serial ports is disabled, so that unauthorized users cannot attach modems or remote access devices to these ports and bypass any network access control.

If the environment utilizes tty devices to facilitate user connections. This recommendation may be ignored.

Remediation:
Create a list of active tty ports:

```
lsitab -a |grep "on:/usr/sbin/getty"
```

If any tty devices are returned from the previous output, lock down each one via:

```
chitab "tty2:2:off:/usr/sbin/getty /dev/tty2"
```

NOTE: Replace tty2 with the relevant port

Audit:
Ensure that all tty devices are now disabled:

```
lsitab -a |grep "on:/usr/sbin/getty"
```

The above command should yield no output:

Reversion:
Re-enable login for the `tty` port/s:

```
chitab "tty2:2:on:/usr/sbin/getty /dev/tty2"
```

NOTE: Replace `tty2` with the relevant port

Default Value: N/A

2.12.2 Miscellaneous Config – disable i4ls (Level 2, Scorable)

Description:
The recommendation is to disable the `i4ls` license manager. This is typically used for C and Cobol license management.

Rationale:
It is recommended that the `i4ls` license manager is disabled. The license manager is needed for C and Cobol compilers etc. If the environment supports NCS and a license server is required, a node locked license server should be used instead.

Remediation:
Identify if `i4ls` is enabled:

```
lsitab i4ls
```

If the command above yields output, remove via:

```
rmitab i4ls
```

Audit:
Ensure that `i4ls` is now disabled:

```
lsitab i4ls
```

The above command should yield no output.

Reversion:
Re-add the `i4ls` startup line to `/etc/inittab`:

```
mkitab "i4ls:2:wait:/etc/i4ls.rc > /dev/null 2>&1 # Start i4ls"
```

Default Value: N/A

2.12.3 Miscellaneous Config – disable NCS (Level 2, Scorable)

Description:

The recommendation is to disable Network Computing System (NCS). It provide tools for designing, implementing, and supporting applications requiring distributed data and distributed computing.

Rationale:
NCS is an implementation of the Network Computing Architecture developed to provide tools for designing, implementing, and supporting applications requiring distributed data and distributed computing. It is recommended that NCS is disabled, unless it is required within the environment.

Remediation:
Identify if NCS is enabled:

```
lsitab -a |grep "/etc/rc.ncs" | cut -f1 -d:
```

If the command above yields output, remove via:

```
rmitab rcncs
```

NOTE: If the output from the `lsitab` command was not `rcncs`, substitute that above.

Audit:
Ensure that NCS is now disabled:

```
lsitab rcncs
```

NOTE: If the output from the `lsitab` command was not `rcncs`, substitute that above.

The above command should yield no output.

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

```
mkitab "rcncs:2:wait:/etc/rc.ncs > /dev/console 2>&1 #Start NCS"
```

Default Value: N/A

2.12.4 Miscellaneous Config – disable httpdlite (Level 2, Scorable)

Description:
The recommendation is to disable `httpdlite.` This is a web server which provides on-line documentation.

Rationale:
`httpdlite` is the Lite NetQuestion Web server software for online documentation. It is recommended that this software is disabled, unless it is required in the environment.

NOTE: The `man` command does not need this to work correctly.

Remediation:
Identify if `httpdlite` is enabled:

```
lsitab httpdlite
```

If the command above yields output, remove via:

```
rmitab httpdlite
```

Audit:
Ensure that `httpdlite` is now disabled:

```
lsitab httpdlite
```

The above command should yield no output.

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

```
mkitab "httpdlite:2:once:/usr/IMNSearch/httpdlite/httpdlite -r
/etc/IMNSearch/httpdlite/httpdlite.conf & >/dev/console 2>&1"
```

Default Value: N/A

2.12.5 Miscellaneous Config – disable pmd (Level 2, Scorable)

Description:
The recommendation is to disable `pmd`. This is the power management service that turns the machine off if it has been idle for a specific amount of time.

Rationale:
`pmd` is the power management service that turns the machine off if it has been idle for a specific amount of time. This recommendation is to disable this service.

Remediation:
Identify if `pmd` is enabled:

```
lsitab pmd
```

If the command above yields output, remove via:

```
rmitab pmd
```

Audit:
Ensure that `pmd` is now disabled:

```
lsitab pmd
```

The above command should yield no output.

Reversion:
Readd the `pmd` startup line to `/etc/inittab`:

```
mkitab "pmd:2:wait:/usr/bin/pmd > /dev/console 2>&1 # Start PM daemon"
```

Default Value: N/A

2.12.6 Miscellaneous Config – disable writesrv (Level 2, Scorable)

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.

Remediation:
Identify if `writesrv` is enabled:

```
lsitab writesrv
```

If the command above yields output, remove via:

```
rmitab writesrv
```

Audit:
Ensure that `writesrv` is now disabled:

```
lsitab writesrv
```

The above command should yield no output.

Reversion:
Readd the `writesrv` startup line to `/etc/inittab`:

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

Default Value: N/A

2.12.7 Miscellaneous Config – Block talk/write (Level 2, Scorable)

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

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

However, there are two exceptions:

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

Remediation:
Disable `talk` and `write` for ALL shells:

```
echo "mesg n" >> /etc/profile
echo "mesg n" >> /etc/csh.login
```

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

```
grep -c "mesg n" /etc/profile
grep -c "mesg n" /etc/csh.login
```

NOTE: Both commands should return a value of `1`

Reversion:
Remove the mesg entries from `/etc/profile` and `/etc/csh.login`:

```
vi /etc/profile
vi /etc/csh.login
```

Default Value: N/A

2.12.8 Miscellaneous Config – enable sar accounting (Level 2, Scorable)

Description:
The recommendation is to enable `sar` performance accounting. This will provide a normal performance baseline which will help identify unusual performance patterns, created through potential attacks via a password cracking program being executed or through a DoS attack etc.

Rationale:
System accounting gathers periodic baseline system data, such as CPU utilization and disk I/O. Once a normal baseline for the system has been established, unauthorized activities, such as a

password cracking being executed and activity outside of normal usage hours may be detected due to departure from the normal system performance baseline. It is recommended that the collection script is run on an hourly basis, every day, to help to detect any anomalies. It is also important to generate and review the system activity report on a daily basis.

There may be 3rd party tools, or in-house written scripts in place which perform a similar function. In this instance this recommendation can be ignored.

Remediation:
Prior to configuring `sar` reporting, ensure that the `bos.acct` fileset is installed:

```
lslpp -l bos.acct
```

NOTE: The `bos.acct` fileset should be listed, along with the currently installed version

If the software is not installed, install from the relevant AIX media pack:

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp –f bos.acct -c -N -g -X -G -Y
```

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

Edit the `adm` user `crontab`:

```
vi /var/spool/cron/crontabs/adm
```

NOTE: There are commented out example system activity report lines. Review and tailor to the needs of the environment:

```
#=================================================================
#      SYSTEM ACTIVITY REPORTS
#  8am-5pm activity reports every 20 mins during weekdays.
#  activity reports every an hour on Saturday and Sunday.
#  6pm-7am activity reports every an hour during weekdays.
#  Daily summary prepared at 18:05.
#=================================================================
#0 8-17 * * 1-5 /usr/lib/sa/sa1 1200 3 &
#0 * * * 0,6 /usr/lib/sa/sa1 &
#0 18-7 * * 1-5 /usr/lib/sa/sa1 &
#5 18 * * 1-5 /usr/lib/sa/sa2 -s 8:00 -e 18:01 -i 3600 -ubcwyaqvm &
```

NOTE: Change and uncomment the lines where appropriate. Refer to the `sar` documentation for further guidance

Create the reporting directory structure and apply the appropriate permissions:

```
mkdir -p /var/adm/sa
chown adm:adm /var/adm/sa
chmod u=rwx,go=rx /var/adm/sa
```

Audit:
Review the `adm` user `crontab:`

```
cat /var/spool/cron/crontabs/adm
```

The above command should yield output which reflects the changes made in the remediation section.

Reversion:
Comment out the entries in the `adm` user `crontab`:

```
vi /var/spool/cron/crontabs/adm
```

Default Value: N/A

2.12.9 Miscellaneous Config – /etc/ftpusers (Level 2, Scorable)

Description:
The `/etc/ftpusers` is a configuration file used by `ftp` daemon. It contains 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 be added into the file.

As part of the default implementation of the customized XML file the `/etc/ftpusers` file will have already been created with a `root` user entry. It also disables the `ftp` service.

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 users with a UID of less that 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
```

Audit:
Review the content `/etc/ftpusers,` ensure there are no duplicate entries：

```
cat /etc/ftpusers
```

Reversion:
Edit `/etc/ftpusers` and leave only the root entry:

```
vi /etc/ftpusers
```

Default Value: N/A

2.12.10 Miscellaneous Config - ftp umask (Level 1, Scorable)

Description:
The umask of the `ftp` service should be set to at least `027` in order to prevent the FTP daemon process from creating world-writable files by default.

Rationale:
The umask of the `ftp` service should be set to at least `027` in order to prevent the FTP daemon process from creating world-writable files by default. These files could then be transferred over the network which could result in compromise of the critical information.

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

Remediation:
Set the default umask of the `ftp` daemon:

```
chsubserver -c -v ftp -p tcp "ftpd -l -u077"
refresh -s inetd
```

NOTE: The umask above restricts read/write permissions for both group and other

Audit:
Validate the umask setting：

```
grep -i ftp /etc/inetd.conf
```

The above command should yield the following output:

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

Default Value: N/A

2.12.11 Miscellaneous Config – ftp banner (Level 1, Scorable)

Description:
Set an `ftp` login banner which displays the acceptable usage policy.

Rationale:
The message in `banner.msg` is displayed for FTP logins. Banners display necessary warnings to users trying to gain unauthorized access to the system and are required for legal purposes. The recommendation is to set the banner as:

"Authorized uses only. All activity will be monitored and reported".

The content may be changed to reflect any corporate AUP.

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

Remediation:
Ensure that the `bos.msg.en_US.net.tcp.client` fileset 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 `ftp` AUP banner:

```
dspcat -g /usr/lib/nls/msg/en_US/ftpd.cat > /root/ftpd.tmp
sed "s/\"\%s FTP server (\%s) ready.\"/\"\%s Authorized uses only. All activity
may be monitored and reported\"/" /root/ftpd.tmp > /root/ftpd.msg
gencat /usr/lib/nls/msg/en_US/ftpd.cat /root/ftpd.msg
```

Audit:
Open a session to the localhost and validate the banner :

```
telnet localhost
```

The above command should yield the following output:

```
220 localhost Authorized uses only. All activity may be monitored and reported
Name (localhost:root):
```

Default Value: N/A

2.12.12 Miscellaneous Config – /etc/motd (Level 1, Scorable)

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.

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. <p> 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 <p> 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

Audit:
Log back into the system via SSH :

```
ssh localhost
```

NOTE: The `/etc/motd` file will now be displayed

Default Value: N/A

2.12.13 Miscellaneous Config – authorized users in at.allow (Level 1, Scorable)

Description:
The `/var/adm/cron/at.allow` file defines which users on the system are able to schedule jobs via `at.`

Rationale:
The `/var/adm/cron/at.allow` file defines which users are able to schedule jobs via `at`. Review the current `at` files and add any relevant users to the `/var/adm/cron/at.allow` file.

As part of the default implementation of the customized XML file the `/var/adm/cron/at.allow` file will have been created with a `root` user entry.

Remediation:
Review the current `at` files:

```
ls -l /var/spool/cron/atjobs
cat /var/spool/cron/atjobs/*
```

NOTE: Review the list of `at` schedules and remove any files which should not be there, or have no content

Add the recommended system users to the `at.allow` list:

```
echo sys >> /var/adm/cron/at.allow
echo adm >> /var/adm/cron/at.allow
```

Add any other users who require permissions to use the `at` scheduler:

```
echo <user> >> /var/adm/cron/at.allow
```

NOTE: Where <user> is the username

Audit:
Review the content `/var/adm/cron/at.allow,` ensure that the content reflects the changes made`:`

```
cat /var/adm/cron/at.allow
```

Default Value: N/A

2.12.14 Miscellaneous Config – authorized users in cron.allow (Level 1, Scorable)

Description:
The `/var/adm/cron/cron.allow` file defines which users on the system are able to schedule jobs via `cron.`

Rationale:
The `/var/adm/cron/cron.allow` file defines which users are able to schedule jobs via `cron`. Review the current `cron` files and add any relevant users to the `/var/adm/cron/cron.allow` file.

As part of the default implementation of the customized XML file the `/var/adm/cron/at.allow` file will have been created with a `root` user entry.

Remediation:
Review the current `cron` files:

```
ls -l /var/spool/cron/crontabs
cat /var/spool/cron/crontabs/*
```

NOTE: Review the list of `cron` schedules and remove any files which should not be there, or have no content

Add the recommended system users to the `cron.allow` list:

```
echo sys >> /var/adm/cron/cron.allow
echo adm >> /var/adm/cron/cron.allow
```

Add any other users who require permissions to use the `cron` scheduler:

```
echo <user> >> /var/adm/cron/cron.allow
```

NOTE: Where <user> is the username

Audit:
Review the content `/var/adm/cron/cron.allow,` ensure that the content reflects the changes made:

```
cat /var/adm/cron/cron.allow
```

Default Value: N/A

2.12.15 Miscellaneous Config – all unlocked accounts must have a password (Level 1, Scorable)

Description:
All unlocked accounts on the server must have a password.

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.

Remediation:
Check for empty passwords:

```
pwdck -n ALL
```

If the command above yields output, set up a password on the account:

```
passwd <username>
```

Audit:
Re-run the command:

```
pwdck -n ALL
```

The command should not yield output

Default Value: N/A

2.12.16 Miscellaneous Config – All user id must be unique (Level 1, Scorable)

Description:
All users should have a unique UID. In particular the only user on the system to have a UID of 0 should be the root user.

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

Remediation:
Examine the user IDs of all configured users:

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

If a number, or numbers are returned from the command above, these are UID which are not unique within the `/etc/passwd` file. Determine the effected username/s:

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

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

To remove:

```
rmuser <username>
```

To change the UID:

```
chuser id=<id> <username>
```

Audit:
Re-run the command:

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

The command above should not yield output

Default Value: N/A

2.12.17 Miscellaneous Config – All group id must be unique (Level 1, Scorable)

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.

Remediation:
Ensure that all group IDs are unique:

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

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

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

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

To remove:

```
rmgroup <groupname>
```

To change the UID:

```
chgroup id=<id> <groupname>
```

Audit:
Re-run the command:

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

The command above should not yield output

Default Value: N/A

2.12.18 Miscellaneous Config – unnecessary user and group removal (Level 2, Scorable)

Description:
Remove unnecessary administrative user accounts to further enhance security.

Rationale:
Remove unnecessary administrative user accounts and groups, if possible. Generic administrative user accounts are targeted by hackers in an attempt to gain unauthorized access to a server.

Remediation:
Remove the `uucp, nuucp, lpd,` and `printq` user accounts and respective groups, if possible:

```
# Remove users
LIST="uucp nuucp lpd printq"
for USERS in $LIST; do
rmuser -p $USERS
rmgroup $USERS
done

# Remove groups
LIST="uucp printq"
for USERS in $LIST; do
rmgroup $USERS
done
```

NOTE:- Other users and groups can be added to the list if required

Audit:
Ensure that the user accounts have been removed :

```
egrep "uucp|nuucp|lpd|printq" /etc/passwd
```

The command should not yield output

Ensure that the groups have been removed:

```
egrep "uucp|printq" /etc/group
```

The command should not yield output

Reversion:
Re-create the user accounts.

Default Value: N/A

2.12.19 Miscellaneous Config /etc/environment PATH (AIX 6.1 only) (Level 1, Scorable)

Description:
This change removes any "." entries from the PATH environment variable in `/etc/environment`. This determines whether or not the current working directory is included in the search path.

Rationale:
The "." will be removed from the PATH variable in `/etc/environment`. All directories must be explicitly defined within the PATH variable. This removes current working directory searching for all users.

NOTE: This recommendation is automatically applied to AIX 5.3 as part of the default customized AIX Security Expert XML file implementation.

Remediation:
Edit the PATH variable in `/etc/environment` if it contains any "." entries:

```
grep "PATH=" /etc/environment | egrep ":\.:|:\.$"
```

If the command above yields output, remove the "." entries:

```
vi /etc/environment
```

Audit:

```
grep "PATH=" /etc/environment | egrep ":\.:|:\.$"
```

The above command should yield no output.

Default Value: dot not present

2.12.20 Miscellaneous Config /etc/profile PATH (Level 1, Scorable)

Description:
This change removes any "." entries from the PATH environment variable in `/etc/profile`. This determines whether or not the current working directory is included in the search path.

Rationale:
The "." will be removed from the PATH variable in `/etc/profile`. All directories must be explicitly defined within the PATH variable. This removes current working directory searching for all users.

Remediation:

Edit the PATH variable in `/etc/profile` if it contains any "." entries:

```
grep "PATH=" /etc/profile | egrep ":\.:|:\.$"
```

If the command above yields output, remove the "." entries:

```
vi /etc/profile
```

Audit:

```
grep "PATH=" /etc/profile | egrep ":\.:|:\.$"
```

The above command should yield no output.

Default Value: dot not present

2.13 Privileged Command Management

One of the primary causes of system outages is inadvertent or accidental command usage when a user has root privileges. Many users seemingly forget that they are logged in as root, or use inappropriate command arguments. The carte blanche use of the root account should be limited to those individuals who administer the operating system. Users such as database administrators, application support teams and troubleshooters can be given privileged access to the commands they need via tools such as sudo or enhanced RBAC. These tools require careful planning and implementation, but ultimately can eradicate the need for the root password.

This section of the benchmark will detail the recommended methods of managing privileged command access.

2.13.1 PCM - sudo (Level 2, Scorable)

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 limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

If the system is AIX 5.3 based, enhanced RBAC is not an available option. If the system is AIX 6.1 based, 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.

The sudo software is packaged as an RPM by IBM and is available on the AIX Toolbox for LINUX media, or via download from the following location:

http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/download.html

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

```
/usr/lib/instl/sm_inst installp_cmd -a -Q -d /tmp -f sudo -c -N -g -X -G -Y
```

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

Once installed refer to the sudo man page for information regarding the creation of a custom `/etc/sudoers` file. It is recommended that, to reduce rule complexity, privileges are assigned at a group level wherever possible:

http://www.gratisoft.us/sudo/man/sudo.html

NOTE: The configuration of sudo is completely dependant on the unique requirements of a given environment.

All editing of the `/etc/sudoers` file must be performed by the following command:

```
visudo
```

Once the `/etc/sudoers` file has been successfully created, validate the syntax of the file:

```
visudo -c
```

Audit:
Validate the `sudo` installation:

```
rpm -q sudo
```

The above command should yield the following output:

```
sudo-1.6.9p15-2noldap
```

NOTE: The version reflected above may differ from the one installed.

Reversion:
De-install the sudo software:

```
rpm -e sudo
```

Default Value: Not Installed

2.13.2 PCM – enhanced RBAC (AIX 6.1 only) (Level 2, Scorable)

Description:
The recommendation is to configure RBAC to reflect the privileged command access requirements for all users of the system. RBAC is a default component of AIX 6.1.

Rationale:
Privileged command access should be limited to and defined by a user's individual needs. Access to a root command prompt should limited, wherever possible, to minimize the risk of inadvertent or deliberate misuse of the account.

If the system is AIX 6.1 based, 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.

Remediation:
Enhanced RBAC improves on its legacy implementation by allowing greater flexibility around command lists and authorization definitions, which can be customized. The definitions are also saved to a kernel table rather than in flat files, which improves security.

The implementation of RBAC is role based, allowing users to be specifically granted access to the privileged commands they need to perform their day to day tasks. The tool can be used to replace sudo in many instances, or indeed to work alongside it.

A successful implementation may also allow the root account to be deprecated.

The RBAC definition files:

```
/etc/security/privcmds
/etc/security/privfiles
/etc/security/privdevs
```

The command used to list the active RBAC definitions, i.e. those loaded into the kernel:

```
lskst
```

The command used to update RBAC definitions in the kernel table:

```
setkst
```

Further details regarding planning and implementation of RBAC can be found within the IBM AIX 6.1 Infocentre:

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/rbac.htm

NOTE: The configuration of enhanced RBAC is completely dependant on the unique requirements of a given environment.

Audit:
N/A

Default Value: N/A

2.14 Encrypted Filesystems (EFS) (AIX 6.1 only)

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

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

2.14.1 EFS - implementation (AIX 6.1 only) (Level 2, Scorable)

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

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

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

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

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

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

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

Load the CLiC kernel extension:

```
/usr/lib/methods/loadkclic
```

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 6.1 Infocentre:

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/efs_efs.htm

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

Audit:
Validate the installation of the CLiC software :

```
lslpp -L |egrep "clic"
```

The above command should yield the following output:

```
clic.rte.includes        4.3.0.0     C      F      CrytoLite for C Library
                                                   Include File
clic.rte.kernext         4.3.0.0            C      F      CrytpLite 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
```

Reversion:
De-install the CLiC fileset:

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

Decrypt all files:

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

Default Value: N/A

2.15 Trusted Execution (TE) (AIX 6.1 only)

This is a further development of the Trusted Computing Base (TCB) packaged with previous versions of AIX. Unlike TCB, Trusted Execution is not an install time only option and it can be enabled on previously installed systems. Its primary purpose is to protect from Trojan horse style attacks, by only allowing the execution of certain executables and kernel extensions.

TE has two modes of operation, online and offline. The online mode provides the most comprehensive security, as a check is made every time a file is loaded into memory. If the integrity checks fail, the file will not be loaded into memory. The offline mode checks file integrity at a specified time, via either the command line or via crontab.

2.15.1 TE - implementation (AIX 6.1 only) (Level 2, Scorable)

Description:
The recommendation is to implement TE to protect the system from Trojan horse style attacks. TE provides a robust system integrity checking process.

Rationale:
One of the common ways a hacker infiltrates a system is through file tampering or the use of a Trojan horse. The implementation of TE can provide a number of integrity checks prior to loading a program into memory, any deviations can also be highlighted when programs and files are validated offline. This ensures that the programs executed are those which are intended to be and not malicious code masquerading as a true program.

When a discrepancy is identified it is classified as either minor or major. A minor discrepancy is automatically reset to the value defined in the TSD. In the event of a major discrepancy the file access permissions are changed to make the file inaccessible.

There is a pre-requisite requirement to install CLiC and SSL software.

Remediation:
It is recommended that TE is configured in online mode. This provides real time protection against Trojan horse attacks.

The `tsd.dat` file contains the important security attributes relating to all of the managed files:

```
cat /etc/security/tsd/tsd.dat
```

NOTE: The `trustchk` command is used to manage the entries in this file.

To enable TE, firstly enable online checking of executables and shell scripts:

```
trustchk -p CHKEXEC=ON
trustchk -p CHKSCRIPT=ON
```

Stop the execution or loading of binaries and files into memory when the integrity checks fail:

```
trustchk -p STOP_ON_CHKFAIL=ON
```

Enable online TE based on the policy selections above:

```
trustchk -p TE=ON
```

To set a Trusted Execution Path or TEP:

```
trustchk -p TEP=<PATH variable>
```

Enable the TEP:

```
trustchk -p TEP=ON
```

NOTE: Commands will not be executed if they reside outside of the TEP.

Further details regarding planning and implementation of TE can be found within the IBM AIX 6.1 Infocentre:

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/bos_trusted_execution.htm&tocNode=toc:front/front.cmb/0/0/11/0/0/1/

NOTE: The configuration of TE is dependant on the unique requirements of a given environment.

Audit:
Ensure that TE is enabled:

```
trustchk -p TE
```

The above command should yield the following output:

```
TE=ON
```

Ensure that TEP is enabled:

```
trustchk -p TEP
```

The above command should yield the following output:

```
TEP=ON
```

Reversion:
Disable TE:

```
trustchk -p TE=off
```

Disable TEP:

```
trustchk -p TEP=off
```

Default Value: Not enabled

2.16 File Permissions Manager (FPM)

Another enhancement in AIX 6.1 is the introduction of `fpm`, this tool automates the removal of `suid` and `sgid` bits on key system files and daemons. There are three levels of automated removal: low, medium and high and the ability to specify a customized file list based on the environmental requirements.

FPM has also been back ported to AIX 5.3 TL-09 and above. The approach in this section for earlier AIX 5.3 levels is to utilize the `find` command to replicate some of this functionality.

2.16.1 FPM - execution (Level 2, Scorable)

Description:
This change utilizes the `fpm` command to remove `suid` and `sgid` bits from operating system files and daemons**.**

Rationale:
In order to improve on standard AIX security, which utilizes `suid` and `sgid` programs, the `fpm` command can remove these bits automatically. The file input list is dependant on the level of customization chosen: high, medium or low. The command also provides a framework to remediate a customized list of files and daemons.

As the `fpm` command is not available below AIX 5.3 TL-09, the `find` and `chmod` commands will be used to replicate this functionality.

Remediation:
AIX 5.3 TL-09 and above and AIX 6.1:

The `fpm` command will be executed with the high level security file list.

Execute the `fpm` command in preview mode to allow a review of the proposed changes:

```
fpm -l high -p
```

NOTE: The input file list is: `/usr/lib/security/fpm/data/high_fpm_list`

A review of the proposed changes may result in a need to implement sudo or RBAC configuration changes to replicate the `suid` or `sgid` functionality. This would then enable the bits of certain systems files and/or daemons to be removed.

If there is a requirement to remove the suid or sgid bits from custom programs place the list in the `/usr/lib/security/fpm/custom/high` directory.

Execute the `fpm` command to implement the changes:

```
fpm -l high
```

Further details regarding the use of the `fpm` tool can be found within the AIX 6.1 Infocentre:

http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.cmds/doc/aixcmds2/fpm.htm

AIX 5.3 TL-08 and below:

As the `fpm` tool is not available within earlier versions of AIX 5.3, the `find` and `chmod` commands will be used to replicate this functionality.

Find all `suid` and `sgid` files installed on the system. Firstly, ensure that all NFS filesystems and cdrom media are un-mounted:

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

Once the output has been reviewed, use the `chmod` command to remove the appropriate `suid` or `sgid` bits:

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

Audit:
AIX 5.3 TL-09 and above and AIX 6.1:

To ensure file compliance to the high level security policy, validate via:

```
fpm -c -l high
```

NOTE: Any deviation from this standard is reported

AIX 5.3 TL08 and below:

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

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

Reversion:
AIX 5.3 TL-09 and above and AIX 6.1:

When the `fpm` command is executed, a copy of the existing file permissions is made to a corresponding date and time log in `/var/security/fpm/log`. Identify and re-instate the default settings:

```
fpm -l default -f /var/security/fpm/log/<default log>
```

AIX 5.3 TL-08 and below:

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

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

Default Value: N/A

2.16.2 FPM - un-owned and world writable files (Level 2, Scorable)

Description:
This change audits the system for both un-owned and world writable directories and files**.**

Rationale:
The `fpm` functionality is limited to the management of `suid` and `sgid` programs and daemons. There are however, other file and directory based management guidelines that should be adhered too. This recommendation is to audit the system for the presence of un-owned and world writable files and directories.

Remediation:
Check for the presence of world writable files and directories:

```
find / -type f -perm -o+w -exec ls -l {} \;
find / -type d -perm -o+w -exec ls -ld {} \;
```

Review the world writable files and directories and where possible, if the application configuration allows, remove access via:

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

If a directory must retain world writable access, ensure that sticky bit is set so that users can only remove the files they create :

```
chmod o+t <dir>
```

NOTE: This will retain world writable permissions, but add a sticky bit to the directory.

Check for the presence of un-owned files and directories:

```
find / \( -nouser -o -nogroup \) -ls
```

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

Remediate the un-owned file and directory list:

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

Audit:
Re-execute the commands to list the world writable files and directories:

```
find / -type f -perm -o+w -exec ls -l {} \;
find / -type d -perm -o+w -exec ls -ld {} \;
```

NOTE: Review the output based on the performed remediation

Re-execute the command to check for the presence of un-owned files and directories:

```
find / \( -nouser -o -nogroup \) -ls
```

NOTE: Review the output based on the performed remediation

Reversion:
Revert the permissions on the relevant files:

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

Default Value: N/A

3. Final Steps

3.1 System Reboot and Backup

Once all of the customization has been successfully performed, reboot the server to initialize all of the new security settings:

```
shutdown -Fr 0
```

When the system has been successfully rebooted, create a `mksysb` system backup to reflect the new server configuration:

If writing to tape:

```
mksysb -i /dev/rmt<x>
```

If writing to a file:

```
mksysb -i /<pathname to file>
```

NOTE: The `mksysb` can subsequently be used as a source to install new systems, which ensures compliance to this benchmark. If this is intended, it is recommended that a `bosinst_data` resource is created within NIM and that the following parameter is defined:

```
RECOVER_DEVICES = no
```

NOTE: This ensures that no device information stored in the current systems ODM will be recovered on a target system during installation.

Appendix A: References

Resource (date webpage)	Location
IBM AIX Operating System Service Strategy Details and Best Practices Dec 2008 (As of Dec 28th 2008)	http://www14.software.ibm.com/webapp/set2/sas/f/best/home.html
AIX Security Expert Password Policy (AIX 5.3 and AIX 6.1 Infocenter Jan 2009)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_pwd_policy_settings.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_pwd_policy_settings.htm
AIX Security Expert Login Policy (AIX 5.3 and AIX 6.1 Infocenter Jan 2009)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_login_policy_settings.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/topic/com.ibm.aix.security/doc/security/aix_sec_expert_login_policy_settings.htm?tocNode=toc:front/front.cmb/0/0/11/2/10/
AIX Security Expert /etc/inittab Settings (AIX 5.3 and AIX 6.1 Infocenter Jan 2009)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcinittab_entries.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcinittab_entries.htm&tocNode=toc:front/front.cmb/0/0/11/2/12/
AIX Security Expert /etc/rc.tcpip Settings (AIX 5.3 and	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcrctcpi

AIX 6.1 Infocenter Jan 2009)	p_services_settings.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcrctcpip_services_settings.htm&tocNode=toc:front/front.cmb/0/0/11/2/13/
AIX Security Expert /etc/inetd.conf Setting (AIX 5.3 and AIX 6.1 Infocenter Feb 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcinetdconf_settings.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_etcinetdconf_settings.htm&tocNode=toc:front/front.cmb/0/0/11/2/14/
AIX Security Expert Disabling Remote Services (AIX 5.3 and AIX 6.1 Infocenter Feb 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_remov_unnec_services.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_remov_unnec_services.htm&tocNode=toc:front/front.cmb/0/0/11/2/16/
AIX Security Expert Automated Authentication (AIX 5.3 and AIX 6.1 Infocenter Feb 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_removal_nonauth_access.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_removal_nonauth_access.htm&tocNode=toc:front/front.cmb/0/0/11/2/17/
AIX Security Expert TCP/IP Hardening (AIX 5.3 and AIX 6.1 Infocenter Mar 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_tuning_network_opts.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_tuning_network_opts.htm&tocNode=toc:front/front.cmb/0/0/11/2/18/

AIX Security Expert Misc Changes (AIX 5.3 and AIX 6.1 Infocentre Mar 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_misc.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_misc.htm&tocNode=toc: nt/front.cmb/0/0/11/2/20/
AIX Security Expert AIX Audit Policy (AIX 5.3 and AIX 6.1 Infocentre Mar 09)	AIX 5.3: http://publib.boulder.ibm.com/infocenter/pseries/v5r3/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_aud_policy_settings.htm AIX 6.1: http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/com.ibm.aix.security/doc/security/aix_sec_expert_aud_policy_settings.htm&tocNode=toc:front/front.cmb/0/0/11/2/11/
AIX 5L Auditing and Accounting (Redbook) SG24-6396-00	http://www.redbooks.ibm.com/redbooks/pdfs/sg246396.pdf
OpenSSH Configuration	http://www.ibm.com/developerworks/eserver/articles/openssh_updated.html http://www.openssh.org/
AIX 5.3 Differences Guide (Redbook) SG24-7463-00	http://www.redbooks.ibm.com/redbooks/pdfs/sg247463.pdf
AIX 6.1 Differences Guide (Redbook) SG24-7559-00	http://www.redbooks.ibm.com/redbooks/pdfs/sg247559.pdf
AIX 6 Advanced Security Features (Redbook) SG24-7430-00	http://www.redbooks.ibm.com/redbooks/pdfs/sg247430.pdf

Appendix B: Change History

Date	Version	Changes for this version
December 21st, 2010	1.0.0	Initial Release