Global Information Assurance Certification Paper

Securing an AIX 5.2 Development Server

Christopher Talianek
Submitted 05/03/2004

SANS CDI East 2003
Washington DC
GCUX Practical Version 2.0
Option 1: Securing Unix Step by Step

Abstract

The following procedures are a systematic instructional guide to installing and configuring an IBM AIX 5.2 application development server.

The server's primary purpose is to build and package an AIX secure operating system toolkit. IBM provides the Red Hat Package Manager software with AIX version 5.x. Open Source software is readily available for Linux and Solaris distributions, but building and installing on AIX can be a challenge. A properly configured development platform with a baseline of the common security tools enables the administrator to easily build and deploy secure AIX servers.

The process consists of an initial baseline build and the installation of the application development tools. The baseline build can be used as a starting image for any application such as email, web, FTP, Oracle database, etc. The build process is automated via Korn Shell scripts, so the hardening process is easily repeatable. The scripts can be run on existing servers that have not been properly hardened when they were built, or on servers that need a housecleaning.

Table of Contents

1.0 Server Specification and Risk Mitigation

1.1 Server Purpose

This application development server is a platform on which system software tools are built and packaged. Unix systems administrators can compile and package Open Source software such as SUDO or TCPWrappers for deployment across the enterprise. The target applications are system tools for use by administrators, not business applications.

A common complaint of AIX administrators is that Open Source software is difficult to compile and deploy on AIX when compared to Linux or Solaris. The toolbox eases the pain of this task by providing an AIX friendly development environment. By packaging the binaries into an RPM format, deployment and maintenance of the software across a large enterprise is greatly simplified.

1.2 Hardware and Operating System Requirements

Powerful hardware is not required. The development server is only used by the Unix administrators, and only one or two administrators are likely to be using the server at any given time. Speed of compilation is not much of an issue, so inexpensive hardware can easily do the job. This makes the server easy to justify when budgets are tight.

The server used in our environment is an RS6000 configured as follows. This server is more powerful than is required for a development platform, but the hardware became available when an application was migrated to bigger hardware, so it was redeployed as the administrator's development toolbox. We use an 18 GB disk as the standard size for the root volume group to contain the operating system. You could probably squeeze the installation onto a 9 GB configuration, but the cost savings is not worth the trouble.

Model:	7044-170
Processor:	(1) Power3 400 MHz
Memory:	1.0 GB
Disks:	Internal, (2) 18.2 GB SCSI, mirrored via LVM
Disk Controller:	Wide Ultra-2 SCSI
Ethernet Adapter:	10/100 MB

The operating system version is AIX 5.2 with maintenance release 2. The same server build and hardening procedures could be applied to AIX 5.1 without a lot of changes, but they have not been tested on version 5.1 so you may need to

make a few adjustments if you need to run on that version. Support for AIX version 4.3.3 reached end-of-life in 2003, so version 4.x cannot be considered.

1.3 Physical Installation

The server is located in a raised-floor data center with all of the typical environmental and physical controls. Key card access is required to enter the data center, and access records are maintained. Only a limited number of system administrators are granted access to the room. Closed-circuit cameras record physical activity in the room. A small staff of operators is in the data center 24 x 365, and is positioned so that they can monitor personnel activities. Air conditioning and humidity controls provide a healthy atmosphere for the servers. The power supply is protected with UPS battery systems, and a small emergency generator building is located on the premises to provide power in the event of an extended power loss.

1.4 Third Party Software

For the baseline AIX build that is deployed across the enterprise, a set of RPM software packages is installed that include security-related tools and general purpose binaries that are used for daily administration tasks.

For the development toolbox, various development tools also need to be installed. These include compilers, libraries, and utilities that are used in the software compilation process. Both the GCC compiler and the native IBM Visual Age C compiler are installed. Generally, the GCC compiler poses fewer compilation issues when building Open Source software, but occasionally the IBM compiler is a better choice, so having both at your disposal gives you flexibility.

IBM provides many of the development environment RPM file sets that are required at URL: http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html (11 January 2004). The RPM file set name indicates the architecture on which the software was built. Some the IBM supplied software was built on older operating system versions such as 4.3.3 and 5.1, but these packages are upward compatible to version 5.2.

The following tables list both the baseline and the development server software that is installed. The Internet web sites where the software can be located are current as of January 11, 2004.

To download compiled cryptographic software supplied by IBM such as OpenSSL, you need to register a user account with IBM at the URL that is provided in the

table. Registration is free, and only takes a few minutes to complete. If you are administering an AIX shop, you probably did this already. Although the specific link is listed in the table below, it is also on the top of the main IBM download page (mentioned above) as "AIX Toolbox Cryptographic Content".

Baseline Source Code:

Package	Purpose	URL
libol-0.3.9	Syslog replacement	http://www.balabit.com/downloads/libol/0.3/libol-0.3.9.tar.gz
openssh-3.7.1p2	Security	http://www.openssh.org/portable.html (Select one of the numerous download mirrors on the web page. Example full URL using one of the mirrors on the web page: ftp://mirrors.rcn.net/pub/OpenBSD/OpenSSH/portable/openssh-3.7.1p2.tar.gz)
openssh AIX patch	Security	http://www.zip.com.au/~dtucker/openssh/ (Look for the latest AIX patch as shown in the following URL) http://www.zip.com.au/~dtucker/openssh/openssh-3.7.1p2-pwexp26.patch (Latest patch as of 05/03/2004)
prngd-0.9.27	Security	http://ftp.aet.tu-cottbus.de/personen/jaenicke/postfix_tls/prngd.html
sudo-1.6.7p5	Security	http://www.courtesan.com/sudo/dist/sudo-1.6.7p5.tar.gz
syslog-ng-1.5.26	Syslog replacement	http://www.balabit.com/downloads/syslog-ng/1.5/src/syslog-ng-1.5.26.tar.gz
tcp_wrappers-7.6	Security	ftp://ftp.cerias.purdue.edu/pub/tools/unix/netutils/tcp_wrappers/tcp_wrappers_7.6-ipv6.3.tar.gz

Baseline RPM Binaries:

Package	Purpose	URL
bash-2.05a	Popular shell	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
lsof-4.61	Admin tool	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
openssl-0.9.6m	Security	http://www6.software.ibm.com/dl/aixtbx/aixtbx-p
readline-4.2a	Read utility	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
textutils-2.0	Admin tools	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
unzip-5.42	Admin tools	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
zip-2.3-3	Admin tools	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
zlib-1.1.4	Compression	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html

Development Server RPM Binaries

Package	Purpose	URL
autoconf-2.53	Source Configuration	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
automake-1.5	Makefile Creation	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
binutils-2.9	Development Utilities	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
bison-1.34	Parser	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
bzip2-1.0.2	Compression Utility	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html

Package	Purpose	URL
db-3.3.11	Database System	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
fileutils-4.1	File Management Utilities	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
findutils-4.1	GNU find and xargs commands	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
flex-2.5.4a	Text pattern recognition tool	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
gawk-3.1.0	GNU awk command	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
gcc-2.9	GCC compiler	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
gdbm-1.8.0	GNU database routines	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
gdbm-devel-1.8.0	Development Libs for GDBM	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
gettext-0.10.39	GNU multi-lingual utilities	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
libtool-1.4.2	Shared library utility	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
m4-1.4	Macro processor	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
make-3.79.1	Build tool for compilation	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
openssl-devel-0.9.6m	OpenSSL development	http://www6.software.ibm.com/dl/aixtbx/aixtbx-p
popt-1.7	Command line parser	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
readline-devel-4.2a	Readline utility library	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
texinfo-4.0-8	Tool for making document files	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html
zlib-devel-1.1.4	Compression library	http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html

1.5 Additional Processes and Services

Our shop uses IBM's Tivoli Storage Manager (TSM) as the standard backup solution for all Mainframe, Unix, and Windows systems. TSM utilizes a backup daemon process that is not part of the baseline operating system. The TSM daemon *dsmc* runs continuously and listens on TCP port 1401.

Secure Shell (SSH) runs on all of the servers across the enterprise as a replacement for the clear-text protocols such as telnet, FTP, and Remote Shell (RSH). SSH runs on TCP port 22. This service is not supplied with the standard AIX installation, so it is included as an additional installation step when the servers are built.

Commercial Tripwire uses a daemon *twagent* on the target servers that communicates with the centralized console. The agent listens on TCP port 1169.

1.6 User Community

The Unix system administrators are the only users that require access to the server. This significantly reduces the load and the daily administration that this server will require. The Unix system administrators have root-level privileges on the server.

1.7 Server Value and Risks

The server's primary value is that it is going to be the central repository for the development and distribution of security-related software tools for the enterprise. There is no corporate intellectual property or confidential data.

Given this profile, the primary goal of protecting this server is to prevent unauthorized modification to the software source or binaries. If an unauthorized user were to modify the security tools in a malicious manner, the modified code could be distributed across the enterprise. Modifications such as the inclusion of back doors and sniffers into the security tools could easily compromise the security of the entire environment.

Since the server is to be located on the internal network without any access to the public Internet, the risk of attack from outside sources is reduced. The server does not offer an abundance of network services and it is physically secured in the data center, so the attack vectors are limited. The primary risk of gaining access to the server is via the administrative interface, which is Secure Shell.

1.8 Risk Mitigation

1.8.1 Build Server with Minimal Operating System File Sets

The default AIX installation process creates a server image that includes Operating System services and features that not required for a typical server. After the initial installation process is completed, we remove the unnecessary file sets. This eliminates applications that could be exploited either remotely across the network or locally for privilege escalation.

1.8.2 Network Based Hardening

All non-essential network services are disabled. Kernel-level configuration disables inherently dangerous behaviors such as source routing, ICMP broadcasting, ICMP redirection, and SYN floods. These measures reduce the attack vectors that an intruder can exploit to either attack the server directly or to use the server to assist in an attack on other servers.

1.8.3 Host Based Hardening

Login banners are implemented that describe use and monitoring policies. File system permissions are tightened with special attention to SUID/SGID executables since these are often the targets of attacks. File creation permissions are improved so that users and processes do not create files that permit undesirable manipulation. Clock synchronization is implemented so that event times are consistent across the enterprise and log files contain reliable notification times. Strong user login and password controls are configured to prevent misuse of valid user accounts.

1.8.4 Replacement of Clear Text Protocols

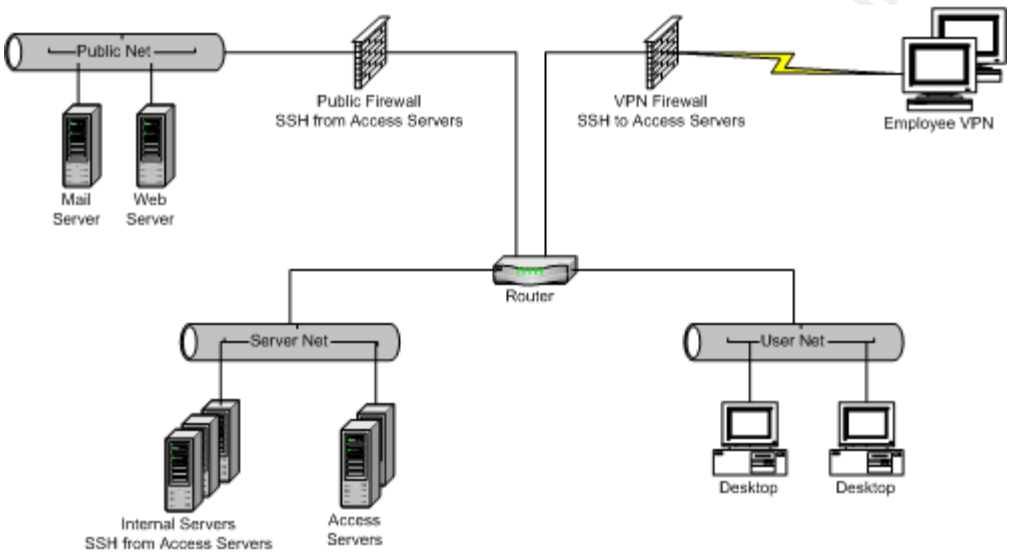
Clear text protocols such as Telnet, FTP, and the Berkeley R-commands (Remote Shell RSH, Remote Copy RCP, etc) are replaced with Secure Shell SSH. This provides stronger authentication mechanisms and provides an encrypted transport to prevent snooping of the network traffic.

1.8.5 Administrative Access Control

In order to limit administrative SSH access to all Unix servers, a redundant pair of administrator access servers is configured. Only system administrators have accounts on these servers, and TCPWrappers is used to limit SSH access on most servers to this pair of source addresses. This also makes firewall rule sets easier to manage since SSH access lists can be reduced to the access server source addresses for most target network segments.

Below is a simplified diagram of a typical network scenario that illustrates the access servers' placement in the network. Firewalls that control access from segments such as an employee VPN entry point or to a target network such as a public segment only need a minimal set of access lists that specify the access servers' SSH traffic. Many corporate networks are not fully compartmentalized using internal firewall controls, so this arrangement can leverage the

TCPWrappers control lists on the individual servers to improve control of SSH traffic. If user segments have both administrators and regular users, TCPWrappers helps to prevent regular users from accessing the SSH service on hosts. TCPWrappers can also help to prevent SSH attacks between servers if a server should be compromised on some other service. This is obviously not as strong of a protection as an internal firewall can provide, but it contributes to defense in-depth. This can be implemented by Unix administrators when network architecture does not provide sufficient internal controls.



1.8.6 Centralized Logging

A centralized log server is placed on the internal network for collecting Syslog traffic from all servers and network devices. This technique is used to protect log integrity if an attacker gains access to a server. A common practice of attackers is to remove evidence of their intrusion by modifying the local log files on a server after they gain access. By writing the log files to a remote server, the evidence is retained for investigative purposes, providing that the log server is not compromised. The baseline hardening process that we use includes the configuration of the remote logging facility. Local logs are also kept for administrator debugging activities in the event that network connectivity is lost.

1.8.7 Auditing

The auditing subsystem is enabled. This collects very detailed system event information such as user account actions, file accesses, system calls, process activities, etc. The auditing subsystem can be configured to monitor specific events of interest, and the monitored events are organized into groups. Groups

are then assigned to specific users. This allows the monitoring of the root account, administrator accounts, and general user accounts to include different levels of detail. Since detailed auditing consumes a lot of disk space and increases CPU load, we are very careful when selecting what is monitored. Collecting too much information produces an overwhelming amount of data. Each organization must decide what level of detail is reasonable for their environment.

1.8.8 User Accountability

All users connecting to all servers in the enterprise must use their own unique login. This includes Unix administrators, application administrators such as Oracle, SAS, or PeopleSoft, and any general users that have a business process that requires a command line on the servers.

Direct root logins are not permitted. Only the Unix administrators are permitted to use the root account, and they must SU from their account to the root account. Application administrators are provided with SUDO for a specified subset of commands that require root permissions.

The only exception to this is direct root login on the console. Only the system administrators have access to the console. The data center access card system records entry into the room, and the video cameras record activity in the room. Although this limited user accountability for the system administrators reduces the security posture somewhat, the risk is considered more acceptable than the possibility of administrator lock-out. Since we will be implementing a non-local, centralized authentication mechanism such as RADIUS, LDAP, or Secure-ID for non-root accounts in the near future, the loss of network connectivity would mean that the administrators would be unable to login using their own accounts. The ability to login and correct problems could increase downtime for critical business applications. The risks were considered and the root logins on the console were selected as the more acceptable risk.

1.8.9 File System Integrity Checking

Tripwire is deployed across the enterprise as a standard method of insuring file system integrity. We selected the commercial version, which can be found on the Internet at URL: http://www.tripwire.com/products/servers/index.cfm (3 May 2004). Our shop has hundreds of servers located in several offices across the country. The centralized management features of the commercial version were required in order for our small administration team to realistically manage the deployment.

Not all companies can afford the commercial Tripwire product, and many cannot afford the time and effort to administer the Open Source version. To assist those shops, this paper includes an implementation of the Trusted Computing Base (TCB) that is provided with AIX. The TCB is not as secure or robust as Tripwire, but it can be leveraged to provide a rudimentary file system integrity checking mechanism.

Whether you are using Tripwire, the TCB, or some other file system integrity assurance tool, the intent is to detect unauthorized modifications to system files. Attackers modify configuration files and executable binaries in order to retain access to a server after the initial intrusion. They may also install some of their own executables that gather information such as account and password information in order to break into other systems. By creating cryptographic checksums of the configuration files and executable binaries, you can periodically verify that the files have not changed. Quality tools such as Tripwire also notify you if new executables are installed.

2.0 Install and Harden the Server

2.1 Media Preparation

2.1.1 Locate the IBM installation CD-ROMS

Locate the initial installation media for AIX 5.2. This is a six CD-ROM set.

Locate the C for AIX compiler CD-ROM.

2.1.2 Create a CD-ROM with the Maintenance Release from IBM

IBM periodically releases a comprehensive patch bundle called a Maintenance Release. This includes all patches that fix bug and security issues. As of 01/24/2004, the current Maintenance Release for AIX 5.2 is level 5200-02. Maintenance Releases and interim patches can be downloaded from the IBM web site at URL: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp (3 May 2004). The IBM web site continually undergoes development, so if this URL becomes obsolete, you can find the new URL with a search engine such as Google using the keywords “IBM Fix Central”. The main download page allows you to select a few options such as hardware class, operating system release, and maintenance release. After supplying your specific information, the web site directs you to the download page.

Download the current maintenance release from IBM. Unpack the TAR file that you downloaded and burn the files onto a CD-ROM for installation.

2.1.3 Create a CD-ROM with the Patches from IBM

IBM releases patches on an as-needed basis between full Maintenance Releases to fix any bugs or security related issues. These patches can be downloaded from the IBM web site at the same URL as the Maintenance Releases: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp. As a general guideline, keep all a repository of all critical fixes, and only include other fixes for problems that you are experiencing. The critical fixes include all security patches. Applying bug fixes for problems that you have not encountered only increases the chances of introducing new problems. When you navigate the web page options, you only need to select the patches as of the latest month shown since the selection will include all of the previous months. Burn the files onto a CD-ROM for installation.

2.1.4 Create a CD-ROM with Add-on Software and Hardening Scripts

Burn a CD-ROM with the following software. For convenience, place each software group into the subdirectories indicated.

- Copy the third party software that you downloaded in Section 1.4 onto the CD-ROM.

  Copy the baseline source files to directory /SOURCES.
  Copy the baseline RPM binaries to directory /RPMS
  Copy the development server RPM binaries to directory /DEVEL-KIT.

- Attached file **specs.zip** contains RPM specification files for creating binaries from the source code that you downloaded. Copy them to /SPECS.

- Attached file **sources.zip** contains a bundle of Korn shell scripts that automate the hardening process. Copy them to /SOURCES.

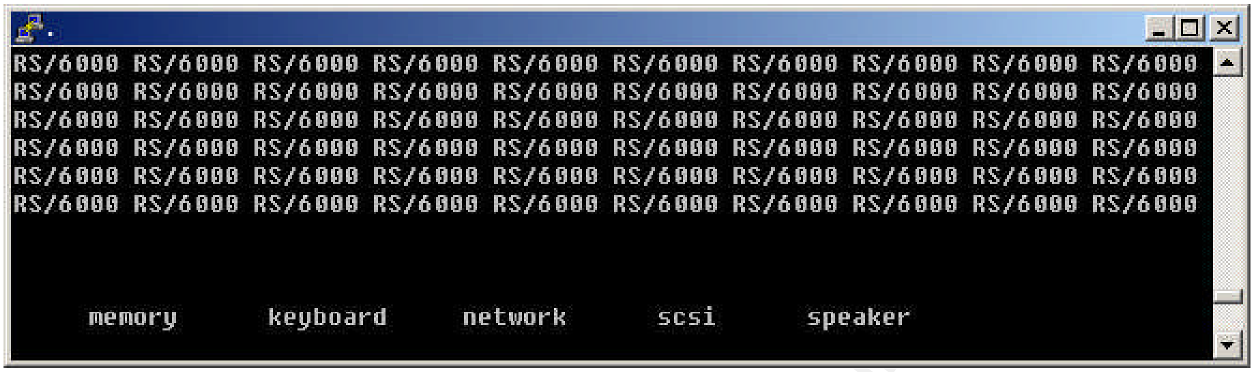
2.2 Install the Initial System Image

This section outlines the procedures for loading the initial AIX 5.2 system image from CD-ROM onto the hard drive.

2.2.1 Initial Load from CD-ROM

- Make sure the network cable is disconnected from the network interface.

- Insert the IBM AIX installation CD-ROM disk 1. Depress the power button on the front of the machine. In a few minutes, the machine will boot from ROM. You will hear several beeps, and the machine will self-test several hardware components which will be displayed on the screen (see screen below). As this occurs, you need to activate the SMS firmware menu by pressing the numeric 1 (one) key several times if you are connected via serial port, or by pressing the F1 key several times if you are connected via VGA port.



- The following menu displays. Configure the boot sequence to use the CD-ROM as the boot device. Select “**2 Multiboot”** on the menu.

```
RS/6000 Firmware
Version SPH03114
(c) Copyright IBM Corp. 2000  All rights reserved.
-----------------------------------------------------------------------
System Management Services
1 Display Configuration
2 Multiboot
3 Utilities
4 Select Language
                                                .------.
                                                |X=Exit|
                                                `------'
```

- The following menu displays. Choose “**4 Select Boot Devices”**.

```
RS/6000 Firmware
Version SPH03114
(c) Copyright IBM Corp. 2000  All rights reserved.
----------------------------------------------------------------------
Multiboot
1 Select Software
2 Software Default
3 Select Install Device
4 Select Boot Devices
5 OK Prompt
6 Multiboot Startup <OFF>
                                                .------.
                                                |X=Exit|
                                                `------'
```

- The following menu displays. Choose “**3 Configure 1st Boot Device”**.

```
RS/6000 Firmware
Version SPH03114
(c) Copyright IBM Corp. 2000  All rights reserved.
----------------------------------------------------------------------
Select Boot Devices
1 Display Current Settings
2 Restore Default Settings
```

```
3 Configure 1st Boot Device
4 Configure 2nd Boot Device
5 Configure 3rd Boot Device
6 Configure 4th Boot Device
7 Configure 5th Boot Device
                                                  .------.
                                                  |X=Exit|
                                                  `------'
```

- The following menu displays. Choose the number of the CD-ROM.

```
Configure 1st Boot Device
Device Current Device
Number Position Name
1        -        Diskette
2        1        SCSI CD-ROM id=@1,0 ( Integrated )
3        2        SCSI 18200 MB Harddisk id=@4,0 ( Integrated )
4        3        SCSI 18200 MB Harddisk id=@5,0 ( Integrated )
5        -        IBM 100/10 Ethernet Adapter  ( Integrated )
6        -        IBM 100/10 Ethernet Adapter  ( slot=5 )
7        -        IBM 100/10 Ethernet Adapter  ( slot=4 )
8        -        IBM 100/10 Ethernet Adapter  ( slot=3 )
9                 None
                                                  .------.
                                                  |X=Exit|
                                                  `------'
```

- The following menu displays, although your options may vary. The CD-ROM should show as the first boot device. Press **X** to exit. Continue pressing **X** to exit from each of the menus as you back out through all of the same menus that brought you here.

```
RS/6000 Firmware
Version SPH03114
(c) Copyright IBM Corp. 2000  All rights reserved.
-------------------------------------------------------------------------
Current Boot Sequence
1 SCSI CD-ROM id=@1,0 ( Integrated )
2 SCSI 18200 MB Harddisk id=@4,0 ( Integrated )
3 SCSI 18200 MB Harddisk id=@5,0 ( Integrated )
4 None
5 None
                                                  .------.
                                                  |X=Exit|
                                                  `------'
```

- The system reboots. You are presented with a screen to select this terminal as the console. Press **2** and **ENTER**. Note: the "2" character does not display on the screen.

- You are presented with a language selection screen. Choose your language to continue.

- The following menu displays. This is an important step because it enables you to select options that enhance the server security. Choose "**2 Change/Show Installation Settings and Install"** and press **ENTER**

```
                        Welcome to Base Operating System
                        Installation and Maintenance

Type the number of your choice and press Enter.
Choice is indicated by >>>.

>>> 1 Start Install Now with Default Settings
    2 Change/Show Installation Settings and Install
    3 Start Maintenance Mode for System Recovery
    88 Help?
    99 Previous Menu

>>> Choice [1]: 2
```

- The Installation and Settings screen displays. Several options need to be changed. Select "**1 System Settings"**.

```
                        Installation and Settings

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

    1 System Settings:
        Method of Installation.............Preservation
        Disk Where You Want to Install.....hdisk0...
    2 Primary Language Environment Settings (AFTER Install):
        Cultural Convention................English (United States)
        Language ..........................English (United States)
        Keyboard ..........................English (United States)
        Keyboard Type......................Default
    3 More Options  (Desktop, Security, Kernel, Software, ...)
>>> 0 Install with the current settings listed above.

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

- On the next menu, select option "**1 New and Complete Overwrite".**

- The next menu enables you to select which disks will be used for the installation. Choose the appropriate disks. If you are going to use LVM mirroring, deselect the mirror disks since they will be configured later.

- The Installation and Settings screen (above) redisplays with your System Settings. Choose "**3 More Options"** which provides some security related settings.

- The following menu displays. All options should be changed as shown below. This menu may vary depending upon your hardware. Older 32-bit processors will not display the 64-bit menu selections. Newer 64-bit hardware shows the following options. The following IBM web page provides additional details on these options: URL: http://publib16.boulder.ibm.com/pseries/en_US/aixins/insgdrf/advanced_options.htm (3 May 2004).

  As you select each item, the option is toggled Yes or No.

  Choose option 1 (Yes) to Enable Trusted Computing Base. This is a security enhancement, especially if you are not able to implement a file system integrity tool such as Tripwire.

  Choose option 2 (Yes) to Enable CAPP and EAL4. This will automatically enable options 3 and 4 (both Yes) and disable option 7 (No). CAPP and EAL4 are industry security standards for which the AIX platform is certified. They are described in detail on the following IBM web page: URL: http://publib16.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixbman/security/capp_eal4plus.htm (3 May 2004).

  Use option 5 (No) to exclude Graphics Software. We are excluding graphics and X-windows for security reasons since X-windows introduce numerous security issues.

  Use option 6 (No) to exclude Documentation Services Software. This contributes to a lean server image. We elected to use Internet and manuals for documentation.

  Use option 7 (No) to exclude drivers for hardware that is not installed on this server. This is required for CAPP and EAL4 standards.

```
                        Install Options

 1.  Enable Trusted Computing Base.............................. Yes
 2.  Enable CAPP and EAL4+ Technology........................... Yes
     (English only, 64-bit kernel enablement, JFS2 file systems)
 3.  Enable 64-bit Kernel....................................... Yes
 4.  Create JFS2 File Systems................................... Yes
     (Requires 64-bit Kernel Enabled)
 5.  Graphics Software.......................................... No
 6.  Documentation Services Software............................ No
 7.  Enable System Backups to install any system................ No
     (Installs all devices and kernels)
```

```
>>> 8.  Install More Software
    0  Install with the current settings listed above.
    88  Help ?
    99  Previous Menu

>>> Choice [8]: 0
```

- An installation summary screen displays. This gives you an opportunity to review your choices for accuracy. Begin the installation if the options are correct, or use the menu to fix any mistakes.

- The installation proceeds. After the installation completes, the system reboots from the newly installed image.

2.2.2 Initial Configuration after Reboot

- Initial Configuration Screens

  Navigate the menus to select the console terminal type, accept the license agreement, and set the root password. Use a strong password for the root account that adheres to your company's password policy. If your company does not have a password policy, use the standard provided further below in this paper. After setting the password, you can exit the initialization menus to return to the login prompt.

- Set the Time Zone and Date

  Log in as root on the console. Use the following commands to set the system clock. Do not be overly concerned about the accuracy since NTP is configured later to provide exact clock synchronization.

```
chtz EST5EDT            (supply your correct time zone)
date mmddHHMMYYYY       (supply the current date and time)
```

- Configure the network interface

  In the following commands:
  Change the references from "ent0" and "en0" to the appropriate interface name.
  Change the hostname "newserver" to the hostname of your new server.
  Change the host address "10.1.1.50" to the address of your new server.
  Change the network mask "255.255.255.0" to your network mask value.
  Change the gateway address from 10.1.1.1 to your gateway.
  You may need to change the media speed as appropriate for your network.

```
chdev -l en0 -a state=down
```

```
chdev -l en0 -a state=detach
rmdev -l en0
rmtcpip
mkdev -l en0
chdev -l 'ent0' -a media_speed='100_Full_Duplex'
mktcpip -h newserver -a 10.1.1.50 -m 255.255.255.0 -i en0 -g 10.1.1.1 -t 'N/A'
lsattr -E -l en0  (Verify the network settings that you selected)
lsattr -E -l ent0 (Verify the network settings that you selected)
```

NOTE: Do not connect the network cable at this time.

2.3 Install the IBM C Compiler

The C compiler should be installed next. We are purposely installing it before patching the system so that the compiler file sets are also patched. Several file sets need to be installed from the initial AIX CD-ROMs as prerequisites.

Install the following prerequisite LPP file sets from the AIX 5.2 CDs:

Base Application Development Math Library	bos.adt.libm
User Heap/Memory Debug Toolkit	memdbg.adt
	memdbg.aix43.adt
SMP Runtime Library	xlsmp.rte
Network Computing System	bos.net.ncs
License Use Management Runtime	ifor_ls.msg.en_us
	Ifor_ls.base

Install the following LPP file sets from the C for AIX CDs:

C for AIX Compiler	vac.C
C for AIX Compiler Messages	vac.msg.en_US.C
User Heap/Memory Debug Messages	memdbg.msg.en_US
XL SMP Runtime Messages	xlsmp.msg.en_US.rte

After installing the file sets, you need to run the licensing procedure. The licensing procedure may vary depending upon your licensing agreement with IBM. Run the following command and answer the prompts based upon your license.

```
cd /var/ifor
/usr/opt/ifor/bin/i4cfg -script
/usr/opt/ifor/bin/i4blt -a -f /usr/vac/cforaix_cn.lic -T 1 -R"sitename"
      /usr/vac/bin/replaceCSET
```

2.4 Install the Latest Patches

The procedures in this section are only required for the initial construction of the Development Toolbox server. The Maintenance Release software is copied to the Toolbox server for automated configuration of subsequent server builds in the

enterprise. After the Development Toolbox is built, an installation TAR image is created that includes all patches, installation scripts, security software, and standard configuration files. The TAR image is used for all server baseline installations.

When IBM releases individual patches or full Maintenance Releases, these are installed onto the Development Toolbox and the installation TAR image is regenerated.

2.4.1 Reconfigure the Initial File System Sizes

The initial file system sizes are rather small. Expand them using the following commands. The numbers shown in the commands are expressed in megabytes.

```
chfs -a size=128M /
chfs -a size=4096M /usr
chfs -a size=1536M /var
chfs -a size=512M /tmp
chfs -a size=128M /home
```

The initial installation from CD-ROM creates a separate file system for **/opt**. Our shop elected to move its contents to the **/usr** file system, remove the **/opt** file system, and create a symbolic link from **/opt** to **/usr/opt** in order to simplify disk management. The procedures contained in this document follow this convention, but you can easily modify the procedures to retain a separate **/opt** file system if you prefer.

Relocate the **/opt** file system to **/usr/opt**, and remove **/opt** using the following commands.

```
cd /
rm /usr/opt/freeware    (this symbolic link becomes obsolete)
mv /opt/* /usr/opt
umount /opt
rmfs /opt
rmdir /opt
ln -s /usr/opt /opt
```

2.4.2 Create the Software Repository Directories

The standard location for the RPM development directories on AIX is **/opt/freeware/src/packages**. Our standard installation process will include Maintenance Release bundles, patches since the latest Maintenance Release, AIX software bundles in standard IBM “LPP” package format, and our in-house developed RPM bundles. To make development and deployment easier, all of the Toolbox installation software will be located under the standard RPM development directory structure.

Make the additional software directories using the following commands:

```
cd /usr/opt/freeware/src/packages
mkdir -m 750 -p DEVEL-KIT INSTALL LPP MAINT/5200-02 PATCHES/5200-02
chown root:system *
chmod 750 *
```

2.4.3 Install the Latest Maintenance Release

Locate the Maintenance Release CD-ROM that you prepared in section 2.1. Insert the CD-ROM into the drive.

Copy the Maintenance Release patches to the software repository directory.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
cd /usr/opt/freeware/src/packages
cp /mnt/* ./MAINT/5200-02
chown -R root:system ./MAINT
chmod -R 750 ./MAINT
umount /mnt
```

Install the Maintenance Release.

```
cd /usr/opt/freeware/src/packages/MAINT/5200-02
inutoc .

(The following is all one long line)
      odmget -q attribute=TCB_STATE PdAt |
      sed "s/deflt = .*/deflt = tcb_disabled/" |
      odmchange -o PdAt -q attribute=TCB_STATE

(This is a single line command)
      installp -acgXd . bos.rte.install

(The following is all one long line)
      /usr/lib/instl/sm_inst installp_cmd -a -d . -f
      '_update_all' -c -N -g -X
```

2.4.4 Install the Latest Patches

Locate the Patches CD-ROM that you prepared in section 2.1. Insert the CD-ROM into the drive.

Copy the patches to the software repository directory.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
cd /usr/opt/freeware/src/packages
cp /mnt/* ./PATCHES/5200-02
chown -R root:system ./PATCHES
chmod -R 750 ./PATCHES
umount /mnt
```

Install the patches.

```
cd /usr/opt/freeware/src/packages/PATCHES/5200-02
inutoc .

(The following is all one long line)
      /usr/lib/instl/sm_inst installp_cmd -a -d . -f
      '_update_all' -c -N -g -X

(The following is all one long line)
      odmget -q attribute=TCB_STATE PdAt |
      sed "s/deflt = .*/deflt = CC_EVAL/" |
      odmchange -o PdAt -q attribute=TCB_STATE
```

Reboot the server.

```
cd /
shutdown -Fr
```

2.5 Install the Add-On Software and Hardening Scripts

2.5.1 Copy the Add-On Software and Scripts from CD-ROM

Locate the Add-On Software and Hardening Scripts CD-ROM that you prepared in section 2.1. Insert the CD-ROM into the drive.

Log in as root on the console. Issue the following commands to copy the software to the hard drive.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
cp /mnt/SOURCES/* /usr/opt/freeware/src/packages/SOURCES
cp /mnt/RPMS/* /usr/opt/freeware/src/packages/RPMS/ppc
cp /mnt/SPECS/* /usr/opt/freeware/src/packages/SPECS
cp /mnt/DEVEL-KIT/* /usr/opt/freeware/src/packages/DEVEL-KIT
cd /usr/opt/freeware/src/packages
chown root:system SOURCES/* RPMS/ppc/* SPECS/* DEVEL-KIT/*
chmod 640 SOURCES/* RPMS/ppc/* SPECS/* DEVEL-KIT/*
umount /mnt
```

2.5.2 Install the Miscellaneous RPMS

A few miscellaneous RPMS are required for both our development server and any AIX server that we build. These include OpenSSL, the bash shell, and compression utilities, etc.

```
cd /usr/opt/freeware/src/packages/RPMS/ppc
rpm -ivh *.rpm
```

(Screen output)

```
bash            ##########
lsof            ##########
openssl         ##########
readline        ##########
textutils       ##########
unzip           ##########
zip             ##########
zlib            ##########
```

2.5.3 Install the Development Kit

The Development Kit is a collection of RPM binaries that give you the ability to compile software and develop your own RPMS. These include the GCC compiler and various development libraries.

```
cd /usr/opt/freeware/src/packages/DEVEL-KIT
rpm -ivh *.rpm
```

(Screen output)

```
autoconf        ##########
automake        ##########
binutils        ##########
bison           ##########
bzip2           ##########
db              ##########
fileutils       ##########
findutils       ##########
flex            ##########
gawk            ##########
gcc             ##########
gdbm            ##########
gdbm-devel      ##########
gettext         ##########
m4              ##########
libtool         ##########
make            ##########
openssl-devel   ##########
popt            ##########
readline-devel  ##########
texinfo         ##########
zlib-devel      ##########
```

2.6 Compile the Installation Toolkit

The development server now has the entire development environment required for building RPMS. The next step is to compile the various software packages for configuring and hardening your operating system.

2.6.1 Customize the Source Configuration Files

Some of the software packages include configuration files that need to be customized for your site. For example, the SUDO configuration file specifies site-specific values such as users, hosts, and commands. The OpenSSH configuration file contains a few parameters that need adjustment for security reasons. The NTP configuration file needs the IP addresses of your specific NTP servers. Examine each of the samples and put your hostnames, IP addresses, and other site-specific values into them.

You could edit the files contained in the source TAR files for these packages, but this can become cumbersome over time because you will be downloading updated sources when bugs or security vulnerabilities are corrected. It is far easier to maintain your customized configuration files in a separate TAR file for each package, and let the RPM build process incorporate the configuration files.

To extract the configuration files from the TAR archives, use the following commands.

```
cd /usr/opt/freeware/src/packages/SOURCES
gunzip -c aix-config-5.2.1.0.tar.gz | tar -xvf -
gunzip -c openssh-3.7.1p2-config.tar.gz | tar -xvf -
gunzip -c radius-1.2-config.tar.gz | tar -xvf -
gunzip -c sudo-1.6.7p5-config.tar.gz | tar -xvf -
gunzip -c syslog-ng-1.5.26-config.tar.gz | tar -xvf -
gunzip -c tcp_wrappers_7.6-ipv6.3-config.tar.gz | tar -xvf -
```

Examine the extracted files and make any customizations that you need for your environment.

In the ZIP files included with this paper, there are sample configuration files in the following TAR archives.

aix-config-5.2.1.0.tar.gz

This TAR archive contains any general Unix configuration file that you modify during the course of a standard installation. Customize these to meet your needs. Of course, you can add or remove files from this list providing that you make the corresponding change in the **aix-config.spec** RPM SPEC file. Note that the files included in this RPM all have the leading pathname ./aix-config-5.2.1.0 prefixed to them.

- **environment** Typical site-specific customizations include changes to environment variables such as PATH or HISTSIZE. In the sample provided, note the TMOUT and TIMEOUT variables are set to 2700 seconds (45 minutes). This security enhancement logs out dormant sessions after the specified time.

- **motd** Include a legal warning banner about acceptable use, monitoring, penalties for misuse, etc. Consult your legal department for an acceptable warning.

- **netsvc.conf** This file is used to specify the ordering of name resolution.

- **ntp.conf** This file configures the time service NTP. Security related portions are shown below. A default "deny all" technique is enabled (restrict default ignore). Although we allow time synchronization to several servers, those servers are not able to query or modify the service on this system (restrict a.b.c.d nomodify notrap noquery). Notice the enhanced logging statement that sends status messages to the syslog facility (logconfig =).

```
restrict default ignore
logconfig =syncevents +peerevents +sysevents +allclock
restrict 10.1.1.1 nomodify notrap noquery
server   10.1.1.1 version 3
```

- **pam.conf pam.conf.no_rad pam.conf.rad**
  These are PAM configuration files (default, no RADIUS, or RADIUS enabled, respectively). *"The Pluggable Authentication Modules (PAM) library is a generalized API for authentication-related services which allows a system administrator to add new authentication methods simply by installing new PAM modules, and to modify authentication policies by editing configuration files."* URL: http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/article.html (3 May 2004).
  In version 5.2, IBM introduced PAM into the AIX operating system. Standard AIX programs that require an authentication mechanism such as SU and FTP are now PAM aware. Many Open Source software packages such as Secure Shell and SUDO have been PAM aware for a long time. The automated installation procedures include the integration of RADIUS as an alternative authentication mechanism to the local passwd database, but the same process could be used for implementing other methods LDAP or SecureID. The automated server configuration process allows you to choose whether you want to use local passwd or RADIUS by installing the appropriate PAM configuration file.

- **profile** This configuration file is often customized to fit site specific needs. In the sample provided in this TAR archive, note the following lines that mark certain environment variables read-only so that users cannot change them. This is only effective for initial login shell, so it has a very limited value, but it may prevent some users from modifying these values in their person profiles or on the command line.

```
typeset -r HISTSIZE
typeset -r TMOUT
typeset -r TIMEOUT
```

```
typeset -r LOGNAME
if [ `id -un` != "root" ]; then
   typeset -r IFS
   typeset -r DISPLAY
fi
```

- **resolv.conf** This configuration file specifies your DNS servers and domains. Edit this to fit your site's DNS requirements.

- **catalog.mic sendmail.cf words**
  These are various other miscellaneous configuration files to be installed. Of course, you can add or remove files from this list providing that you make the corresponding change in the **aix-config.spec** RPM SPEC file

openssh-3.7.1p2-config.tar.gz

- **ssh_config** This is the Secure Shell client configuration file. Place any site-specific changes that you require on all servers into this file. SSH protocol version 1 has had many security-related exposures and it is generally considered weaker than version 2, so it is disabled in this sample.

```
# cxt: all hosts
Host *
# cxt: enable X11 forwarding
ForwardX11 yes
# cxt: disable protocol v1
Protocol 2
```

- **sshd_config** This is the Secure Shell server configuration file. Place any site-specific changes that you require on all servers into this file. The changes in the sample provided are listed below. Note the following. Only protocol version 2 is allowed. Direct root logins are disabled so that users must first login using their own unique ID so that accountability is maintained. X11 forwarding is enabled due to site requirements, not for security reasons. The MOTD file is used as a login banner for convenience.

```
# cxt: disable protocol v1
Protocol 2
# cxt: disable root login
PermitRootLogin no
# cxt: enable X11 forwarding
X11Forwarding yes
# cxt: disable motd since we do it with banner option
PrintMotd no
# cxt: display motd as banner
Banner /etc/motd
```

radius-1.2-config.tar.gz

- **radius_client.conf** This configuration file specifies the required values for contacting the RADIUS server such as IP address, shared secret, and UDP port numbers.

sudo-1.6.7p5-config.tar.gz

- **sudoers** This configuration file specifies who can execute commands with root privileges via the "sudo" command. It also specifies the specific commands that may be executed on particular hosts. The exact configuration is very site specific. There are an infinite number of ways to configure SUDO to permit users to execute procedures with root privileges without actually giving those users the root account. Consult the online manual page at URL: http://www.courtesan.com/sudo/man/sudoers.html (3 May 2004) on how to customize this for your environment.

syslog-ng-1.5.26-config.tar.gz

- **syslog-ng.conf** This configuration file controls the behavior of the SYSLOG-NG syslog client software. This is installed onto all of the AIX servers in the enterprise so that a standard method of local and remote logging is maintained.

  Security related settings:

  Syslog-NG has the ability to create the target directory for the log files if it is not found. This is dangerous so we disable it. This avoids the potential for a specially crafted syslog packet to be able to create directories somewhere in the file system if the $HOST macro is used. As an extra precaution, we explicitly set the owner, group, and mode parameters to restrictive values in case an administrator inadvertently enables the directory creation using the $HOST macro.

```
create_dirs(no);
dir_owner(root);
dir_group(system);
dir_perm(0700);
```

  Syslog-NG creates the target log file using the hard-coded file names in the configuration file. We ensure safe owner, group, and mode values with the following parameters.

```
owner(root);
group(system);
perm(0640);
```

  The ability of Syslog-NG to use TCP based communications instead of the standard syslog UDP communications ensures the reliability of the message delivery. We enable this in the configuration file with the following statement. You can use any port number that you want. Since the standard UDP port is 514, and we are disabling remote shell, which uses TCP 514, our shop elected to use TCP 514.

```
destination d_log_host1 { tcp("syslogger1" port(514) ); };
```

- **syslog-ng-server.conf** This configuration file controls the behavior of the SYSLOG-NG syslog server software. This is only installed onto the central syslog servers. At least one central syslog server should be configured, but two provides redundancy in case of a failure. Budgets are often the deciding factor.

  Security related settings:

  We use the same directory and file creation settings in the server configuration file as are shown in the client configuration above.

  The configuration file is setup to listen for both UDP and TCP connections on port 514.

```
# standard udp connections
source s_udp { udp( ip("SERVERNAMEGOESHERE")   port(514) ); };
# tcp connections
source s_tcp { tcp( ip("SERVERNAMEGOESHERE")   port(514)
              max-connections(256) keep-alive(yes) ); };
```

  This allows the central log server to service both Syslog-NG clients and native syslog clients. This is rather convenient for the interim period during a Syslog-NG implementation when your environment will have a mix of both clients. It also allows you to accept UDP based logging from other non-Unix clients such as routers or firewalls that are not capable of TCP based logging. The SERVERNAMEGOESHERE value in the above statements is automatically edited with the server name during the RPM installation process since the SPEC file includes that logic.

  We elected to log each server's messages into a subdirectory that uses the hostname in the path. This places each server's logs into it's own directory. The administrators like this because it creates a concise log file with only that particular host's messages. Since we disabled the automatic directory creation, the administrators must manually create the /log/HOSTNAME directory on the log server when they implement a new server.

```
destination hosts {
   file("/log/$HOST/messages");
};
log { source(s_udp); destination(hosts); };
log { source(s_tcp); destination(hosts); };
```

  We also elected to log each server's messages into one large composite log file in the /log/ALL_HOSTS directory.

```
destination all_hosts {
   file("/log/ALL_HOSTS/messages");
};
log { source(s_udp); destination(all_hosts); };
log { source(s_tcp); destination(all_hosts); };
```

Fortunately, we have an enormous amount of disk space on an EMC disk array, so we have the luxury of allocating some extra space to accommodate this. There are two benefits to a composite log. Automated log parsing and alerting is far easier with one log file since you do not need to process a lot of individual files. Another very important benefit is that it sequences the activity of hosts across the environment in one central log.

tcp_wrappers_7.6-ipv6.3-config.tar.gz

- **hosts.deny** This configuration file specifies which source hosts are denied TCP/UDP services supplied by specific daemons that are TCPWrappers aware. The safest implementation is to deny all services in this file and configure only the permitted connections in the hosts.allow file. This can be accomplished with a single line in the hosts.deny file.

```
ALL: ALL
```

- **hosts.allow** This configuration file specifies which source hosts are permitted TCP/UDP services supplied by specific daemons that are TCPWrappers aware. The following line only permits SSH from source addresses 10.10.1.1 and 10.10.1.2.

```
sshd: 10.10.1.1 10.10.1.2
```

2.6.2 Create New RPM Configuration TAR Archives

After editing any of the configuration files in the previous step, you need to create a new TAR archive with the modified files that contain your edits. This ensures that your custom configuration files are bundled into the RPM binaries for installation.

For each TAR file that you made configuration file changes, recreate the archive as follows. The Syslog-NG configuration file archive is used as an example.

```
cd /usr/opt/freeware/src/packages/SOURCES
```

(The following command is one long line)

```
tar –cvf - syslog-ng-server.conf syslog-ng.conf | gzip –c
>syslog-ng-1.5.26-config.tar.gz

chown root:system syslog-ng-1.5.26-config.tar.gz
chmod 640 syslog-ng-1.5.26-config.tar.gz
```

2.6.3 Build the RPM Installation Binaries

Now that your configuration files are customized to suit your environment, you need to create the RPM installation binaries. These software packages enable

you to install customized Open Source software and AIX configuration files on all of the servers in your enterprise.

Build the RPM for each software package. For each package, an RPM SPEC file instructs the RPM system how to compile and install the software. You can optionally edit the SPEC files to change installation directories, file ownerships, or other installation procedures, but the supplied versions should be fine for most shops. After you build each RPM package, watch for any error messages. The last message that you should see is “exit 0”. Some of the software packages are also installed at this time. This is because they are prerequisites for the compilation of subsequent packages. During the hardening process later on, all of the software is installed.

Change to the directory where the SPEC files are installed.

```
cd /usr/opt/freeware/src/packages/SPECS
```

Build the AIX installation and configuration utilities.

```
rpm -ba aix-bin.spec
rpm -ba aix-config.spec
rpm -ba aix-harden.spec
rpm -ba aix-never-delete.spec
```

Optionally build the Tivoli Storage Manager configuration. TSM is a popular backup solution among IBM shops since it is an IBM Tivoli product. If your shop uses another package, you will need to replace this step with your vendor’s product configuration. This RPM does not contain the TSM software, which is purchased separately from IBM. The RPM just contains your customized configuration files for TSM.

```
rpm -ba aix-tsm.spec
```

Build and install the TCPWrappers software.

```
rpm -ba tcp_wrappers.spec
rpm -ivh ../RPMS/ppc/tcp_wrappers-7.6-ipv6.3.aix5.2.ppc.rpm
```

Build and install the Pseudo Random Number Generator software.

```
rpm -ba prngd.spec
rpm -ivh ../RPMS/ppc/prngd-0.9.27-1.aix5.2.ppc.rpm
```

Build the Syslog-NG software. We will only install the library portion at this time because the native AIX syslog daemon has not yet been disabled.

```
rpm -ba libol.spec
rpm -ivh ../RPMS/ppc/libol-0.3.9-1.aix5.2.ppc.rpm
rpm -ba syslog-ng.spec
```

Build the SUDO software.

```
rpm -ba sudo.spec
```

Build the RADIUS software. We actually need just the client portion, but this procedure will build both the server and client software.

```
rpm -ba radius.spec
```

Build the OpenSSH software.

```
rpm -ba openssh.spec
```

2.6.4 Copy any Additional Shop-Specific Software to the Server

Every shop has a few software packages that they like to install on all of their machines such as diagnostics or performance measurement tools. No two shops are the same, so the installation process needs to accommodate this. The installation scripts will install any AIX LPP filesets that they find in the directory /usr/opt/freeware/src/packages/LPP. Make a separate subdirectory for each package, and you can arbitrarily name it. To add your favorite tools to your standard distribution, copy the software as an LPP file set from your installation media to this subdirectory (command: smitty maint). The installation scripts find each subdirectory and run an "installp" against the filesets found underneath. A few examples that our shop likes are shown below.

Subdirectory	**Contents**
bos.content_list	This enables the "which_fileset" command, a favorite of many AIX administrators. 5.2.0.0 AIX Release Content List
bos.dosutil	DOS Utilities for manipulating DOS formatted disks 5.2.0.0 DOS Utilities
diagnostics	Diagnostics software for when hardware hiccups 5.2.0.0 devices.chrp.base 5.2.0.0 devices.common.IBM.modemcfg 5.2.0.0 devices.common.base
tsm	Tivoli Storage Manager tivoli.tivguid 1.1.0.0 IBM Tivoli GUID on AIX tivoli.tsm.books.en_US.client 5.2.0.0 TSM BOOKS - Using UNIX Clients - HTML Format 5.2.0.0 TSM BOOKS - Using UNIX Clients - PDF Format tivoli.tsm.client.api.32bit 5.2.0.0 TSM Client - Application Programming Interface tivoli.tsm.client.ba.32bit 5.2.0.0 TSM Client - Backup/Archive Base Files 5.2.0.0 TSM Client - Backup/Archive Common Files 5.2.0.0 TSM Client - Backup/Archive WEB Client 5.2.0.0 TSM Client - IMAGE Backup Client 5.2.0.0 TSM Client - NAS Backup Client

2.6.5 Prepare a Tripwire Golden Image

This section describes how to prepare a site-wide deployment of the commercial version of Tripwire version 4.10 released in March 2004.

The first step is to install and configure Tripwire on the development server. This is used as a template or "Golden Image" for configuring all of the other servers in your environment.

The process for installing Tripwire is described in detail in the documentation included with the product. An abridged transcript is included here since there is no value in duplicating the entire Tripwire documentation set. After the configuration on the development server is completed, the configuration, policy, and Tripwire key files are then bundled along with the Tripwire software into an RPM installation package.

If you have a CD-ROM from Tripwire, mount the CD-ROM and copy the /ibm_aix directory to your RPM source directory.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
cd /usr/opt/freeware/src/packages/SOURCES
mkdir -m 700 ./tripwire-4.10
cp -r /mnt/ibm_aix/* ./tripwire-4.10
umount /mnt
```

If you downloaded the software from www.tripwire.com, the TAR archive **tfs_410_en_aix_full.tgz** is built with a parent directory of "./tfs_410_aix_full". The parent directory in the TAR archive should be changed to be consistent with the RPM specification files by making the parent directory "./tripwire-4.10". Burn a CD-ROM with the TAR archive, mount it on the AIX server, copy it to the RPM source directory, and rename the parent directory.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
cd /usr/opt/freeware/src/packages/SOURCES
gunzip -c /mnt/tfs_410_en_aix_full.tgz | tar -xvf -
mv tfs_410_aix_full tripwire-4.10
umount /mnt
```

Clean up the permissions on the tripwire source.

```
chown -R root:system ./tripwire-4.10
find ./tripwire-4.10 -type d -exec chmod 700 {} \;
find ./tripwire-4.10 -type f -exec chmod 400 {} \;
chmod 500 ./tripwire-4.10/install.sh
```

Edit the installation configuration file to customize the Tripwire configuration for your site. This configuration file is read by the Tripwire install script to change default settings such as email address, reporting level, and file creation permissions. Some of the values that you may want to consider are shown below. Fortunately, the Tripwire folks put many comments in the file and the names of the parameters are self-explanatory. The manuals also explain what each value controls.

```
cd tripwire-4.10
cp install.cfg install.cfg.YYYYMMDD (save with a date stamp)
vi install.cfg
```

Edit these parameters. Notice that the file modes are changed from the factory default of 644 to a restricted 600 so that only the root user has access to these critical files. You need to supply your mail server and email address for any email deliveries. Notice the TWEVENT_TRACKING parameter is enabled so that the Tripwire reports include the information in the AIX auditing subsystem.

```
TWCFGRIGHTS=0600
TWDBRIGHTS=0600
TWREPORTRIGHTS=0600
TWPOLICYRIGHTS=0600
TWAGENTCFGRIGHTS=0600
TWSCHEDULERIGHTS=0600
TWLOGRIGHTS=0600
TWAUTHKEYRIGHTS=0600
TWTASKRIGHTS=0600
TWSMTPHOST="themailserver.foo.com"
TWEMAILREPORTLEVEL=4
TWGLOBALEMAIL="johndoe@foo.com"
TWSYSLOG=TRUE
TWSYSLOGREPORTLEVEL=2
TWEVENT_TRACKING=TRUE
INSTALL_INIT_SCRIPT=TRUE
```

Run the Tripwire installation script using your customized installation configuration file.

```
cd /usr/opt/freeware/src/packages/SOURCES/tripwire-4.10
./install.sh $(pwd)/install.cfg
```

<Screen output and prompts during the install>
<Some of the output has been omitted for brevity>

```
Installer program for:
Tripwire for Servers Version 4.1 for UNIX Operating Systems
Copyright 1998-2004 Tripwire, Inc.
Tripwire is a registered trademark of Tripwire, Inc. All rights
reserved.

LICENSE AGREEMENT for Tripwire(R) for Servers Version 4.1 for
UNIX
Please read the following license agreement.  You must accept the
agreement to continue installing Tripwire for Servers.

Press ENTER to view the License Agreement.
      <omitted output>
Please type accept to indicate your acceptance of this
license agreement. [do not accept]  accept
-------------------------------------------
Checking for programs specified in install configuration file...
      <omitted output>
Checking for a previous version of Tripwire...
      <omitted output>
Checking for an active Tripwire Agent...
      <omitted output>
Install Tripwire Agent
      <omitted output>
Install Tripwire for Servers Agent? [Y/n]  y
```

```
-----------------------------------------------
Verifying installation directories...
The installer will copy Tripwire for Servers files to the
following directories:
       TWROOT: /usr/local/tripwire/tfs
              <Various path name notices display>
        TWPDF: /usr/local/tripwire/tfs/docs
Continue with installation? [y/N]  y
Finding and creating directories...
      <omitted output>
Copying files...
      <omitted output>
Tripwire Site and Local Key Creation
      <omitted output>
Site Key Passphrase
The passphrase must be at least 8 characters long and contain at
least one digit and at least one non-digit.
Enter the site keyfile passphrase:  passphrase
Verify the site keyfile passphrase: passphrase
Generating key (this may take several minutes)...
Key generation complete.

Local Key Passphrase
The passphrase must be at least 8 characters long and contain at
least one digit and at least one non-digit.
Enter the local keyfile passphrase:       passphrase
Verify the local keyfile passphrase:      passphrase
Generating key (this may take several minutes)...
Key generation complete.

-----------------------------------------------
Generating Tripwire plaintext configuration file...
      <omitted output>
Select a mail method for e-mail reports.
    1) SMTP (default)
    2) SENDMAIL
    3) Do not send Tripwire reports by e-mail.
Enter the number of your preference: (1)  1
      <omitted output>
FQDN of your SMTP server:(mail.example.com) themailserver.foo.com
      <omitted output>
SNMP Host Information
      <omitted output>
Enable SNMP trap reporting? [y/N]  n
-----------------------------------------------
Creating signed configuration file...
Please enter your site passphrase:  passphrase
Wrote configuration file: /usr/local/tripwire/tfs/bin/tw.cfg
-----------------------------------------------
Customizing default policy file...
-----------------------------------------------
Creating signed policy file...
Please enter your site passphrase:  passphrase
Wrote policy file: /usr/local/tripwire/tfs/policy/tw.pol
-----------------------------------------------
Generating Tripwire Agent plaintext configuration file...
```

```
Specify Agent IP Address
  If this machine has more than one network interface card (NIC),
  you may specify the IP address you want Tripwire Agent to
  listen on. If you do not specify an IP address, Tripwire
  Agent uses this machine's primary NIC IP address by default.
Enter a specific IP address for Agent communication: (primary IP)

Select an Agent Port Number
  The installer did not detect a specified port number to use to
  communicate with Tripwire Manager.  We recommend that you use
  port 1169, the registered Tripwire port.
Enter the port number to use: [1-65535] (1169)
-----------------------------------------------
Creating signed Agent configuration file...
Please enter your site passphrase:  passphrase
Wrote configuration file: /usr/local/tripwire/tfs/bin/agent.cfg
-----------------------------------------------
Installing Tripwire Agent Autostart Script
      <omitted output>
On your system, the script will be copied to the directory: /etc
and added to the file /etc/inittab using mkitab.  A backup of
/etc/inittab will be saved in /tmp.

Attempt to install the start script? [Y/n]  y
/etc/inittab -> /tmp/inittab.233472
For your reference, a copy of the Tripwire Agent start script,
rc.twagent, has been copied to the directory:
/usr/local/tripwire/tfs/bin
      <omitted output>
-----------------------------------------------
The Installation succeeded.
      <omitted output>
-----------------------------------------------
Starting the Tripwire Agent
  If you plan to manage this installation with Tripwire Manager,
  you may want to start the Tripwire Agent now.  The Tripwire
  Agent allows Tripwire Manager to connect to this Tripwire
  for Servers installation.
Start the Tripwire Agent now? [Y/n]  y
The Tripwire Agent was started successfully.
      <omitted output>
-----------------------------------------------
Thank you for installing Tripwire software.
```

Add the Tripwire binaries directory to your PATH.

```
export PATH=$PATH:/usr/local/tripwire/tfs/bin
```

Customize the policy file to reduce false positives. The default policy file as supplied by Tripwire Inc. is pretty close to a production-ready version. The biggest problem that our shop encountered was many false positives. The Open Source software that the RPM file sets install use /usr/local/bin and /usr/local/etc, so these directories also need to be added. Do not be overly concerned with getting your policy perfect the first time. As software is added to

the systems, the policy requires adjustments. The goal is to create a baseline for the just the operating system itself.

Export the current policy, use a text editor to make the changes listed below, and then import the updated policy. Since this is a commercial version of Tripwire, a copy of the entire policy file "twpol.txt" is not included to avoid possible copyright issues.

```
cd /usr/local/tripwire/tfs/policy
cp -pi twpol.txt twpol.txt.YYYYMMDD (Save the original file)
twadmin --print-polfile >twpol.txt
vi twpol.txt                        (Make changes shown below)
twadmin --create-polfile twpol.txt
```

Changes to Baseline Tripwire Policy for AIX

Section: Tripwire Data Files

Original Rule:	$(TWDB)/database.twd.bak -> $(SEC_CONFIG)-G;
Replacement Rule:	!$(TWDB)/database.twd.bak;
Reason:	Reduce noise; Every time the Tripwire database is updated, the "database.twd" is updated and flagged by Tripwire. There is no need to also alter on the backup copy change.
New Rule:	!$(TWDB)/database.twd.tmp;
Reason:	Eliminate noise generated by the database temporary file.

Section: System configuration files

Uncomment:	/etc/objrepos/ -> $(SEC_CRIT)-mc (recurse=0) ;
Reason:	Eliminate false positives due to mutable AIX ODM database files.
New Rules:	/usr/local/etc -> $(SEC_CRIT); /usr/local/bin -> $(SEC_BIN); /usr/local/sbin -> $(SEC_CRIT);
Reason:	Add protection to new /usr/local directories for Open Source.
Uncomment:	/etc/lpp/diagnostics/data/ -> $(SEC_CRIT)-mc (recurse=0);
Reason:	Eliminate false positives due to mutable diagnostic data files.
New Rules:	!/etc/ntp.drift; !/etc/ntp.drift.TEMP;
Reason:	Eliminate false positives due to normal NTP daemon activity.

Section: System Directories

Delete Rule:	/audit -> $(SEC_CRIT);
Reason:	Directory is relocated during hardening process.

Section: Other Filesystems

Delete Rule:	/share -> $(SEC_CRIT)-mcb (recurse=0);
Reason:	Directory does not exist on AIX 5.

Note: This is the only rule in this section, so remove the section.

Section: Temporary directories

Original Rule: /tmp -> $(SEC_CONFIG)-ni (recurse=0);
New Rule: !/tmp;
Original Rule: /usr/tmp -> $(SEC_INVARIANT);
New Rule: !/usr/tmp;
Original Rule: /var/tmp -> $(SEC_INVARIANT);
New Rule: !/var/tmp;
Original Rule: /var/dt/tmp -> $(SEC_INVARIANT) (recurse=0);
New Rule: !/var/dt/tmp;
Reasons: Eliminate false positives due to very volatile temporary files.

Section: Variable Security Files (add this new section)

New Rule: /etc/security/failedlogin -> $(SEC_LOG)-e;
Reason: Add protection to failed login attempts log.

New Rules: /etc/security/portlog -> $(SEC_LOG)-e;
/etc/security/lastlog -> $(SEC_LOG)-e;
/etc/security/passwd -> $(Dynamic);
/etc/security/group -> $(Dynamic);
/etc/security/user -> $(Dynamic);
/etc/security/pwdhist.dir -> $(Dynamic);
/etc/security/pwdhist.pag -> $(Dynamic);
Reason: Add protection to critical authentication files.

New Rule: /etc/security/audit/config -> $(IgnoreNone)-ramc;
Reason: Eliminate false positives due to audit subsystem restarts modifying the timestamp on the audit configuration file.

New Rules: !/etc/utmp;
!/var/audit;
!/etc/security/oenviron;
!/etc/security/ogroup;
!/etc/security/olimits;
!/etc/security/ologin.cfg;
!/etc/security/opasswd;
!/etc/security/oportlog;
!/etc/security/osmitacl.group;
!/etc/security/osmitacl.user;
!/etc/security/osysck.cfg;
!/etc/security/ouser;
!/etc/security/ouser.roles;
!/etc/opasswd;
!/etc/ogroup;
!/etc/security/audit/oconfig;
!/etc/sudoers.tmp;
!/etc/security/tcbck.LCK;
Reason: Eliminate false positives on temporary/backup security files.

Customize the configuration file to suit your environment. Changes to the configuration are site dependent, and the baseline configuration provided with

the product is reasonable for most sites. Listed below are a few changes that you may wish to consider.

```
cd /usr/local/tripwire/tfs/bin
cp -pi twcfg.txt twcfg.txt.YYYYMMDD       (Save original file)
twadmin --print-cfgfile >twcfg.txt
vi twcfg.txt                          (Make changes shown below)
twadmin --create-cfgfile --site-keyfile ../key/site.key twcfg.txt
```

Changes to Baseline Tripwire Configuration for AIX

Parameter:	SYSLOGREPORTING=TRUE
Action:	Verify that this feature is TRUE. This enables Tripwire reporting to the syslog facility in addition to any email or SNMP alerts.
Parameter:	SYSLOGNOVIOLATIONS=FALSE
Action:	Change to TRUE. This logs a message to the syslog facility if no violations are found during a system check. This provides the opportunity to write a validation scan on the central log server to verify that Tripwire is running its periodic scans.
Parameter:	SYSLOG_CONST=TRUE
Action:	Change to TRUE. This instructs Tripwire to log all events, not just the events related to Tripwire's configuration itself.
Parameter:	MAIL_LOCALIZED=TRUE
Action:	Change to FALSE. This disables Japanese localization of email.

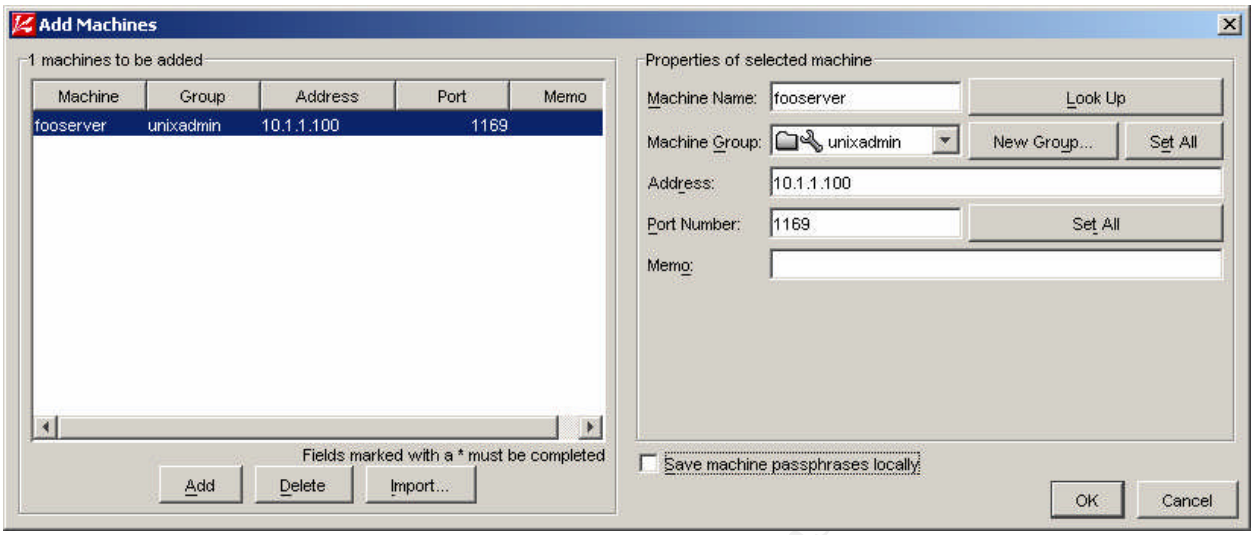
Create the new Tripwire signature database.

```
tripwire --init
```

The following screen output is generated. Do not be concerned about complaints of missing files.

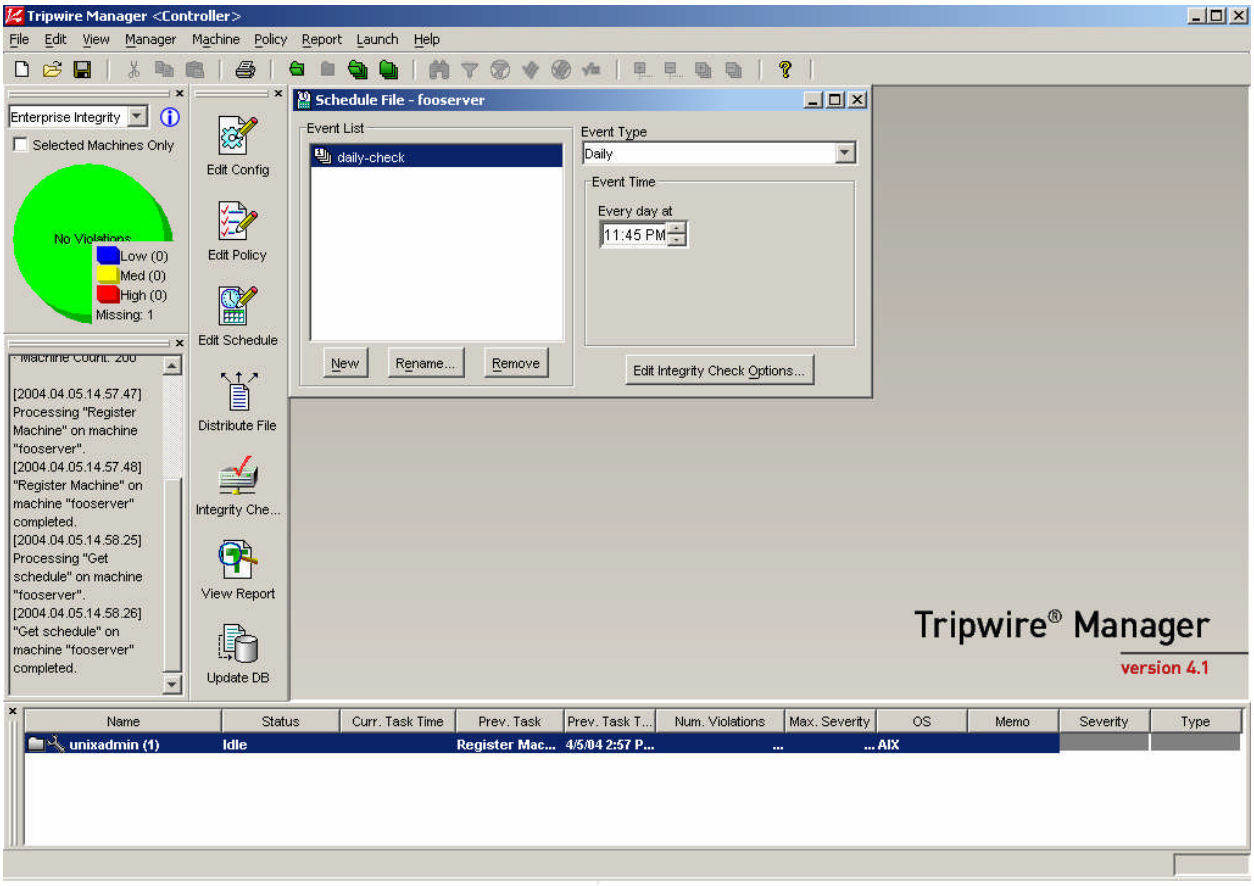
```
Parsing policy file: /usr/local/tripwire/tfs/policy/tw.pol
Generating the database...
*** Processing Unix File System ***
Note: Tripwire could not find the following objects:
   /.dt
   /usr/local/tripwire/tfs/report/agent.log
   /usr/local/tripwire/tfs/key/authentication.dat
   /usr/lpp/X11/bin
   /usr/dt/bin
   /etc/security/pwdhist.dir
   /etc/security/pwdhist.pag
   /.dtprofile
   /.Xauthority
Please enter your local passphrase: <supply your passphrase>
Wrote database file: /usr/local/tripwire/tfs/db/database.twd
The database was successfully generated.
```

Launch the Tripwire Manager Console software and register this server using the menu options Manager / Add Machines (screen shot shown below). This creates the **/usr/local/tripwire/tfs/key/authentication.dat** file.

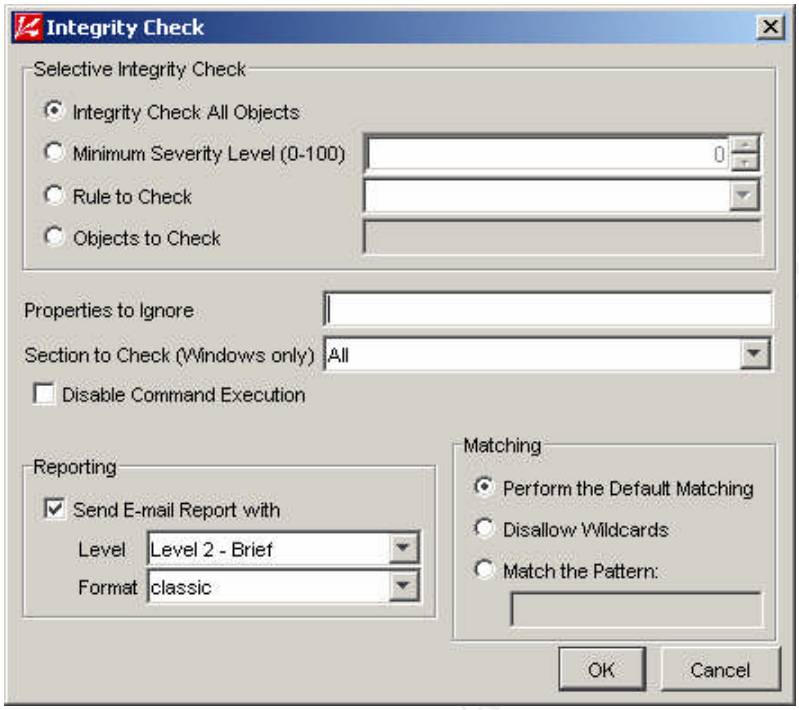


Launch the Tripwire Manager Console software and schedule this server for daily integrity checks using the **Edit Schedule** button (screen shot shown below). This creates the **/usr/local/tripwire/tfs/db/schedule.dat** file.

Click on the **Rename** button and give the job a meaningful name like "daily-check". Schedule the job for late in the evening or some other off-hours time.



Click on the **Edit Integrity Check Options** button to adjust any detailed options such as including an email report.



Adjust the permissions on the schedule data file since Tripwire creates it with world-read permissions.

```
chmod 600 /usr/local/tripwire/tfs/db/schedule.dat
```

2.6.6 Create the Tripwire RPM Installation Package

With the Tripwire "Golden Image" created, you are now ready to prepare an RPM file set for installation of the Tripwire software and configuration across the enterprise.

Create a TAR archive of the Tripwire source.

```
cd /usr/opt/freeware/src/packages/SOURCES
tar -cvf - ./tripwire-4.10 | gzip -c >tripwire-4.10.tar.gz
chown root:system tripwire-4.10.tar.gz
chmod 640 tripwire-4.10.tar.gz
```

Create the RPM custom configuration TAR archive containing your installation configuration changes, key files, and policy. The RPM specification file installs the files when you install the Tripwire RPM.

```
cd /usr/opt/freeware/src/packages/SOURCES
```

```
cp -p tripwire-4.10/install.cfg .
cp -p /usr/local/tripwire/tfs/bin/agent.cfg .
cp -p /usr/local/tripwire/tfs/bin/tw.cfg .
cp -p /usr/local/tripwire/tfs/policy/tw.pol .
cp -p /usr/local/tripwire/tfs/key/local.key .
cp -p /usr/local/tripwire/tfs/key/site.key .
cp -p /usr/local/tripwire/tfs/key/authentication.dat .
cp -p /usr/local/tripwire/tfs/db/schedule.dat .
            (The following three lines are one long command)
tar -cvf – install.cfg agent.cfg tw.cfg tw.pol local.key site.key
            authentication.dat schedule.dat |
            gzip -c >tripwire-4.10-config.tar.gz
chmod 600 tripwire-4.10-config.tar.gz
chown root:system tripwire-4.10-config.tar.gz
            (The following two lines are one long command)
rm install.cfg agent.cfg tw.cfg tw.pol local.key site.key
            authentication.dat schedule.dat
```

Create the RPM installation file set.

```
cd /usr/opt/freeware/src/packages/SPECS
rpm –ba tripwire.spec
```

Remove the Tripwire source directory since it is no longer needed.

```
rm -rf ./tripwire-4.10
```

2.7 Harden the Operating System Image

With all of our software now packaged as RPM installation file sets, we can begin the process of configuring the Operating System. This process is accomplished using the hardening scripts supplied in the attached ZIP file, which are now conveniently packaged into an RPM binary on your development server.

The hardening scripts perform a lot of work, and it is important to understand what they are doing. The resulting operating system configuration works nicely in our shop, but your environment may need a few small adjustments. Understanding each script's actions and the associated configuration files that drive the scripts will enable you to easily tailor the procedures to your environment. The name of each script that is called by the menu is shown in each section heading below as a convenient reference. Guidelines for editing and repackaging the RPM file set are explained further below.

Any original system configuration files that are modified during the script executions are saved as *filename*.yyyymmdd_hhmmss (date-time stamp).

2.7.1 Install the Hardening Scripts

Issue the following commands to install the hardening scripts.

```
cd /opt/freeware/src/packages/RPMS/ppc
rpm -ivh aix-harden-5.2.1.0-0.aix5.2.ppc.rpm
```

2.7.2 Execute the Hardening Scripts

The hardening process includes a menu script (setup_aix.sh) that allows you to individually select processes to run, or to run all of them in a non-interactive mode. There are a few command line options available, which are displayed by supplying the "-?" argument as shown below. Each of the individual processing scripts that are called by the menu can also be run manually, and they display a help message using the "-?" argument too.

The AIX Installation CD-ROMs automatically install X11 graphical software and manual pages. Our shop normally does not install these features, but some shops do. The X and M flags prevents the removal of that software during the hardening process. Some shops also use a centralized authentication store for user credentials such as RADIUS or LDAP. RADIUS authentication is included with this process and the option to enable the RADIUS uses the R flag. The configuration will then use the local /etc/security/passwd file that is native to AIX.

```
cd /usr/local/bin
./setup_aix.sh -?
```

(Screen output)

```
Usage: setup_aix.sh -X -M –R -D

Actions: installation setup for AIX

Optional parameters:
-X enables the installation of X11 software, default is no X11
-M enables the installation of man pages, default is no man pages
-R enables the installation of RADIUS authentication, default is no RADIUS
-D disables removal of development tools and libraries, default is to remove
```

Run the hardening process. Since we are building a development server, we add the "-D" command line flag to prevent removing development file sets such as application development libraries and the IBM C compiler licensing service. As a demonstration of alternative authentication mechanisms, the "-R" flag is supplied to enable RADIUS authentication.

```
cd /usr/local/bin
./setup_aix.sh -R -D
```

(Screen output – notice the command line flags are displayed at the top)

```
AIX 5.2.0.0 INSTALLATION           -R -D
 0. Run the entire installation
 1. Mirror the rootvg logical volumes
 2. Configure the filesystems
 3. Configure LPP filesets
 4. Apply latest maintenance level filesets
 5. Configure file permissions
 6. Configure init inetd and rc daemons
 7. Configure security files
 8. Configure RADIUS
 9. Configure users and groups
10. Configure RPM filesets
11. Configure error logging
12. Configure cron
13. Configure Trusted Computing Base
14. Configure misc items
15. Configure auditing system
16. Configure tripwire
17. Configure boot devices
18. Remove installation utilities

Enter selection, or x to exit:
```

The menu displays. Option 0 (zero) runs the entire installation. Optionally, you can run selected portions of the hardening. One note of caution: The hardening steps are ordered carefully because there are some dependencies. For example, we apply maintenance patches in step 4 after we installed any add-on

software in step 3 because we want the add-on software to receive all of the possible maintenance updates. If for some reason you find a need to run a selective hardening sequence, perform the steps in ascending numerical order.

Enter the 0 (zero) and press the ENTER key. The hardening process starts.

2.7.2.1 Mirror the rootvg logical volumes (setup_mirror.sh)

System availability is a key component of a secure system. Mirroring of the root volume group provides disk redundancy for when a hard drive crashes. If your systems provide hardware level raid, you do not need this step.

The script examines the root volume group for any partitions that are not mirrored. If any are found, the following prompt displays.

```
There are unmirrored logical volumes in the rootvg volume group.
The current configuration will be displayed so that you can
decide what actions need to taken in order to complete the
mirroring.
Press ENTER to display the current configuration.
```

Press the ENTER key. The volume group configuration displays.

```
===== ALL PHYSICAL VOLUMES ========================================
hdisk0          0006ccffc4447ed4                    rootvg          active
hdisk1          0006ccff42f322a4                    None
===== ROOT VOLUME GROUP USES THE FOLLOWING PHYSICAL VOLUMES ==========
rootvg:
PV_NAME           PV STATE       TOTAL PPs   FREE PPs   FREE DISTRIBUTION
hdisk0            active         542         324        108..00..00..107..109
==== LOGICAL VOLUMES STATUS ========================================
rootvg:
LV NAME             TYPE       LPs   PPs   PVs  LV STATE      MOUNT POINT
hd5                 boot       1     1     1    closed/syncd  N/A
hd6                 paging     16    16    1    open/syncd    N/A
hd8                 jfs2log    1     1     1    open/syncd    N/A
hd4                 jfs2       4     4     1    open/syncd    /
hd2                 jfs2       128   128   1    open/syncd    /usr
hd9var              jfs2       48    48    1    open/syncd    /var
hd3                 jfs2       16    16    1    open/syncd    /tmp
hd1                 jfs2       4     4     1    open/syncd    /home
====================================================================
Standard input: END
```

Press ENTER at the end of the display paging, and the following prompt displays.

```
Options:
P. Add a physical volume to rootvg
X. Exit
```

Enter P to add physical disk for mirroring, or X to exit and skip mirroring completely.

If you are mirroring your drives and P was selected, available hard drives are displayed. Choose a hard drive number to use (1).

```
Available physical volumes:
1. hdisk1 18200MB
X. Exit
Select the physical volume to add: 1
```

You are prompted for confirmation.

```
About to add hdisk1 to rootvg.  OK (y,n): y
```

The script examines the root volume group configuration, and determines that we have an available drive to use, but we need to execute the mirroring. The following prompt displays.

```
There are unmirrored logical volumes in the rootvg volume group.
The current configuration will be displayed so that you can
decide what actions need to taken in order to complete the
mirroring.
Press ENTER to display the current configuration.
```

Press the ENTER key. We can see that the second hard drive (hdisk1) is now active. The screen output below is truncated to show only the new disk.

```
===== ALL PHYSICAL VOLUMES ===================================
hdisk0          0006ccffc4447ed4         rootvg          active
hdisk1          0006ccff42f322a4         rootvg          active
            <Same output as previous display above>
Standard input: END
```

You are prompted to mirror the logical volumes within the root volume group. Enter an M to choose mirroring.

```
Options:
M. Mirror one or more logical volumes
X. Exit
Enter your selection: M
```

All partitions display. You can choose to mirror selected partitions, or mirror all of them. We will choose A for all volumes in this demonstration.

```
Unmirrored logical volumes:
    LV NAME    TYPE     LPs  PPs   PVs  LV STATE      MOUNT POINT
 1. hd5        boot     1    1     1    closed/syncd  N/A
 2. hd6        paging   16   16    1    open/syncd    N/A
 3. hd8        jfs2log  1    1     1    open/syncd    N/A
 4. hd4        jfs2     4    4     1    open/syncd    /
 5. hd2        jfs2     128  128   1    open/syncd    /usr
 6. hd9var     jfs2     48   48    1    open/syncd    /var
 7. hd3        jfs2     16   16    1    open/syncd    /tmp
 8. hd1        jfs2     4    4     1    open/syncd    /home
 A. All Volumes
 X. Exit
Select the logical volume to mirror:
```

You are prompted for confirmation.

```
About to mirror all logical volumes.  OK (y,n): y
```

The mirroring proceeds.

```
Mirroring hd5 ...
Mirroring hd6 ...
Mirroring hd8 ...
Mirroring hd4 ...
Mirroring hd2 ...
Mirroring hd9var ...
Mirroring hd3 ...
Mirroring hd1 ...
Mirroring completed. Press ENTER.
```

This completes the disk mirroring process.

2.7.2.2 Configure the filesystems (setup_filesystems.sh)

This script performs the following actions.

- Expand the file systems as specified in the script configuration file setup_filesystems.conf. You may wish to edit the configuration file to adjust the values to suit your needs. The initial file systems as installed from CD-ROM are rather small. They are expanded as follows:

/	128 MB
/usr	1536 MB
/var	1536 MB
/tmp	512 MB
/home	128 MB
/mksysb	2048 MB

  These are reasonable values for most shops. If your specific needs differ, you can edit the script to supply your values. Look at the routine “expand filesystems” in the script and you will see the obvious lines to edit.

- Migrate opt file system contents to /usr/opt. Remove file system /opt. Our shop sees no need for the /opt file system to be separate. We like to migrate it to within the /usr file system into /usr/opt. Your mileage may vary.

- Migrate /audit directory contents to /var/audit.
  The /audit directory, which resides in the root file system, is where the AIX auditing subsystem places its output. We will enable auditing, so lots of output is going to be placed into this directory. The root file system is a bad choice for this, so the scripts move the contents to /var/audit and create a symbolic link from /audit. You should monitor your /var file system usage since this is where all of the auditing and syslog output is placed.

- Create the /mksysb file system.
  Our shop creates a nightly “mksysb” backup in the /mksysb file system for system recovery purposes. This is a common practice. As any AIX administrator knows, this is also very handy for migrating the operating system to a different piece of hardware. We like having this in a separate file system, but your preference may differ. The nightly tape backups include this file system so that the image is copied to tape.

- Expand swap.
  The default swap space is very small. Each shop uses their estimation method for calculating how much to allocate, so you may want to examine the “expand swap paging space” routine in the script. It is clearly commented. We use a 50% of real memory calculation, with a 2GB minimum value.

- Configure dump devices.
  The command “sysdumpdev -e” gives the recommended dump partition size, but IBM support technicians informed us that adding a 20% is a good idea. The script uses this calculation.

- Make the CD-ROM mount point and file system entry.
  This is an administrator’s convenience issue. Adding the CD-ROM device to the mount point in /etc/filesystems makes mounting the CD-ROM a little quicker.

The script output is as follows.

```
setup_filesystems.sh: start Sat Feb 28 17:51:44 EST 2004
mksysb
File system created successfully.
2096884 kilobytes total disk space.
New File System size is 4194304
REALMEM=1024 SWAP_TARGET=2048 SWAP_SIZE=512 PPSIZE=32
setup_filesystems.sh: adding 48 partitions to swap space hd6
lg_dumplv
lg_dumplv2
setup_filesystems.sh: end Sat Feb 28 17:52:01 EST 2004
```

2.7.2.3 Configure LPP file sets (setup_lpp.sh)

This script performs the following actions.

- Installs any site-specific LPP file sets found in the directories underneath /opt/freeware/src/packages/LPP

  This action was described in the section “Install Any Add-On Software” above. This step installs any extra IBM LPP file sets (backup software, Tivoli products, etc) that your site requires.

- The following unnecessary AIX LPP file sets are removed:

Java*	bos.docsearch.*
bos.msg.en_US.docsearch.*	bos.msg.en_US.txt.tfs
bos.net.snapp	bos.net.uucp
bos.sysmgt.nim.master	bos.sysmgt.nim.spot
bos.sysmgt.quota	bos.sysmgt.trcgui_samp
csm.* ssp.* sysmgt.*	tivoli.tsm.client.ba.32bit.web

- If the X11 packages option was not selected (-X), the following unnecessary AIX LPP file sets are removed:

X11.adt.lib	X11.apps.aixterm
X11.apps.clients	X11.apps.config
X11.apps.custom	X11.apps.rte
X11.apps.util	X11.apps.xterm
X11.base.common	X11.base.lib
X11.base.rte	X11.base.smt
X11.base.xpconfig	X11.fnt.coreX
X11.fnt.defaultFonts	X11.fnt.iso1
X11.loc.en_US.base.lib	X11.loc.en_US.base.rte
X11.motif.lib	X11.motif.mwm
X11.msg.en_US.apps.aixterm	X11.msg.en_US.apps.clients
X11.msg.en_US.apps.config	X11.msg.en_US.apps.custom
X11.msg.en_US.apps.rte	X11.msg.en_US.base.common
X11.msg.en_US.base.rte	X11.msg.en_US.motif.lib
X11.msg.en_US.motif.mwm	bos.txt.spell
bos.txt.spell.data	bos.txt.tfs
bos.txt.tfs.data	rsct.*

- If the development packages option was not selected (-D), the following unnecessary AIX LPP file sets are removed:

bos.adt.base	bos.adt.include	bos.adt.lib
bos.net.ncs	bos.net.nis.client	bos.net.tcp.adt
ifor_ls.base.cli	ifor_ls.msg.en_US.base.cli	

The script output is as follows.

```
setup_lpp.sh: start Sat Feb 28 18:55:26 EST 2004
setup_lpp.sh: logging software installation to
/var/adm/setup_lpp.229390.log
setup_lpp.sh: logging fileset removals to
/var/adm/setup_lpp.229390.log
setup_lpp.sh: end Sat Feb 28 18:56:42 EST 2004
```

If any errors occur, the script traps them and complains to the screen. A log file is written to /tmp that records software installation and removal. The IBM installation utility “installp” that the script runs will generate a large amount of screen activity. If any problems occur, they scroll off the screen and the

administrator has no idea what happened. By writing the actions to this log, the administrator can review the log to see what occurred.

2.7.2.4 Apply latest maintenance level filesets (setup_maintlevel.sh)

This script installs all of the latest maintenance level patches to the operating system. IBM provides periodic updates to the operating system that include all patches since the last maintenance level release, bug fixes, and general enhancements.

You may need to archive the maintenance level sets for a few versions if you have some servers that cannot be upgraded for operational or political reasons. To accommodate this, the script locates the latest maintenance level in a subdirectory using the maintenance level number (i.e. 5200-01 vs. 5200-02).

The script disables the Trusted Computing Base and then enables it after the upgrade is completed. This is to accommodate a bug in the AIX upgrade process for TCB enabled servers. This should only be a temporary workaround until IBM fixes the problem.

This script performs the following actions.

- Disable the Trusted Computing Base.
- Install the LPP file set “bos.rte.install” since it is needed for the installation process itself.
- Install all of the maintenance level files located in the directory /opt/freeware/src/packages/MAINT/5200-02 (where 5200-02 is the current maintenance release number).
- Install all of the interim patches located in the directory /opt/freeware/src/packages/PATCHES/5200-02 (where 5200-02 is the current maintenance release number).
- Enable the Trusted Computing Base.

The script output is as follows.

```
setup_maintlevel.sh: start Sat Feb 28 19:30:39 EST 2004
setup_maintlevel.sh: disable TCB to accommodate bug in maint
level files
setup_maintlevel.sh: applying maint level 5200-02 ...  Logging to
/var/adm/setup_maintlevel.maint.258082.log
setup_maintlevel.sh: applying latest patches ...  Logging to
/var/adm/setup_maintlevel.patches.258082.log
setup_maintlevel.sh: reset TCB to original state: CC_EVAL
```

```
setup_maintlevel.sh: We must REBOOT the server so that the
updates can take effect.
You should restart the installation after the reboot completes.
Reboot now y,n: y
```

This script traps the output to files in /tmp as did the previous step. If the script reports an error, check the log file for details.

You are prompted to reboot. IBM recommends the reboot after applying the maintenance level, so the script advises the administrator to boot. Enter Y at the prompt, and wait for the machine to reboot.

After the server reboots, log in on the console as root. Issue the following commands to continue the hardening process. This will execute the menu script again.

```
cd /usr/local/bin
./setup_aix.sh -R -D
```

Select option 0 to run the entire installation. The menu script detects that you are continuing the installation. You are prompted to skip previously completed portions. Enter Y at the prompt.

```
Some steps were run at a previous time.  Skip completed steps
y,n,x=exit ? y
```

2.7.2.5 Configure file permissions (setup_perms.sh)

This script sets file permissions (owner, group, and mode) as specified in the two configuration files **setup_perms.conf** and **setup_perms_local.conf**. File permission changes are also recorded in the Trusted Computing Base configuration file /etc/security/sysck.cfg.

The configuration file setup_perms.conf restricts the default permissions as installed by the AIX CD-ROMs. Read, write, and execute permissions for the "others" level is removed from many executables, particularly if they have the set-user-id (SUID) or set-group-id (SGID) bits turned on. Since a common exploit technique for gaining root access is to exploit vulnerability in an SUID binary, by restricting non-root users from running such binaries reduces the exposure. This technique cannot be used on all SUID binaries, or system operation may be impaired. The "passwd" command is an example of such since everyone needs to be able to set their password using this command and it has the SUID bit enabled. Some non-SUID binaries also have the "others" permission removed since there is no reason that general users should need these commands in our shop. One example is the "ipcrm" command for removing shared-memory segments.

The list of binaries included in this data file and the exact permissions have been determined by trial-and-error. It works well in our shop, but you may need to adjust a few permissions to suit your needs.

The second configuration file setup_perms_local.conf handles local system deviations from the standard configuration. Some machines may need to have a few commands permissions adjusted for special user or application requirements on those hosts. In order to prevent losing customizations in the event that this script is executed later, those customizations can be entered into this configuration file, which overrides any setting in the baseline setup_perms.conf configuration.

The script output is as follows.

```
setup_perms.sh: start Sat Mar 6 16:16:48 EST 2004
setup_perms.sh: Logging changes to log file
/var/adm/setup_perms.9280.log
setup_perms.sh: end Sat Mar 6 16:18:01 EST 2004
```

2.7.2.6 Configure init, inetd, and rc daemons (setup_daemons.sh)

This script disables any unnecessary daemon processes that are executed at startup time. In the AIX system these can be started from four different configuration locations, so all four are addressed in this procedure. Every service that is disabled is listed in a configuration file so that you can customize what is disabled to suit your particular requirements.

This script performs the following actions.

- It removes any unnecessary daemon processes that are started in the **/etc/inittab** system configuration file. Daemons to be removed are specified in the script configuration file **setup_daemons_init.conf**.
  - piobe — printer I/O backend
  - qdaemon — queue daemon for printing
  - writesrv — allows TTYs to write notes to each other
  - uprintfd — kernel messaging, generally unused

- It removes any unnecessary daemon processes that are started in the **/etc/inetd.conf** system configuration file. Daemons to be removed are specified in the script configuration file **setup_daemons_inetd.conf**. The inetd configuration has no services configured after this process completes, so inetd itself could be disabled. Our shop uses some applications that start from inetd, so it is not disabled in this procedure, but you may elect to do so.
  - comsat — notifies incoming electronic mail
  - daytime — an obsolete time service
  - ftpd — FTP (file transfer protocol) daemon
  - fingerd — finger daemon
  - rlogind — remote login daemon
  - rexecd — remote execution daemon

rshd	remote shell daemon
sendmail	mail delivery daemon
talkd	tool talk daemon
telnetd	telnet daemon
time	an obsolete time service
tftpd	TFTP (trivial file transfer protocol) daemon
uucpd	UUCP (Unix-to-Unix copy) daemon

- It removes any unnecessary daemon processes that are started in the /etc/rc.tcpip system configuration file. Daemons to be removed are specified in the script configuration file **setup_daemons_tcpip.conf**.

/usr/sbin/aixmibd	SNMP MIB data collection daemon
/usr/sbin/hostmibd	SNMP DPI2 daemon
/usr/sbin/muxatmd	ATM network MUX daemon
/usr/sbin/portmap	RPC port map daemon
/usr/sbin/snmpd	SNMP main service daemon
/usr/sbin/snmpmibd	SNMP MIB daemon
/usr/sbin/syslogd	IBM syslog daemon (replaced by Syslog-NG daemon)

- It removes any unnecessary daemon processes that are started in the /etc/rc.nfs system configuration file. Daemons to be removed are specified in the script configuration file **setup_daemons_nfs.conf**.

nfsd	Network File Systems daemon
rpc.lockd	NFS RPC lock daemon
rpc.mountd	NFS RPC mount daemon
rpc.statd	NFS RPC status daemon
keyserv	Key service daemon for NIS/NFS login process
nis_cachemgr	NIS cache manager daemon
rpc.nispasswdd	NIS password update daemon
rpc.nisd	NIS service daemon
rpc.yppasswdd	NIS password request daemon
ypbind	NIS client daemon
ypserv	NIS man daemon
ypupdated	NIS information update daemon

- It installs a new RC script **/etc/setup_rc.netparms** that adjusts kernel parameters that reduce vulnerabilities in the IP protocol suite. This script is added to the **/etc/inittab** system startup configuration.

rfc1323=1	Enables extended TCP/IP protocol features
tcp_sendspace=524288	Expands kernel space for TCP transmission
tcp_recvspace=524288	Expands kernel space for TCP reception
bcastping=0	Disables response ICMP broadcast pings
clean_partial_conns=1	Improves SYN attack protection
directed_broadcast=0	Prevents directed broadcasts to the gateway
icmpaddressmask=0	Prevents ICMP address mask requests
ipforwarding=0	Disables IP packets forwarding if multi-homed

ipignoreredirects=1	Disables responses to ICMP routing redirection
ipsendredirects=0	Disables sending ICMP routing redirection
ip6srcrouteforward=0	Disables forwarding of source routed packets
ipsrcrouteforward=0	Disables forwarding of source routed packets
ipsrcrouterecv=0	Drops source routed packets that are received
ipsrcroutesend=0	Prevents source routed packet transmissions
nonlocsrcroute=0	Prevents strictly source routed packet sending
tcp_pmtu_discover=0	Disables TCP path MTU discovery
udp_pmtu_discover=0	Disables UDP path MTU discovery

The script output is as follows.

```
setup_daemons.sh: start Sat Mar 6 17:47:18 EST 2004
0513-095 The request for subsystem refresh was completed successfully.
setup_daemons.sh: end Sat Mar 6 17:47:18 EST 2004
```

2.7.2.7 Configure security files (setup_sec_files.sh)

This script configures several files in the /etc/security directory to improve the security related settings for user passwords, default groups for new users, login controls, environmental size limits (ulimits), and a default user profile.

This script performs the following actions.

- It touches a password dictionary file, which will be installed later

- It edits the system configuration file **/etc/security/user** to include the following settings for the default stanza:

umask="077"	default file creation mask
pwdwarntime=5	number of days warning of password expiration
loginretries=3	number of failed login attempts before locking account
histexpire=52	passwords can not be reused for 52 weeks
histsize=20	number of password iterations are allowed
maxage=8	maximum age in weeks before password change
maxexpired=1	maximum allowed number of weeks passed maxage
minalpha=2	minimum number of alphabetic in password
minother=2	minimum number of other characters in password
mindiff=4	minimum number of unique characters in password
maxrepeats=2	maximum number of repeated characters in password
dictionlist=/usr/share/dict/words	file for password dictionary checks

- It creates a new group SUADMIN. Users must belong to this group to be able to “su” to the root account. This makes use of a stolen root password more difficult since it limits which users are allowed to become root.

- It edits the system configuration file **/usr/lib/security/mkuser.default** to set the default group list for new system administrator accounts. The "admin" stanza's group list is set to "system,staff,SUADMIN".

- It edits the system configuration file **/etc/security/login.cfg** to include the following settings for the default stanza:
  logindisable=3 number of failed login attempts before locking port
  logininterval=60 seconds between failed logins before locking port
  loginreenable=30 minutes after which locked port is enabled
  logindelay=5 seconds to delay new login prompt after failed attempt
  herald= acceptable user banner to present at login
  "**\n\r***WARNING: To protect the system from unauthorized use and to ensure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Automated Information System is prohibited and could be subject to criminal and civil penalties.***\n\r***login: "*

- It edits the system configuration file **/etc/security/login.cfg** file to specify the valid shells in the "usw" stanza:
  /bin/sh /bin/bsh /bin/csh /bin/ksh /bin/tsh
  /usr/bin/sh /usr/bin/bsh /usr/bin/csh /usr/bin/ksh /usr/bin/tsh

- It edits the system configuration file **/etc/security/limits** to include the following settings for the default stanza. Other than disabling core files to prevent passwords from being exposed in them, these values may vary a lot for your site, so review them carefully. Our shop needs these specific values. The "root" stanza is also edited for zero core size.
  fsize= -1 disables the soft maximum file size that a user can create
  core=0 ensures that core files have a zero size
  cpu= -1 disable the CPU limits for a user process
  data= -1 disables the soft maximum process data segment size
  rss=65536 sets the soft maximum limit for process memory allocation
  stack=65536 sets the soft maximum process stack size
  nofiles=2000 sets the soft maximum number of open files

- The script configuration file **setup_profile.conf** is copied to the default skeleton profile **/etc/security/.profile** for new users. We are primarily interested in removing the PATH environment variable from individual users' profiles so that the system-wide profile determines the default PATH in one central configuration file. You may wish to customize this file for your needs.

The script output is as follows.

```
setup_sec_files.sh: start Sat Mar 6 19:07:20 EST 2004
setup_sec_files.sh: end Sat Mar 6 19:07:21 EST 2004
```

2.7.2.8 Configure RADIUS (setup_radius.sh)

This script configures RADIUS as a centralized, remote authentication mechanism. If you want to use a different remote authentication mechanism such as LDAP, the configuration changes are very similar. You can use this script as a basis for implementing the LDAP configuration changes.

IBM's web site documents alternative authentication mechanisms with Pluggable Authentication Modules (PAM) at URL: http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm (3 May 2004). You need to click on the PAM link in the left frame so that the right frame displays the PAM page.

This web page describes in detail the IBM implementation of PAM and its integration to the AIX security subsystem. It is somewhat confusing in its explanation of the exact configuration changes required to implement authentication mechanisms such as LDAP or RADIUS. The setup_radius.sh script demonstrates exactly what needs to be done during the implementation.

It should be noted that the specific authentication method is configured on an individual user basis. This allows you to choose classic passwd authentication for the root user and other "system" accounts such as root, oracle, apache, or sshd, and choose PAM authentication for regular user accounts that login to the system.

This script performs the following actions.

- It edits the system configuration file **/etc/security/user** to include the following settings for the default stanza. These are the original default entries, but the "registry" parameter is not explicitly set. The missing default causes bugs when the alternative PAM authentication is assigned to individual users, so it is very important that this is configured. It also sets the password expiration for the user to never expire, since this is controlled by the RADIUS server itself.

```
registry=files
SYSTEM=compat
maxage=0
```

- It edits the system configuration file **/usr/lib/security/methods.cfg** to enable PAM as an authentication method. The IBM web site mentioned above describing PAM explains this as follows:

  *AIX security services can be configured to call PAM modules through the use of the existing AIX loadable authentication module framework. When the **/usr/lib/security/methods.cfg** file is set up correctly, the PAM load module routes AIX security services*

*(**passwd**, **login**, and so on) to the PAM library. The PAM library checks the **/etc/pam.conf** file to determine which PAM module to use and then makes the corresponding PAM SPI call. Return values from PAM are mapped to AIX error codes and returned to the calling program.*

The specific changes to this configuration file are the addition of the following lines:

```
PAM:
        program = /usr/lib/security/PAM

PAMfiles:
        options = auth=PAM,db=BUILTIN
```

- It changes existing regular user accounts to use PAM for authentication and existing system accounts to use local passwd authentication. Regular accounts are actual users who are permitted to login. This excludes system accounts such as root or sshd. In order to keep our users organized into these two groups, our shop numbers system accounts from 0 to 199 and regular accounts from 200 and above. The script examines the user id number and adjusts the authentication accordingly.

  User id < 200

  ```
  registry=files
  SYSTEM=compat
  maxage=0
  ```

  User id => 200

  ```
  registry=PAMfiles
  SYSTEM=PAMfiles
  ```

The script output is as follows.

```
setup_radius.sh: start Sat Mar 13 18:25:00 EST 2004
setup_radius.sh: end Sat Mar 13 18:25:01 EST 2004
```

2.7.2.9 Configure users and groups (setup_users.sh)

This script removes unwanted users and groups, renumbers some users and groups, adds the system administrators' personal accounts, and adjusts some of the attributes of the root account.

This script performs the following actions.

- It removes unwanted users as listed in the script configuration file **setup_users_udel.conf**. These accounts are not needed and could possibly be abused, so they are removed. You can adjust the list if you have special needs. These users should not own any files or directories, but the user "nobody" is assigned to any files without an owner just to be

sure. The snapp user has a profile /usr/sbin/snapp/.profile which is removed.

guest lp lpd uucp nuucp snapp

- It removes unwanted groups as listed in the script configuration file **setup_users_gdel.conf**. These groups are not needed and could possibly be abused, so they are removed. You can adjust the list if you have special needs. These groups should not own any files or directories, but the group "nobody" is assigned to any files without a group just to be sure.

  uucp ecs usr perf snapp

- It renumbers any groups to a specific group id number that you may want as listed in the configuration file **setup_users_gnum.conf**. After the groups are renumbered, the groups are corrected on all existing files and directories with the old number. For consistency, our shop numbers the system groups for add-on software in the 100-199 range.

  sshd 100

- It renumbers any users to a specific user id number that you may want as listed in the configuration file **setup_users_unum.conf**. After the users are renumbered, the users are corrected on all existing files and directories with the old number. For consistency, our shop numbers the system accounts for add-on software in the 100-199 range.

  sshd 100
  invscout 150

- It creates a new group SUADMIN. Users must belong to this group to be able to "su" to the root account. This makes use of a stolen root password more difficult since it limits which users are allowed to become root.

- It adds our system administration staff's personal user accounts. This ensures our administrators are able to login onto new machines. You need to edit the configuration file **setup_users_admin.conf** to add your staff's accounts. These accounts are created with primary group = system, other groups = system, staff, SUADMIN. If RADIUS is selected, the maxage is set to zero since the RADIUS server controls password expiration.

  doej 200 John Doe

  If RADIUS is not chosen as an installation option, you are prompted to set an initial password for each account. After building a new machine, you need to inform your fellow administrators what their password is so that they change it when forced upon initial login. If RADIUS is chosen as an

option, the flag that forces these new users to set their password on initial login is cleared since the password is on the RADIUS server.

- It sets various root account parameters.

  Core file size is set to zero since we do not want passwords inadvertently appearing in core files somewhere in the file system.

  Remote login disabled. Administrators must login using their own account and "su" to the root account.

  The root home directory is moved from "/" to "/home/root". This is our shop's preference to prevent administrators from accidentally filling the root file system. We would rather have them accidentally fill the home file system to avoid headaches.

The script output is as follows.

```
setup_users.sh: start Sat Mar 13 21:08:00 EST 2004
setup_users.sh: end Sat Mar 13 21:08:05 EST 2004
```

2.7.2.10 Configure RPM filesets (setup_rpm.sh)

This script installs the RPM sets that you compiled earlier, and it removes a few unwanted RPM sets that are installed from the initial IBM CD-ROM. The particular RPM sets to be added or deleted are listed in script configuration files that you can customize to suit your needs.

This script performs the following actions.

- It removes unwanted RPM sets as specified in the script configuration file **setup_rpm_del.conf**. The following RPM sets are removed.
  cdrecord
  mkisofs

- It installs **aix-never-delete-1.0-0.aix5.2.ppc.rpm**. This RPM is intended to help prevent the accidental removal of aix-config-5.2.1.0-0.aix5.2.ppc.rpm, which installs your site-specific configuration files such the system profile, DNS resolver, NTP time configuration file, and others. This is accomplished using a circular dependency in the RPM specification file for the RPM sets. Each has a dependency on the other, so the only way to remove the aix-config RPM is to either specify the "—no-deps" option for ignoring dependencies or to simultaneously delete the aix-never-delete RPM. This prevents an administration from accidentally performing an "rpm –e aix-config" which would remove several important

configuration files. Notice the name “aix-never-delete” also gives an uninformed administrator a hint that he is doing something wrong.

- It installs the RPM sets as specified in the script configuration file **setup_rpm_add.conf**. The following RPM sets are added.
  - bash-2.05a-1.aix4.3.ppc.rpm
  - aix-bin-5.2.1.0-0.aix5.2.ppc.rpm
  - aix-config-5.2.1.0-0.aix5.2.ppc.rpm
  - aix-tsm-5.1.5-1.aix5.2.ppc.rpm
  - libol-0.3.9-1.aix5.2.ppc.rpm
  - lsof-4.61-3.aix5.1.ppc.rpm
  - openssh-3.7.1p2-1.aix5.2.ppc.rpm
  - openssh-clients-3.7.1p2-1.aix5.2.ppc.rpm
  - openssh-server-3.7.1p2-1.aix5.2.ppc.rpm
  - openssl-0.9.6m-2.aix5.1.ppc.rpm
  - prngd-0.9.27-1.aix5.2.ppc.rpm
  - radius-client-1.1-0.aix5.2.ppc.rpm
  - sudo-1.6.7p5-2.aix5.2.ppc.rpm
  - syslog-ng-1.5.26-0.aix5.2.ppc.rpm
  - tcp_wrappers-7.6-ipv6.3.aix5.2.ppc.rpm
  - textutils-2.0-5.aix4.3.ppc.rpm
  - unzip-5.42-2.aix4.3.ppc.rpm
  - zip-2.3-3.aix4.3.ppc.rpm
  - zlib-1.1.4-3.aix4.3.ppc.rpm

- It installs the appropriate PAM configuration file based upon whether you selected to configure RADIUS. The aix-config RPM (above) installs both a RADIUS (/etc/pam.conf.rad) and a non-RADIUS (/etc/pam.conf.no_rad) version of the PAM configuration file. The script copies the appropriate version to the active configuration file /etc/pam.conf.

The script output is as follows.

```
setup_rpm.sh: start Sat Mar 20 17:40:12 EST 2004
aix-bin         ##############################################
warning: /etc/environment saved as /etc/environment.rpmorig
warning: /etc/mail/sendmail.cf saved as
/etc/mail/sendmail.cf.rpmorig
warning: /etc/motd saved as /etc/motd.rpmorig
warning: /etc/netsvc.conf saved as /etc/netsvc.conf.rpmorig
warning: /etc/ntp.conf saved as /etc/ntp.conf.rpmorig
warning: /etc/profile saved as /etc/profile.rpmorig
warning: /usr/share/dict/words saved as
/usr/share/dict/words.rpmorig
aix-config      ##############################################
aix-tsm         ##############################################
You must register the client with the server.
Remember to run the dsmc command later to complete this process
openssh         ##############################################
openssh-clients ##############################################
openssh-server  ##############################################
```

```
0513-071 The sshd Subsystem has been added.
0513-059 The sshd Subsystem has been started. Subsystem PID is
188440.
radius-client    ################################################
sudo             ################################################
syslog-ng        ################################################
stopping native syslog service
0513-044 The syslogd Subsystem was requested to stop.
0513-071 The syslog-ng Subsystem has been added.
starting syslog-ng service
0513-059 The syslog-ng Subsystem has been started. Subsystem PID
is 168168.
Error creating AF_INET socket (Error 0)
Error initializing configuration, exiting.
setup_rpm.sh: end Sat Mar 20 17:40:43 EST 2004
```

The two error messages after the syslog-ng startup may occur because the DNS resolver is not yet configured. You can ignore these messages since we will be configuring DNS and the logger will be properly started.

Note that if you use the IBM backup product Tivoli Storage Manager (TSM), you must run the "dsmc" command as root to register the host as a backup client to the TSM server. You are prompted for the node name and a password.

2.7.2.11 Configure error logging (setup_errlog.sh)

The script increases the error log size from 1 megabyte to 4 megabytes, and the error log buffer from 16 kilobytes to 32 kilobytes. This ensures that error messages are not lost in the event that many errors are experienced in a short time, such as when a server is under attack. The script uses the following command to execute this.

```
/usr/lib/errdemon -s4194304 -B32768
```

This script modifies the error logging to also send its error messages to the syslog facility. This ensures that errors are easily correlated to syslog messages, and that the errors are logged to the remote syslog server. This is important if an attack generates error log messages since we want to ensure that those messages are saved on a remote server for forensic purposes.

The error syslog technique described above was taken from the Austin Gresham's GCUX practical on the GAIC web site URL: http://www.giac.org/practical/Austin_Gresham_GCUX.doc (20 March 2004). Austin cites his source for this technique as Seigert, Andreas. The AIX Survival Guide. Addison-Wesley, 1998.

The error log entries are sent to the syslog facility by making a configuration entry into the ODM database (Object Data Manager). The database is similar to

the registry on a Windows server. The script configuration file **setup_errlog.conf** contains the following ODM entry.

```
errnotify:
        en_pid = 0
        en_name = "syslog"
        en_persistenceflg = 1
        en_label = ""
        en_crcid = 0
        en_class =""
        en_type = ""
        en_alertflg = ""
        en_resource = ""
        en_rtype = ""
        en_rclass = ""
        en_method = "/usr/bin/errpt -l $1 | /usr/bin/tail -1 |
                    /usr/bin/logger -t errpt -p daemon.notice"
```

This entry is added to the ODM using the following command.

```
odmadd setup_errlog.conf
```

The script produces the following output.

```
setup_errlog.sh: start Sat Mar 20 19:37:51 EST 2004
setup_errlog.sh: end Sat Mar 20 19:37:57 EST 2004
```

2.7.2.12 Configure cron (setup_cron.sh)

This script configures the “cron” and “at” scheduling systems so that the “root” and “adm” administrative users are the only accounts that can access these systems. This prevents attackers from abusing the scheduler.

The script performs the following actions.

- It renames the /var/adm/cron/at.deny and /var/adm/cron/at.allow files. A date stamp is added to the file name so that the originals are preserved.
- It creates a new /var/adm/cron/at.allow file and adds the root user to the file.
- It renames the /var/adm/cron/cron.deny and /var/adm/cron/cron.allow files. A date stamp is added to the file name so that the originals are preserved.
- It creates a new /var/adm/cron/cron.allow file and adds the root and adm users to the file.
- It ensures that the file permissions for at.allow and cron.allow are bin:cron:640 so that arbitrary users cannot modify or read the files.
- It edits the root crontab file /var/spool/cron/crontabs/root to include a few jobs that our shop adds to all standard configurations. These include typical administrative actions to be performed on a periodic basis such as

running the mksysb backup, log rotations, running system accounting processes, and periodically delivering the mail (sendmail). You can edit this script to suit your needs since every shop has its own unique requirements, but these are a fine start.

The script produces the following output.

```
setup_cron.sh: start Sat Mar 20 20:26:22 EST 2004
setup_cron.sh: end Sat Mar 20 20:26:22 EST 2004
```

2.7.2.13 Configure Trusted Computing Base (setup_tcb.sh)

This script configures the Trusted Computing Base, which is a tripwire-like file system integrity database located in **/etc/security/sysck.cfg**. Unfortunately, the database is not encrypted and it only tracks a few essential attributes about the files such as checksum, owner, group, mode, and file type (file, symbolic link, etc). By default, the TCB is configured to use a weak 32-bit Cyclic Redundancy Check checksum, but this script will configure it to use strong MD5 checksums. A default set of critical files is configured in the TCB database, but you can add or delete any files that you deem necessary. Since we add a few Open Source software packages to the baseline IBM build, the critical files in these packages are added to the TCB. The RPM spec files included in this hardening process are enhanced to include registering their files into the TCB at installation time.

The TCB could be used as a poor-man's tripwire, and it is better than not using any file integrity checking. If you are going to use it as your only method of integrity checking, make sure to keep an offline copy of the sysck.cfg database file either on removable media or in a remote server repository. Our shop uses Tripwire, but the TCB process is included here as an option for your shop. Read the man page on the "tcbck" command carefully because it is easy to damage your permissions if the command is misused.

This script performs the following actions.

- It modifies the TCB database to use MD5 checksums. The MD5 binary is added to the system in the textutils RPM.

  ```
  tcbck -a sysck checksum=/usr/bin/md5sum
  ```

- It removes the following mutable files from the database. These attributes of these files change frequently under normal operating conditions, which generates many false alarms.

  /dev/pts/* /dev/tty* /dev/lft*
  /dev/random /dev/urandom

- It removes the checksums for the following log files from the database, but the permissions are still registered.
  /etc/security/lastlog /etc/security/portlog

- It fixes a few miscellaneous incorrect entries for non-existent files and symbolic links so that the database is clean.

- It registers the audit subsystem directory, since we are enabling detailed auditing.

The script produces the following output. You can ignore the complaints about the invalid entries because they are corrected during the process.

```
setup_tcb.sh: start Sat Mar 27 12:42:05 EST 2004
3001-039 The name uucp is not a known group.
3001-015 The entry for /etc/ppp/mkppp is not valid.
setup_tcb.sh: end Sat Mar 27 12:44:58 EST 2004
```

2.7.2.14 Configure miscellaneous items (setup_misc.sh)

This script configures a few miscellaneous items that just do not fit into any of the other hardening categories.

The script performs the following actions.

- It increases the user license count.

- It creates the /etc/ftpusers configuration file and populates it with the user accounts listed in the script configuration file setup_ftpusers.conf. This file lists users that are denied FTP access. Users such as root, system, and guest should never be allowed to use FTP. The list provided includes many common FTP users such as oracle and apache that are not even included in the standard AIX distribution, but may find their way onto your system as you add applications. Although the hardening process disables FTP, this file is configured in the event that an administrator would enable FTP accidentally.

The script produces the following output.

```
setup_misc.sh: start Sat Mar 27 13:16:42 EST 2004
chlicense: The system must be rebooted before the new number of
           fixed licenses will take effect.
setup_misc.sh: end Sat Mar 27 13:16:42 EST 2004
```

2.7.2.15 Configure auditing system (setup_audit.sh)

This script configures and starts the AIX auditing system. The auditing system detects and records fine-grained system events such as file opening, reads, writes, and process executions. It also records high-level events such as reboots and logical disk volume reconfiguration. The user and time stamp are included in the auditing logs so that you have a thorough audit trail. The system is very flexible, so it can be configured to meet your specific needs. Since auditing creates overhead and uses a lot of disk space, you need to be very selective in what you decide to audit.

The commercial version of Tripwire is able to link the audit logs into its reporting facility. This unique feature enables Tripwire to report on files that were created and then deleted, which is not normally within the capability of file integrity checkers since they typically report modifications to existing files. This feature is particularly useful to detect if an attacker loads program code and then deletes it after execution. It also alerts you to a common hacker technique of writing network traces to a log file that is deleted after the trace starts. This hides the file from a directory listing, but the file still exists on disk until the trace is killed. Since auditing can detect the file deletion, it is able to provide that information to Tripwire.

The auditing configuration file /etc/security/audit/config contains a listing of all of the events to be audited. Audit events are grouped together, and the audit group is then assigned to individual users. This enables you to log a reduced set of activities for unprivileged users or log a very detailed set of events for more powerful users such as root.

The IBM web site contains detailed configuration information at URL: http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm (3 May 2004).

This script performs the following actions.

- It ensures that the /var/audit output directory exists and has restrictive permissions.

- It relocates any files in the default audit output directory /audit into /var/audit. This prevents the root filesystem from filling with audit logs.

- It edits the auditing configuration file to create a custom auditing class with interesting audit events. The following events are audited, which is a combination of some IBM default classes and the custom class. You probably will want to adjust the list to suit your needs and available disk space, but this list is a reasonable start. It includes the important events that Tripwire is able to link in its reporting.
  General class:

USER_SU	PASSWORD_Change	FILE_Unlink	FILE_Link
FILE_Rename	FS_Chdir	FS_Chroot	PORT_Locked

PORT_Change FS_Mkdir FS_Rmdir

Objects class:

S_ENVIRON_WRITE S_GROUP_WRITE S_LIMITS_WRITE
S_LOGIN_WRITE S_PASSWD_READ S_PASSWD_WRITE
S_USER_WRITE AUD_CONFIG_WR

Subsystem Resource Controller (SRC) class:

SRC_Start SRC_Stop SRC_Addssys SRC_Chssys
SRC_Delssys SRC_Addserver SRC_Chserver SRC_Delserver

Custom class:

PROC_Reboot FS_Mount FS_Umount FILE_Mknod FILE_Mode
FILE_Owner FILE_Fchmod FILE_Fchown DEV_Create TCPIP_config
TCPIP_connect TCP_kbind

- It assigns the custom auditing class as the default for all users, including root.
- It starts the auditing system executable.
- It adds the auditing executable to the /etc/inittab startup file so that auditing is enabled at boot time.
- It adds a TCB database entry for the new auditing output directory.

The script produces the following output.

```
setup_audit.sh: start Sat Mar 27 13:54:37 EST 2004
setup_audit.sh: end Sat Mar 27 13:54:37 EST 2004
```

2.7.2.16 Configure tripwire (setup_tripwire.sh)

This script installs the Tripwire RPM file set and initializes the Tripwire database.

The script performs the following actions.

- It installs the RPM using "`rpm -ivh`".
- It initializes the database using "`tripwire --init`".
- It updates the policy file with the server hostname using the pair of commands "`twadmin --print-polfile`" and "`tripwire --update-policy`".

The script produces the following output. You are prompted to supply the tripwire pass phrases during the script execution. Do not be concerned about warnings of missing files. These are an indication that Tripwire is configured to protect those files, but the files do not exist. In the example output below, X-windows files were not installed and the password history files have not yet been created since nobody has changed a password yet.

```
setup_tripwire.sh: start Sat Apr 3 12:39:04 EST 2004
tripwire    ##############################################
The Tripwire Agent was started successfully.
Please enter your site passphrase:  <supply passphrase>
Wrote policy file: /usr/local/tripwire/tfs/policy/tw.pol
Parsing policy file: /usr/local/tripwire/tfs/policy/tw.pol
Generating the database...
*** Processing Unix File System ***
Note: Tripwire could not find the following objects:
   /.dt
   /usr/lpp/X11/bin
   /usr/dt/bin
   /etc/security/pwdhist.dir
   /etc/security/pwdhist.pag
   /.dtprofile
   /.Xauthority
Please enter your local passphrase: <supply passphrase>
Wrote database file: /usr/local/tripwire/tfs/db/database.twd
The database was successfully generated.
setup_tripwire.sh: end Sat Apr 3 12:39:34 EST 2004
```

2.7.2.17 Configure boot devices (setup_boot.sh)

This script determines which disk drives have boot partitions and then writes a fresh copy of the initial boot code onto those drives. This ensures that the boot code matches the operating system, since we made so many changes to software and configurations. It also ensures that all mirror disk copies have the initial boot code.

This script performs the following actions.

- It lists the root volume group to find the boot partitions.
  ```
  lsvg -l rootvg
  ```
- It finds the physical hard drives with the boot partition.
  ```
  lsvg -M rootvg | grep "boot partition value from lsvg"
  ```
- It writes the boot information to the hard drives.
  ```
  bosboot –ad disk_device_names
  ```
- It creates the boot list with disk volumes.
  ```
  bootlist -m normal disk_device_names
  ```

The script produces the following output.

```
setup_boot.sh: start Sat Mar 27 14:19:38 EST 2004
bosboot: Boot image is 14268 512 byte blocks.
bosboot: Boot image is 14268 512 byte blocks.
setup_boot.sh: We must REBOOT the server so that the updates can
take effect.
You should restart the installation after the reboot completes.
```

```
Reboot now y,n: y
```
You must reboot for the changes to take effect.

2.7.2.18 Remove installation utilities (setup_cleanup.sh)

This script removes the installation utilities, RPM installation file sets (just the RPM files, not the installed packages in the file systems), the IBM maintenance release files, and the IBM patch files. None of these is required any more since they are all installed. This releases the disk space since these files consume a lot of space.

The script produces the following output.

```
setup_cleanup.sh: start Sat Mar 27 14:18:22 EST 2004
setup_cleanup.sh: end Sat Mar 27 14:18:27 EST 2004
```

CAUTION:
When you are building servers, this step is normally run as the last step to cleanup all of the installation utilities. Since this server is your development toolbox from which you will be distributing these utilities, DO NOT RUN THIS PROCEDURE. It will remove files that you need to build your all of your other servers!

2.7.3 Connect the Network Cable

Since the development toolkit server is now completely built and hardened, it is safe to connect to the network. Plug in the network cable into the network interface. You should be able to ping the gateway to verify connectivity.

The development toolkit server is ready for service.

3.0 Building Servers Using the Development Toolkit

Now that your development toolkit is completed, you are ready to build hardened AIX servers using the automated tools. The following describes how to prepare an installation CD-ROM with all of the tools that you built, and how to run the installation. Typical installation time is less than an hour from the moment the CD-ROM is installed until the server is completely built and hardened.

3.1.1 Prepare a CD-ROM with the software

You need to prepare an Installation Toolkit on CD-ROM that contains all of the RPM file sets and patches. Since many servers have a read-only CD and they do not have CD burners, the process below creates an installation TAR archive that contains everything required to automatically build a secure server. Use a desktop that has a CD burner to Secure Copy the TAR from the development server to the desktop, and then burn the CD.

Use the following command to copy all of the required software into a TAR archive. You may want to place the command into a shell script for ease of use.

```
cd /usr/opt/freeware/src/packages
tar -cvf - \
      ./LPP/*"
      ./MAINT/5200-02/*
      ./PATCHES/5200-02/*
      ./RPMS/ppc/aix-bin-5.2.1.0-0.aix5.2.ppc.rpm
      ./RPMS/ppc/aix-config-5.2.1.0-0.aix5.2.ppc.rpm
      ./RPMS/ppc/aix-harden-5.2.1.0-0.aix5.2.ppc.rpm
      ./RPMS/ppc/aix-never-delete-1.0-0.aix5.2.ppc.rpm
      ./RPMS/ppc/aix-tsm-5.1.5-1.aix5.2.ppc.rpm
      ./RPMS/ppc/libol-0.3.9-1.aix5.2.ppc.rpm \
      ./RPMS/ppc/lsof-4.61-3.aix5.1.ppc.rpm \
      ./RPMS/ppc/openssh-3.7.1p2-1.aix5.2.ppc.rpm \
      ./RPMS/ppc/openssh-clients-3.7.1p2-1.aix5.2.ppc.rpm \
      ./RPMS/ppc/openssh-server-3.7.1p2-1.aix5.2.ppc.rpm \
      ./RPMS/ppc/openssl-0.9.6m-1.aix5.1.ppc.rpm \
      ./RPMS/ppc/prngd-0.9.27-1.aix5.2.ppc.rpm \
      ./RPMS/ppc/radius-client-1.1-0.aix5.2.ppc.rpm \
      ./RPMS/ppc/sudo-1.6.7p5-2.aix5.2.ppc.rpm \
      ./RPMS/ppc/syslog-ng-1.5.26-0.aix5.2.ppc.rpm \
      ./RPMS/ppc/tcp_wrappers-7.6-ipv6.3.aix5.2.ppc.rpm \
      ./RPMS/ppc/textutils-2.0-5.aix4.3.ppc.rpm \
      ./RPMS/ppc/tripwire-4.10-0.aix5.2.ppc.rpm \
      ./RPMS/ppc/unzip-5.42-2.aix4.3.ppc.rpm \
      ./RPMS/ppc/zip-2.3-3.aix4.3.ppc.rpm \
      ./RPMS/ppc/zlib-1.1.4-3.aix4.3.ppc.rpm \
      | gzip -c >/var/tmp/setup.tar.gz
```

3.1.2 Load the New Server with AIX 5.2

Follow the same procedure described in Section 2.2 “Install the Initial System Image” to load the new server with AIX 5.2 using the vendor supplied media.

Make sure that the network cable is not connected to the server until all of the installation and hardening procedures are completed.

3.1.3 Load the Installation Toolkit

Log in as root on the new server.

Insert the Installation Toolkit CD-ROM that you created in Section 3.1 above. Mount the CD-ROM and copy the TAR image onto the server. The /opt file system will be expanded to be large enough to contain the TAR. This is a temporary measure and the file system is removed during the installation process.

```
mount -o ro -V cdrfs /dev/cd0 /mnt
chfs -a size=1024M /opt
cd /opt/freeware/src/packages
gunzip -c /mnt/setup.tar.gz | tar -xvf -
```

3.1.4 Run the Configuration Procedure

Follow the same process described in Section 2.7 “Harden the Operating System Image” to install and execute the hardening scripts. After the last reboot, you can permit the scripts to remove themselves, the RPMs, and all of the patch files since they are no longer needed on the new server.

The new server is ready. You may connect the network cable now.

4.0 Ongoing Maintenance Procedures

The ongoing maintenance procedures for the Development Toolkit server are same basic procedures as for any other server in the enterprise, so this section details a maintenance plan for the AIX environment in general.

4.1.1 Overall Plan

- Backups

  The backup strategy consists of two parts: an AIX **mksysb** backup of the root volume group, and a Tivoli Storage Manager (TSM) backup of the entire system.

- AIX Maintenance Level Releases

  Periodically, IBM releases a Maintenance Level software package that bundles all of the patches released to-date. The patches receive additional quality assurance testing, and interoperability is tested. These are scheduled for installation across the enterprise on an as-released basis.

- AIX Interim Patches

  IBM releases interim patches known as APARs (authorized program analysis report) to AIX administrators. APAR patches are released on an as-needed basis for correcting bugs and security exposures. Generally, only the security patches are installed unless a specific bug behavior is encountered which necessitates the need for an APAR fix.

- Re-Hardening Procedures

  Whenever IBM supplied patches or Maintenance Levels are installed onto an existing system, the IBM installation procedures may add unwanted daemons into the system startup files. They may also set permissions on executables back to the factory standards, which our installation toolkit had customized. Portions of the hardening process must be executed on systems that received patches or Maintenance Levels to ensure that the security posture is maintained.

- Open Source Patches

Updates to the Open Source Software that is incorporated into the standard build are applied on an as-needed basis. Generally, only the security patches are installed unless a specific bug behavior is encountered which necessitates the need for an Open Source patch. This is the same methodology applied to the IBM supplied AIX APARs.

- Security Bulletins and Patch Implementation Schedules

  Subscription to CERT and SANS advisory mail lists provides notification to the Unix administration staff of possible security vulnerabilities. A shared group mailbox is configured and all Unix administrators have access to the mailbox. Each week, one of the administrators is assigned the duty of being the "on-call" support lead. The on-call support lead is responsible for monitoring the mailbox for security advisories. The advisories are reviewed with the Security Operations Manager and the associated patches scheduled for installation as determined by the level of risk. High-risk exposures are patched very quickly, and medium to low risk exposures are scheduled accordingly. Sign up for the email newsletters at the following web sites.

  http://www.sans.org/newsletters/ (3 May 2004)
  http://www.us-cert.gov/cas/index.html (3 May 2004)

- Local and Centralized Logging

  The standard configuration saves syslog messages both locally and to the centralized log server. All servers need to rotate their local logs periodically, and purge old logs so that the file system does not completely fill. The primary purpose for the local logs is to provide logs for debugging purposes when network connectivity is down. It is also convenient to be able to view the logs locally when debugging instead of requiring a second session on the log server. Automated monitoring of the logs for conditions that require administrator attention is performed on the central log server, so no log monitoring process is required on each individual server.

- Configuration Integrity

  Tripwire is used to ensure the integrity of the system configuration. All vital binaries and configuration files are monitored for changes. Integrity checks are scheduled on a daily basis and the on-call administrator is responsible for investigating any Tripwire alerts. Fortunately, the use of the commercial version of Tripwire facilitates this activity with centralized management software. Unexpected changes must be investigated and resolved. System changes that cannot be explained are reported to the Security Operations team for further handling.

- Installation Procedures

The installation procedures need occasional modification as server requirements change or new versions of the operating system, patches, and Open Source software are deployed. All changes to the installation process are implemented on the Development Toolkit server and tested on a spare server for accuracy. Detailed documentation must be maintained so that the process can be easily understood by any member of the system administration team.

4.1.2 Backup Strategy

The **mksysb** is a backup format that is unique to IBM AIX platform. It creates a bootable backup image that contains everything in the root volume group, which enables the administrator to recreate a working system. An interesting feature of the mksysb is that if it is written to a tape, the tape becomes both a boot image and a backup of the operating system. The mksysb process is described in detail on IBM's web site at URL: http://publib16.boulder.ibm.com/doc_link/en_US/a_doc_lib/aixins/insgdrf/backing_up_system.htm (3 May 2004).

Another useful feature of the mksysb is that it permits restoration to differing hardware platforms. The mksysb backup from a small 7044P server can be restored onto a large Regatta server, or vice-versa. AIX will configure all of the appropriate device drivers that are specific to the target hardware. This is very handy when a server has a catastrophic hardware failure and the only available spare servers are different hardware models.

TSM is a centralized backup solution that runs on a TSM server. The TSM server communicates with an agent daemon on all of the servers in the enterprise. Backups are sent across the network to the TSM server, which is connected to a large tape library for centralized, automated tape storage. Many shops elect to build a separate backup network so that the primary network is not overloaded by the backups. Essentially, this is just a second network interface card on each server that connects to dedicated switches and routers, and the TSM server is located on this network.

TSM backs up every file on the system, including the mksysb image located in the /mksysb file system. If a bare-metal restoration is required, the mksysb is used to restore the base operating system, and then any applications or data is restored onto the working system.

4.1.3 AIX Maintenance Level Releases

IBM releases full Maintenance Levels on an infrequent basis that is dependent upon the amount of interim patches that have been released since the last full Maintenance Level. AIX 5.2 level 02 was released on 10/13/2003 and level 01 was released on 05/14/2003. Historically, a Maintenance Level Release has been issued for AIX 5.x once in the spring, and once in the fall. Checking the IBM web site bi-monthly for new Maintenance Releases takes only a few minutes and should be sufficient to remain aware of new releases.

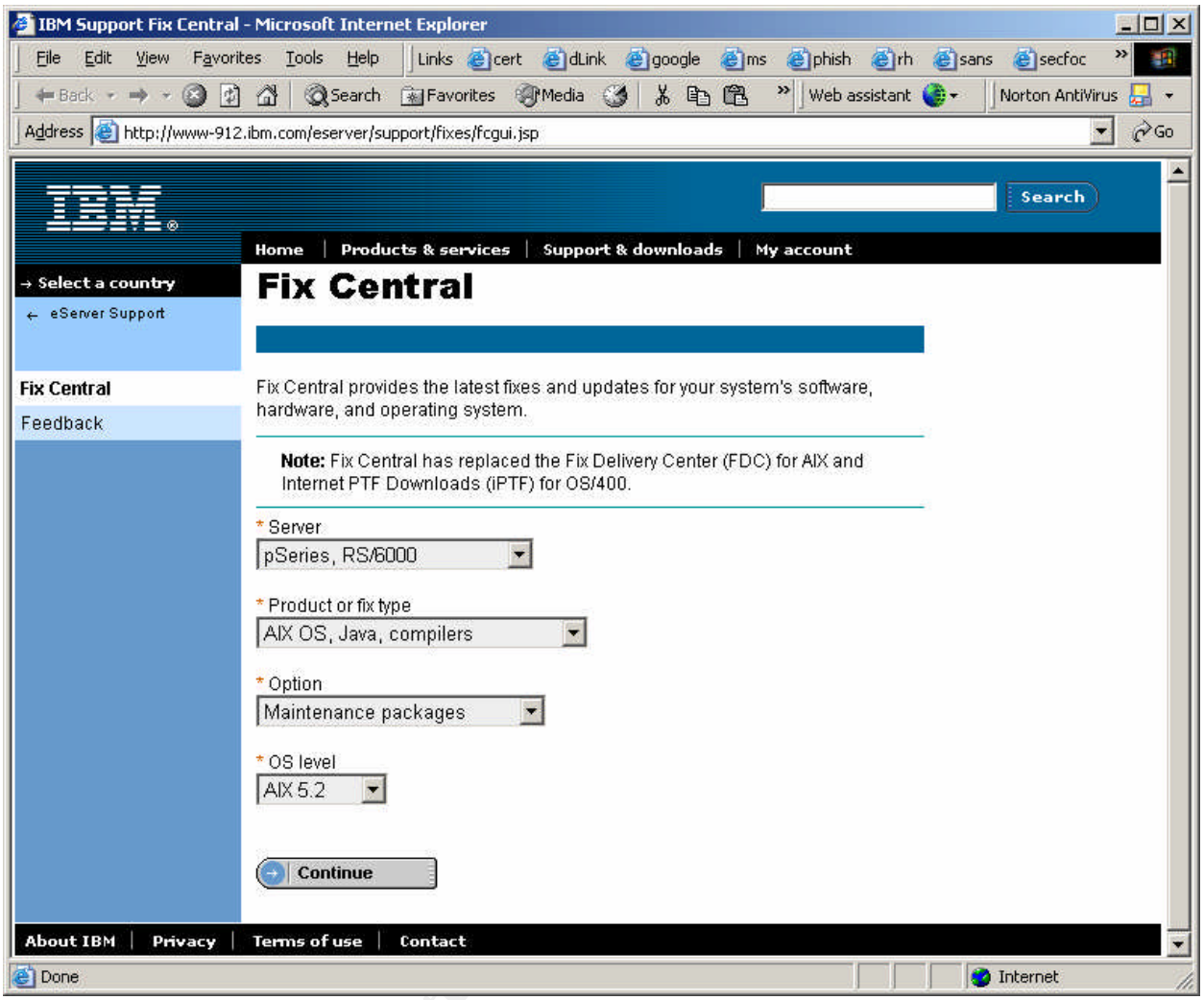
New releases incorporate all of the interim patches, not just security fixes. This means that if you are routinely applying all of the security fixes but only installing the bug fixes for which you have experienced problems, there is a lot of code in the new release that you have not tested. There may also be updates to the interim patches related to quality assurance testing, so patches that you are already using may be modified when they are included in the full Maintenance Level. Although IBM has historically been very thorough in their software testing, all software has bugs, so Maintenance Levels must be put through careful testing in your shop before deployment into the environment.

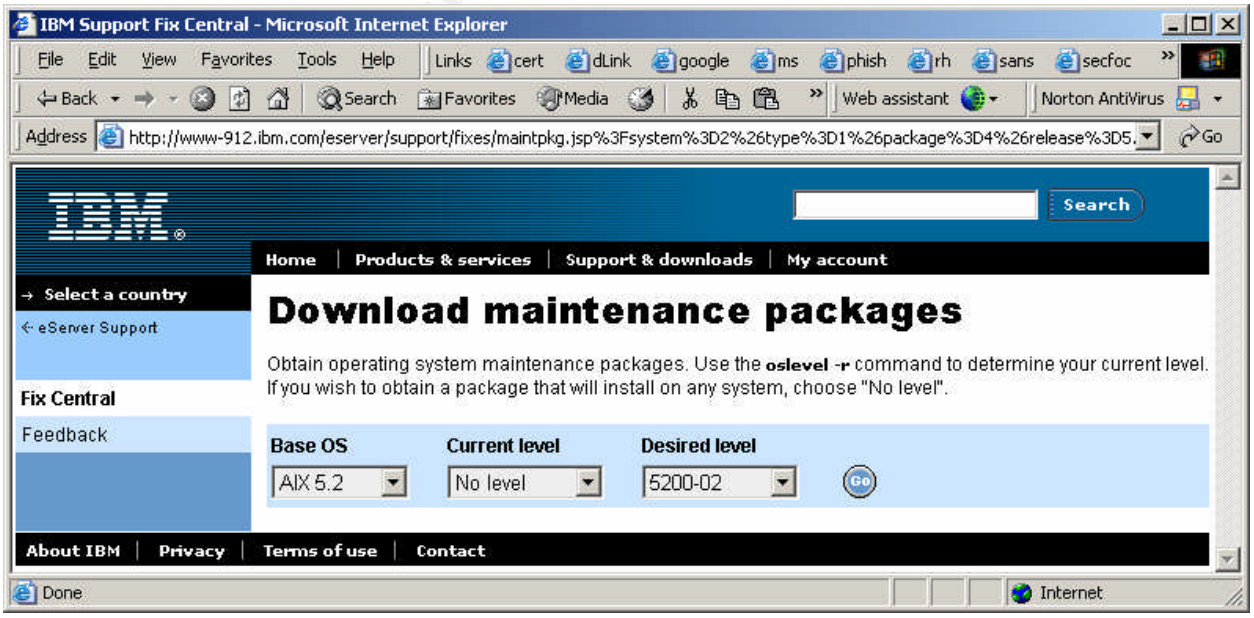
After thoroughly testing the release, it needs to be incorporated into the installation scripts on the development toolkit and a new "Golden Image" should be created for deployment of new servers. Copy the Maintenance Release files to the development toolkit server into the directory `/opt/freeware/src/packages/MAINT/5200-##` (where `5200-##` is the current maintenance release number).

The release also needs to be deployed onto existing servers in the environment. This can be done by either copying the software onto CD-ROM or creating a TAR archive of the files and Secure Copying (SSH) the TAR to the target systems. Follow the IBM instructions on the software download page to ensure that you are installing the updates correctly. The server needs to be re-hardened after the Maintenance Level Release is applied, which is described in a following section.

The URL http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp (3 May 2004) takes you to the IBM Fix Central web site for downloading Maintenance Level Releases. A few sample screens are included below to demonstrate how to answer the prompted to download release 02 for AIX 5.2.

Remember to make a new installation CD-ROM as described in section 3.0. If you are using Tripwire, update the signature database as described in a section below.





4.1.4 AIX Interim Patches

IBM releases interim patches known as APARs (authorized program analysis report). APAR patches are released on an as-needed basis for correcting bugs and security exposures. The patches do not receive the intensive quality assurance testing that the full Maintenance Releases receive, so there is a risk that an interim patch may cause problems in your environment.

It is generally good practice to install only the security patches unless a specific bug behavior is encountered which necessitates the need for an APAR fix. You only need to install the security patches for software that is installed on your systems. Some shops elect to not install security patches for software that is installed but disabled. For example, the telnet daemon is installed as a component in the AIX file set **bos.net.tcp.client**. This file set includes many TCP client programs, and the server is not going to be very useful without it, so nearly every server will include the file set. If you disable the telnet daemon in the configuration file /etc/inetd.conf, you could elect to not patch this file set if a security vulnerability is discovered in the telnet daemon. There are trade-offs in the decision to either patch or not patch in this scenario. By installing the patch, you risk incurring a problem in any of the individual programs included in the file set. By not installing the patch, you risk an administrator enabling a vulnerable telnet daemon. Our shop chooses to always patch, and we spend the time to test the patch to mitigate the risk of installing buggy software.

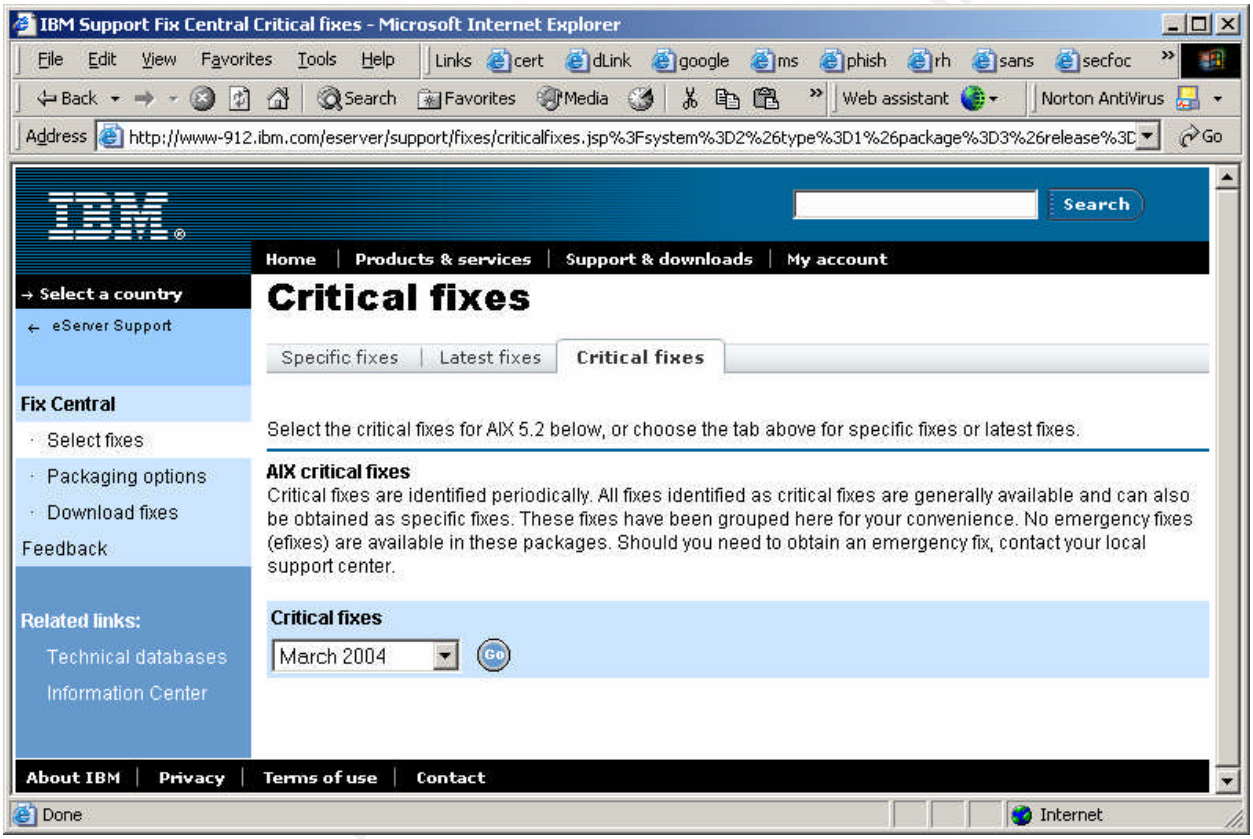
The patches are downloaded from the same URL listed above for the Maintenance Releases. Instead of selecting the option “Maintenance packages” in the pull-down box, choose “Critical fixes”. A second screen appears with an option to select the month of the release (shown below). Choose the latest month unless you have a specific need to retrieve an older patch. The next screen (shown below) gives you the option to download all critical fixes, or just the security fixes. The security fixes are the minimum that you need, but it is worth reviewing the other fixes in case there is a very serious defect in a software package that your shop uses. Judge your risk level carefully.

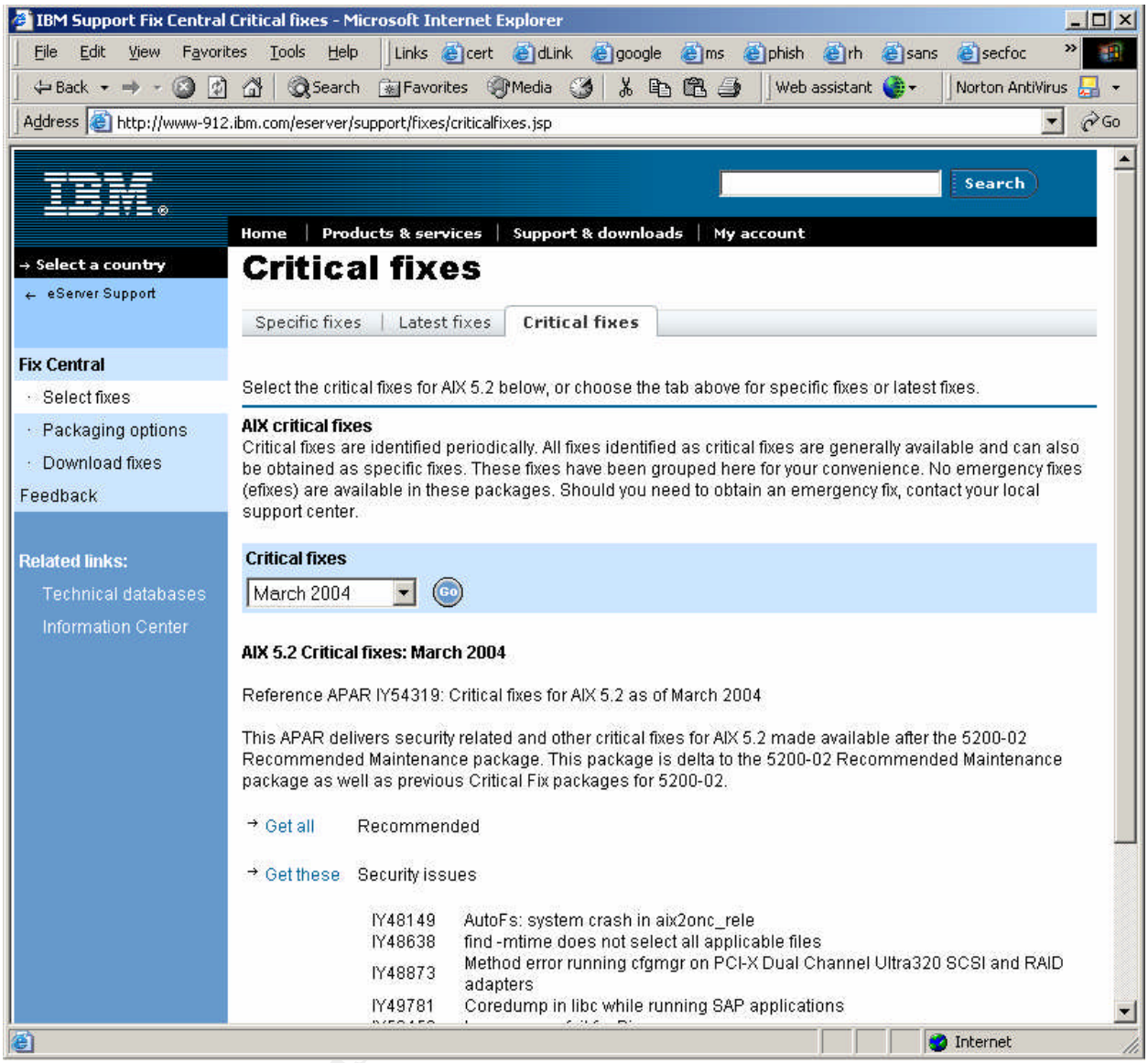
After thoroughly testing the patches, they need to be incorporated into the installation scripts on the development toolkit and a new “Golden Image” should be created for deployment of new servers. Copy the patch files to the development toolkit server into the directory `/opt/freeware/src/packages/PATCHES/`**`5200-`**`##` (where **`5200-`**`##` is the current maintenance release number).

The release also needs to be deployed onto existing servers in the environment. This can be done by either copying the software onto CD-ROM or creating a TAR archive of the files and Secure Copying (SSH) the TAR to the target systems.

Follow the IBM instructions on the software download page to ensure that you are installing the updates correctly. The server needs to be re-hardened after the Maintenance Level Release is applied, which is described in a following section.

Remember to make a new installation CD-ROM as described in section 3.0. If you are using Tripwire, update the signature database as described in a section below.





4.1.5 Re-Hardening Procedures

Whenever IBM supplied patches or Maintenance Levels are installed onto an existing system, the IBM installation procedures may add unwanted daemons into the system startup files or set permissions on executables back to the factory standards.

In order to bring the system back into compliance with security standards, portions of the hardening process need to be run again. Copy the hardening toolkit RPM **aix-harden-5.2.1.0-0.aix5.2.ppc.rpm** to the server along with the patches. After installing a Maintenance Release or interim patches, install the

RPM (rpm -ivh aix-harden-5.2.1.0-0.aix5.2.ppc.rpm) and run the following portions of the installation hardening process.

```
cd /usr/local/bin
./setup_aix.sh -R -D
```

Choose these individual options on the menu.

```
5. Configure file permissions
6. Configure init inetd and rc daemons
13. Configure Trusted Computing Base
```

You can remove the RPM when the re-hardening is completed (rpm -e aix-harden-5.2.1.0-0.aix5.2.ppc.rpm).

If you are using Tripwire, update the signature database as described in a section below.

4.1.6 Open Source Patches

When security vulnerabilities are announced for any of the Open Source software that you deploy with the toolkit, you need to download the fix, incorporate it into your software repository on the development toolkit server, rebuild the RPM, and install it onto all of your servers in the enterprise.

Sometimes an entirely new TAR archive is released for the software. Sometimes just the affected files are modified and released. Read the instructions on the Open Source web site for the software package for specific details on how to correct the problem.

If a new TAR archive is released, copy the new TAR file into the directory /usr/opt/freeware/src/packages/SOURCES on the development toolkit server. If the name of the TAR archive includes a version number, which it usually does, edit the specification file to reflect the new TAR file name. Build a new RPM for distribution. The following summarizes the basic steps using the SUDO software as an example. Assume that your current version is 1.6.7p4 and the new version is 1.6.7p5.

- Download the new software from http://www.courtesan.com/sudo/dist/ (3 May 2004)
- Copy sudo-1.6.7p5.tar.gz to /usr/opt/freeware/src/packages/SOURCES
- Set the permissions on the TAR file

```
cd /usr/opt/freeware/src/packages/SOURCES
chown root:system sudo-1.6.7p5.tar.gz
chmod 640 sudo-1.6.7p5.tar.gz
```

- Edit the RPM specification file to reflect the new version number so that the new TAR file is used for the compilation

```
cd /usr/opt/freeware/src/packages/SPECS
vi sudo.spec
```

Edit the following line to change the release number

```
%define ver     1.6.7p4
```

- Build a new RPM for distribution

```
rpm -ba sudo.spec
```

If a patch is released that needs to be applied to the current distribution, copy the patch into the directory /usr/opt/freeware/src/packages/SOURCES on the development toolkit server. Rename the patch file so that it can be easily identified with its associated software package. Edit the specification file to use the new patch TAR file. Build a new RPM for distribution. The following summarizes the basic steps using the SUDO software as an example. Assume that the patch file is named foo.

- Download the new software from http://www.courtesan.com/sudo/dist/ (3 May 2004)
- Copy foo to /usr/opt/freeware/src/packages/SOURCES
- Rename the patch file to indicate its association with the software

```
cd /usr/opt/freeware/src/packages/SOURCES
mv foo sudo-1.6.7p5-foo.patch
```

- Set the permissions on the patch file

```
chown root:system sudo-1.6.7p5-foo.patch
chmod 640 sudo-1.6.7p5-foo.patch
```

- Edit the RPM specification file to increment the RPM release number and incorporate the patch during compilation

```
cd /usr/opt/freeware/src/packages/SPECS
vi sudo.spec
```

Edit the following line to increment the release number

```
%define rel     3
```

Add the following line just after the “Source0” and “Source1” lines near the top of file to specify the patch file

```
Patch0:  %{name}-%{version}-foo.patch
```

Add the following lines just after the “%setup” lines in the “%prep” section to include the patch file before compilation

```
# put the freeware patch command in the PATH
PATH=/usr/opt/freeware/bin:$PATH
export PATH
%patch0 -p0
```

- Build a new RPM for distribution

```
rpm -ba sudo.spec
```

After building the new RPM, copy it to the affected servers to the directory /usr/opt/freeware/src/packages/RPMS/ppc and install the update. If the release number is incremented, the “--force” option is not needed. Use the “-U” option to update an RPM. Note the version 1.6.7p5-3 includes the new release level “3”.

```
cd /usr/opt/freeware/src/packages/RPMS/ppc
rpm -Uvh sudo-1.6.7p5-3.aix5.2.ppc.rpm
rm sudo-1.6.7p5-3.aix5.2.ppc.rpm
```

If the release number is incremented, the installation scripts need to be edited to reflect the new RPM file name since the release number is imbedded into the file name. On the development toolkit server, edit the file setup_rpm_add.conf in the directory /usr/opt/freeware/src/packages/SOURCES/aix-harden-5.2.1.0 to change the RPM file name to use the correct release number. See the section

below “Guidelines for Modifying the Installation Procedures” for details on how to create an updated RPM for the installation hardening process.

Since the RPM specification file installs the files with the proper startup process and permissions, you do not need to run any re-hardening procedures.

Remember to make a new installation CD-ROM as described in section 3.0. If you are using Tripwire, update the signature database as described in a section below.

4.1.7 Configuration Integrity - Tripwire

File system integrity is assured by using the Tripwire software package. Tripwire creates strong checksums for specific files on the server, and it saves those checksums in an encrypted database. A configuration file specifies which files are protected. A well-configured Tripwire system includes all the system executables and all of the system configuration files. The following guidelines apply to the commercial version of Tripwire, which deviates somewhat from the free Academic Source release.

Whenever a change is made to a file, its checksum changes. Running periodic Tripwire scans will generate a report that indicates if any files have been modified since the last time the database was updated. The installation process configures Tripwire to run the verification every night. An email is sent to the system administrator’s mailbox for review. Tripwire can be configured to send a report even if there are no violations. This reassures the administrator that the Tripwire scans are executing. In the subject line of the email, a summary of the low, medium, and high violations is included, so it becomes an easy task to view the subject lines for violations without requiring each email to be opened.

Tripwire is also configured to write the results of the nightly scans to the Syslog facility, so all of the reports are also written to the centralized Syslog server for auditing purposes. As an alternative to processing the reports with individual email, you could alternatively parse the log files on the central log server and generate a summary email, SNMP traps, or send alerts to centralized alerting software.

You need to designate an individual who reviews the Tripwire reports periodically. A daily review is a good idea, but at least a frequent and consistent review is mandatory. In a small shop, the administrator who changes a server configuration may also run a Tripwire report and update the database immediately. In a large shop with strict System Change procedures, it may be desirable to have a separate individual manage the Tripwire service so that any unapproved changes are caught by a the dedicated Tripwire administrator. Pick

a strategy that fits your environment without becoming too burdensome. Many shops are overloaded with work, so you need to be realistic in how much effort your procedures require.

Integrity check reports are executed by the Tripwire scheduler periodically, but you can run and view them at any time using the Management Console by simply clicking on the appropriate buttons. The command line for running the integrity check is (mode check):

```
tripwire -m c
```

The default report file is written to /usr/local/tripwire/tfs/report with the file name hostname-YYYYMMDD-HHMMSS.twr (hostname and date-time stamp).

The administrator reviews the report and verifies that only her changes are flagged in the report. Any other changes are investigated to determine who made them and why. Unexplained changes are reported to the security team for further investigation.

If the changes are all valid, the database needs to be updated. The update process uses the report file to perform the update. The command line for running the update is (mode update):

```
tripwire -m u -r /usr/local/tripwire/tfs/report/report-file-name
```

After issuing the command, the "vi" editor is invoked and the administrator can review the tripwire report. The report flags each change and allows the administrator to mark or unmark each change for updating. A sample change to the /etc/hosts file is shown below. Note the "[**x**]" flag for approval. Removing the **x** rejects the change during the database update. When the report review and approval is completed, writing the file (vi command "**:wq**") will begin the update process. Tripwire prompts for the pass phrase before the update proceeds.

```
---------------------------------------------------------------
Rule Name: System configuration files (/etc)
Severity Level: 100
---------------------------------------------------------------

Remove the "x" from the adjacent box to prevent updating the
database
with the new values for this object.

Modified:
[x] "/etc/hosts"
```

4.1.8 Guidelines for Modifying the Installation Procedures

If you need to edit a script or a data file that the scripts use, follow these guidelines. Remember that the scripts are bundled into an RPM file set for easy distribution and installation. You need to extract the scripts from the TAR, edit them, recreate the TAR, and recreate the RPM binary. Don't panic, its easy.

- Unpack the TAR archive

```
cd /usr/opt/freeware/src/packages/SOURCES
gunzip -c aix-config-5.2.1.0.tar.gz | tar -xvf -
```

- Edit the file in the directory /usr/opt/freeware/src/packages/SOURCES/aix-config-5.2.1.0

- Recreate the TAR archive. (This is one long line)

```
tar –cvf - ./aix-harden-5.2.1.0 | gzip –c > aix-harden-
5.2.1.0.tar.gz
```

- Recreate the RPM file set. If you are familiar with software version controls, you can edit the aix-harden.spec file to increase the release number before building the RPM so that you can track software release versions properly.

```
cd /usr/opt/freeware/src/packages/SPECS
rpm –ba aix-harden.spec
```

- If you already installed the hardening scripts, you need to reinstall them for your modified file to be installed. Notice that we need the “force” option (using double dashes) to upgrade the RPM to the same version. If you increment the release number in the aix-harden.spec file, the RPM command will naturally perform the upgrade and it will not require the “force” option. In addition, the binary RPM file will have an incremented version number such as aix-harden-5.2.1.0-1.aix5.2.ppc.rpm.

```
cd /usr/opt/freeware/src/packages/RPMS/ppc
rpm –Uvh --force aix-harden-5.2.1.0-0.aix5.2.ppc.rpm
```

5.0 Test and Verify the Setup

The following procedures must be performed with root level privileges.

5.1.1 Verify the AIX Maintenance Level and Installation Integrity

This verifies actions performed by the script setup_maintlevel.sh.

The most important hardening procedure is the application of the current patch sets. This step has more impact on how secure an operating is than any other step. This can be easily verified.

Verify the OS level. This should show the current Maintenance Level, which is 02 as of 04/24/2004.

```
# oslevel -r
5200-02
```

Verify that all of the expected patch file sets are found. Note that the initial base operating system install (5.2.0.0) is missing some file sets. This is expected since the hardening procedures remove some of the undesirable packages. All of the patch levels (5200-01_AIX_ML and 5200-02_AIX_ML) should be found.

```
# instfix -i | grep AIX_ML
    Not all filesets for 5.2.0.0_AIX_ML were found.
    All filesets for 5200-01_AIX_ML were found.
    All filesets for 5200-02_AIX_ML were found.
```

Verify that the LPP file sets are complete. Each file set may have components installed into / (root), /usr, and /usr/share. This verifies that all parts are synchronized and all requisite file sets are installed.

```
# lppchk –v
(No output is good)
```

Verify that the file sets' checksums file sizes are consistent with the software (SWVPD) database. We expect only the following errors. The errors are generated because of the removal of these items during the hardening process.

```
# lppchk -c
lppchk: 0504-206 File /home/guest could not be located.
lppchk: 0504-206 File /var/adm/cron/at.deny could not be located.
lppchk: 0504-206 File /var/adm/cron/cron.deny could not be
located.
```

Verify that the expected symbolic links are found.

```
# lppchk –l
(No output is good)
```

5.1.2 Verify Active Network Services

This verifies actions performed by the script setup_daemons.sh.

The hardening procedures disabled all network services except Secure Shell (TCP-22), and they added Tripwire's agent (TCP-1169) and Tivoli Storage Manager backup (TCP-1401). Verify that these are the only services listening on network ports. Also, verify that the syslog service is connecting to the central log server.

```
# netstat -anf inet
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address       Foreign Address  (state)
tcp4       0   0    *.22                *.*               LISTEN
tcp4       0   0    *.1169              *.*               LISTEN
tcp4       0   0    *.1401              *.*               LISTEN
tcp4       0   0    10.x.x.x.36871      10.x.x.x.514      ESTABLISHED
tcp4       0 208    10.x.x.x.22         10.x.x.x.37904    ESTABLISHED
```

Notice the "state" column, which shows network services that are "listening" on ports. The only services are TCP-22, TCP-1169, and TCP-1401. The last line which is "established" on TCP-22 is the active SSH connection of the login shell that is used to connect to the server while the "netstat" command is issued.

Notice the "established" connection to port 514 (10.x.x.x.514). This is the syslog connection to the central log server, so we know that the remote syslog service is running properly.

5.1.3 Verify "root" Can Not Login Remotely

This verifies actions performed by the scripts setup_users.sh, setup_misc.sh, and the SSH RPM's.

The hardening procedure disables remote root login using the native AIX security subsystem. Secure Shell is also configured to prevent remote root login. Although the FTP server is disabled, root FTP login is also disabled as a precautionary measure.

Verify that root is configured to not allow remote login. The '-a' option allows the display of selected user attributes. The "rlogin" attribute controls remote logins. The value should be false.

```
# lsuser -a rlogin root
root rlogin=false
```

Verify that SSH is configured to not allow root login. The PermitRootLogin parameter should be set to "no" in the SSH daemon's configuration file.

```
# grep -i root /etc/ssh/sshd_config

#PermitRootLogin yes          (comment, notice the leading #)
# cxt: disable root login     (comment, notice the leading #)
PermitRootLogin no
```

Verify that FTP does not allow root login. We cannot actually verify this since FTP is disabled, but we can check the configuration file.

```
# grep root /etc/ftpusers
root
```

Test remote root login. On another host, try to login as the root user. Notice the failed login attempts are logged on the local server. Despite the wording of the syslog messages, the password entered for root was correct, which is why it is a good idea to try more than once.

Remote host:

```
$ ssh -l root servername
            ************************** WARNING
            ********************************
      .. big bad warning message ..
*******************************************************************
root@servername's password:
Permission denied, please try again.
root@servername's password:
Permission denied, please try again.
root@servername's password:
```

Local host (hardened server):

```
            # tail /var/adm/messages
Apr 24 15:32:00 secure2 sshd[241670]: Failed password for root from
10.98.200.241 port 37973 ssh2
Apr 24 15:32:05 secure2 syslog: ssh: failed login attempt for root from
access1p.nro.glic.com
Apr 24 15:32:15 secure2 sshd[241670]: Failed password for root from
10.98.200.241 port 37973 ssh2
Apr 24 15:32:25 secure2 syslog: ssh: failed login attempt for root from
access1p.nro.glic.com
```

5.1.4 Verify that TCPWrappers is Working

TCPWrappers is compiled into the Secure Shell software so that access controls can be enabled. If you decide to limit specific hosts or networks that are permitted access to SSH, try connecting from a disallowed source. Be sure to try to login as a valid non-root user on the hardened server so that the test is valid. Notice the “refused connect” message in the log file.

Remote host:

```
$ ssh -l doej servername      (john doe user login attempt)
```

Local host (hardened server):

```
# tail /var/adm/messages
Apr 24 15:43:15 secure2 sshd[196826]: refused connect from
10.x.x.x
```

5.1.5 Verify that Cron Usage is Restricted

This verifies actions performed by the scripts setup_cron.sh and setup_perms.sh.

The hardening procedures limit the use of the “at” scheduler to only root, and limit the use of the “cron” scheduler to only root and adm.

Verify the configuration files. Only the “allow” files should exist, and they must be populated with the correct users. The “deny” files should not be found.

```
# cat /var/adm/cron/at.allow
root

# cat /var/adm/cron/cron.allow
root
adm

# ls /var/adm/cron/at.deny /var/adm/cron/cron.deny
ls: 0653-341 The file /var/adm/cron/at.deny does not exist.
ls: 0653-341 The file /var/adm/cron/cron.deny does not exist.
```

Try using the service as a regular user (example uses doej – John Doe).

```
# crontab -l doej
crontab: 0481-109 You are not authorized to use the cron command.
```

The permissions are also restricted on the “at” and “crontab” binaries, so non-root users are not able to even execute the commands. Switch to a regular user account and try to execute the commands.

```
# su - doej
$ crontab -l
ksh: crontab: 0403-006 Execute permission denied.
$ at -l
ksh: at: 0403-006 Execute permission denied.
$ exit
```

5.1.6 Verify that Commercial Tripwire is Installed and Configured

This verifies actions performed by the script setup_tripwire.sh, and it verifies that the Tripwire RPM includes the custom configuration changes.

Verify that the agent daemon is running.

```
            # ps -ef | grep twagent
   root 151568 143566 0 16:15:02 pts/0  0:00 grep twagent
   root 249902      1 0   Apr 06     -  4:00
                              /usr/local/tripwire/tfs/bin/twagent
```

Print the policy file and look for changes to the standard policy.

```
# /usr/local/tripwire/tfs/bin/twadmin --print-polfile | more
# Tripwire text policy
# Generated from binary policy version 4.0.0
            # Tripwire text policy
# Generated from binary policy version 4.0.0
##########################################################################
#                                                                       ##
########################################################################## #
#                                                                       # #
#                General Use Policy file for IBM AIX                    # #
#                            V2.2.5                                     # #
#                         August 26, 2003                               # #
#                                                                      ##
##########################################################################
##########################################################################
```

(Lots more output - omitted)

(The following section is all custom rules that you should see)

```
(rulename="Variable Security Files", emailto=$(SIG_MED_MAILRECIPIENTS),
severity
=$(SIG_MED))
{
   /etc/security/failedlogin -> $(SEC_LOG)-e;
   /etc/security/portlog -> $(SEC_LOG)-e;
   /etc/security/lastlog -> $(SEC_LOG)-e;
   /etc/security/passwd -> $(Dynamic);
               /etc/security/group -> $(Dynamic);
   /etc/security/user -> $(Dynamic);
   /etc/security/pwdhist.dir -> $(Dynamic);
   /etc/security/pwdhist.pag -> $(Dynamic);
   /etc/security/audit/config -> $(IgnoreNone)-ramc;
   !/etc/utmp;
   !/var/audit;
   !/etc/security/oenviron;
   !/etc/security/ogroup;
   !/etc/security/olimits;
   !/etc/security/ologin.cfg;
   !/etc/security/opasswd;
   !/etc/security/oportlog;
   !/etc/security/osmitacl.group;
   !/etc/security/osmitacl.user;
   !/etc/security/osysck.cfg;
   !/etc/security/ouser;
   !/etc/security/ouser.roles;
   !/etc/opasswd;
   !/etc/ogroup;
```

```
!/etc/security/audit/oconfig;
!/etc/sudoers.tmp;
!/etc/security/tcbck.LCK;
        }
```

5.1.7 Verify that Permissions are Restricted on most SUID/SGID Files

This verifies actions performed by the script setup_perms.sh.

The execution permissions for the "other" level is removed for nearly all executable files that have the Set-User-ID or Set-Group-ID bit enabled. Verify that this has been successful.

The following command finds any files with the SUID bit (4000) or SGID (2000) bit enabled and then performs an additional find for the "others" execute bit (0001).

(This is one long line, not two)

```
# find $(find / -perm -2000 -o -perm -4000 -print) -perm -0001
      -exec ls -ld {} \;
```

The following files need to permit "others" to execute them.

```
-r-sr-xr-x  1 root system    6204 Sep 15 2002  /usr/bin/logout
-r-sr-xr-x  1 root security 18830 Aug 21 2003  /usr/bin/passwd
-r-sr-xr-x  1 root system    8266 Sep 15 2002  /usr/bin/rm_mlcache_file
-r-sr-xr-x  1 root security 20274 Aug 21 2003  /usr/bin/su
---s--x--x  1 root system  176286 Mar 20 16:32 /usr/bin/sudo
-rwsr-xr-x  1 root system 1623590 Jun 06 2003
                           /usr/tivoli/tsm/client/ba/bin/dsmtca
-rwsr-xr-x  1 root system 1623590 Jun 06 2003
                           /usr/tivoli/tsm/client/api/bin/dsmtca
```

5.1.8 Verify that Unwanted Users and Groups are Removed

This verifies actions performed by the script setup_users.sh.

Unnecessary users and groups were removed during the hardening process. Verify that they do not exist on the system. No output should result from the commands.

```
# egrep -i 'guest|lp|lpd|uucp|nuucp|snapp' /etc/passwd
# egrep -i 'uucp|ecs|usr|perf|snapp' /etc/group
```

5.1.9 Verify that Auditing is Configured and Running

This verifies actions performed by the script setup_audit.sh.

Detailed auditing is configured during the hardening process, and it can be verified using the following steps.

Verify that auditing is on.

```
# audit query | head -2
auditing on
audit bin manager is process 192656
```

Verify that the “custom” auditing events are configured. The exact output may vary if you elected to change some of the specific events for your shop.

```
# audit query | grep custom

custom – FILE_Owner,FILE_Mode,DEV_Create,TCPIP_config,
TCPIP_connect,PROC_Reboot,FS_Mount,FS_Umount,FILE_Mknod,
FILE_Fchmod,FILE_Fchown,TCP_kbind
```

Verify that the root user and the default user creation are using the custom auditing events.

```
# egrep '(root|default) =' /etc/security/audit/config
root = general,objects,SRC,custom
default = general,objects,SRC,custom
```

Appendix A – Development Toolkit Directory Listing

The following is a listing of the Toolkit Development server's directory /usr/opt/freeware/src/packages so that you may verify your installation and configuration. The BUILD directory is populated with source files during compilation, so you do not need to put any files there manually. Remember, as new versions of the Open Source software is released, the version numbers below will change, but the locations will remain the same.

```
./BUILD
./RPMS
./RPMS/ia64
./RPMS/noarch
./RPMS/powerpc
./RPMS/ppc
./RPMS/ppc/bash-2.05a-1.aix4.3.ppc.rpm
./RPMS/ppc/lsof-4.61-3.aix5.1.ppc.rpm
./RPMS/ppc/openssl-0.9.6m-1.aix5.1.ppc.rpm
./RPMS/ppc/readline-4.2a-1.aix4.3.ppc.rpm
./RPMS/ppc/textutils-2.0-5.aix4.3.ppc.rpm
./RPMS/ppc/unzip-5.42-2.aix4.3.ppc.rpm
./RPMS/ppc/zip-2.3-3.aix4.3.ppc.rpm
./RPMS/ppc/zlib-1.1.4-3.aix4.3.ppc.rpm
./RPMS/ppc/aix-bin-5.2.1.0-0.aix5.2.ppc.rpm
./RPMS/ppc/aix-config-5.2.1.0-0.aix5.2.ppc.rpm
./RPMS/ppc/aix-harden-5.2.1.0-0.aix5.2.ppc.rpm
./RPMS/ppc/aix-never-delete-1.0-0.aix5.2.ppc.rpm
./RPMS/ppc/aix-tsm-5.1.5-1.aix5.2.ppc.rpm
./RPMS/ppc/libol-0.3.9-1.aix5.2.ppc.rpm
./RPMS/ppc/prngd-0.9.27-1.aix5.2.ppc.rpm
./RPMS/ppc/sudo-1.6.7p5-2.aix5.2.ppc.rpm
./RPMS/ppc/tcp_wrappers-7.6-ipv6.3.aix5.2.ppc.rpm
./RPMS/ppc/syslog-ng-1.5.26-0.aix5.2.ppc.rpm
./RPMS/ppc/syslog-ng-server-1.5.26-0.aix5.2.ppc.rpm
./RPMS/ppc/openssh-3.7.1p2-1.aix5.2.ppc.rpm
./RPMS/ppc/openssh-clients-3.7.1p2-1.aix5.2.ppc.rpm
./RPMS/ppc/openssh-server-3.7.1p2-1.aix5.2.ppc.rpm
./RPMS/ppc/radius-server-1.2-0.aix5.2.ppc.rpm
./RPMS/ppc/radius-client-1.2-0.aix5.2.ppc.rpm
./RPMS/ppc/tripwire-4.10-0.aix5.2.ppc.rpm
./SOURCES
./SOURCES/aix-bin-5.2.1.0.tar.gz
./SOURCES/aix-config-5.2.1.0.tar.gz
./SOURCES/aix-harden-5.2.1.0.tar.gz
./SOURCES/aix-tsm-5.1.5.tar.gz
./SOURCES/libol-0.3.9.tar.gz
./SOURCES/openssh-3.7.1p2-config.tar.gz
./SOURCES/openssh-3.7.1p2-pwexp26.patch
./SOURCES/openssh-3.7.1p2.tar.gz
./SOURCES/prngd-0.9.27.tar.gz
./SOURCES/radius-1.2-config.tar.gz
./SOURCES/radius-1.2.tar.gz
```

```
./SOURCES/radius_pam.patch
./SOURCES/sudo-1.6.7p5-config.tar.gz
./SOURCES/sudo-1.6.7p5.tar.gz
./SOURCES/syslog-ng-1.5.26-config.tar.gz
./SOURCES/syslog-ng-1.5.26.tar.gz
./SOURCES/tcp_wrappers_7.6-ipv6.3-config.tar.gz
./SOURCES/tcp_wrappers_7.6-ipv6.3.tar.gz
./SOURCES/aix-config-5.2.1.0
./SOURCES/aix-config-5.2.1.0/catalog.mic
./SOURCES/aix-config-5.2.1.0/environment
./SOURCES/aix-config-5.2.1.0/motd
./SOURCES/aix-config-5.2.1.0/netsvc.conf
./SOURCES/aix-config-5.2.1.0/ntp.conf
./SOURCES/aix-config-5.2.1.0/pam.conf
./SOURCES/aix-config-5.2.1.0/pam.conf.no_rad
./SOURCES/aix-config-5.2.1.0/pam.conf.rad
./SOURCES/aix-config-5.2.1.0/profile
./SOURCES/aix-config-5.2.1.0/resolv.conf
./SOURCES/aix-config-5.2.1.0/sendmail.cf
./SOURCES/aix-config-5.2.1.0/words
./SOURCES/syslog-ng-server.conf
./SOURCES/sudoers
./SOURCES/radius_client.conf
./SOURCES/aix-bin-5.2.1.0
./SOURCES/aix-bin-5.2.1.0/log-rotate.conf
./SOURCES/aix-bin-5.2.1.0/log-rotate.sh
./SOURCES/aix-bin-5.2.1.0/ntpset.sh
./SOURCES/ssh_config
./SOURCES/syslog-ng.conf
./SOURCES/sshd_config
./SOURCES/hosts.deny
./SOURCES/hosts.allow
./SOURCES/aix-harden-5.2.1.0
./SOURCES/aix-harden-5.2.1.0/setup_aix.sh
./SOURCES/aix-harden-5.2.1.0/setup_audit.sh
./SOURCES/aix-harden-5.2.1.0/setup_boot.sh
./SOURCES/aix-harden-5.2.1.0/setup_rc.netparms
./SOURCES/aix-harden-5.2.1.0/setup_cleanup.sh
./SOURCES/aix-harden-5.2.1.0/setup_cron.sh
./SOURCES/aix-harden-5.2.1.0/setup_ftpusers.conf
./SOURCES/aix-harden-5.2.1.0/setup_errlog.sh
./SOURCES/aix-harden-5.2.1.0/setup_filesystems.sh
./SOURCES/aix-harden-5.2.1.0/setup_lpp.sh
./SOURCES/aix-harden-5.2.1.0/setup_maintlevel.sh
./SOURCES/aix-harden-5.2.1.0/setup_mirror.sh
./SOURCES/aix-harden-5.2.1.0/setup_misc.sh
./SOURCES/aix-harden-5.2.1.0/setup_perms.sh
./SOURCES/aix-harden-5.2.1.0/setup_profile.conf
./SOURCES/aix-harden-5.2.1.0/setup_daemons_nfs.conf
./SOURCES/aix-harden-5.2.1.0/setup_registry.sh
./SOURCES/aix-harden-5.2.1.0/setup_rpm.sh
./SOURCES/aix-harden-5.2.1.0/setup_perms.conf
./SOURCES/aix-harden-5.2.1.0/setup_tcb.sh
./SOURCES/aix-harden-5.2.1.0/setup_tcb_state.sh
./SOURCES/aix-harden-5.2.1.0/setup_users.sh
./SOURCES/aix-harden-5.2.1.0/setup_rpm_add.conf
./SOURCES/aix-harden-5.2.1.0/setup_radius.sh
```

```
./SOURCES/aix-harden-5.2.1.0/setup_users_gdel.conf
./SOURCES/aix-harden-5.2.1.0/setup_users_udel.conf
./SOURCES/aix-harden-5.2.1.0/setup_users_unum.conf
./SOURCES/aix-harden-5.2.1.0/setup_users_gnum.conf
./SOURCES/aix-harden-5.2.1.0/setup_sec_files.sh
./SOURCES/aix-harden-5.2.1.0/setup_daemons.sh
./SOURCES/aix-harden-5.2.1.0/setup_daemons_init.conf
./SOURCES/aix-harden-5.2.1.0/setup_rpm_del.conf
./SOURCES/aix-harden-5.2.1.0/setup_errlog.conf
./SOURCES/aix-harden-5.2.1.0/setup_perms_local.conf
./SOURCES/aix-harden-5.2.1.0/setup_daemons_inetd.conf
./SOURCES/aix-harden-5.2.1.0/setup_daemons_tcpip.conf
./SOURCES/aix-harden-5.2.1.0/setup_users_admin.conf
./SOURCES/aix-harden-5.2.1.0/setup_filesystems.conf
./SOURCES/aix-harden-5.2.1.0/setup_tripwire.sh
./SOURCES/tripwire-4.10-config.tar.gz
./SOURCES/tripwire-4.10.tar.gz
./SOURCES/aix-tsm-5.1.5
./SOURCES/aix-tsm-5.1.5/dsm.sys
./SOURCES/aix-tsm-5.1.5/inclexcl
./SOURCES/aix-tsm-5.1.5/starttsm.sh
./SOURCES/aix-tsm-5.1.5/dsm.sys.template
./SPECS
./SPECS/aix-bin.spec
./SPECS/aix-config.spec
./SPECS/aix-harden.spec
./SPECS/aix-never-delete.spec
./SPECS/aix-tsm.spec
./SPECS/libol.spec
./SPECS/openssh.spec
./SPECS/prngd.spec
./SPECS/radius.spec
./SPECS/sudo.spec
./SPECS/syslog-ng.spec
./SPECS/tcp_wrappers.spec
./SPECS/tripwire.spec
./SRPMS
./SRPMS/aix-bin-5.2.1.0-0.src.rpm
./SRPMS/aix-config-5.2.1.0-0.src.rpm
./SRPMS/aix-harden-5.2.1.0-0.src.rpm
./SRPMS/aix-never-delete-1.0-0.src.rpm
./SRPMS/aix-tsm-5.1.5-1.src.rpm
./SRPMS/tcp_wrappers-7.6-ipv6.3.src.rpm
./SRPMS/prngd-0.9.27-1.src.rpm
./SRPMS/libol-0.3.9-1.src.rpm
./SRPMS/syslog-ng-1.5.26-0.src.rpm
./SRPMS/sudo-1.6.7p5-2.src.rpm
./SRPMS/radius-1.2-0.src.rpm
./SRPMS/openssh-3.7.1p2-1.src.rpm
./SRPMS/tripwire-4.10-0.src.rpm
./DEVEL-KIT
./DEVEL-KIT/autoconf-2.53-1.aix4.3.noarch.rpm
./DEVEL-KIT/automake-1.5-1.aix4.3.noarch.rpm
./DEVEL-KIT/binutils-2.9.aix51.020209-4.aix5.2.ppc.rpm
./DEVEL-KIT/bison-1.34-2.aix4.3.ppc.rpm
./DEVEL-KIT/bzip2-1.0.2-2.aix4.3.ppc.rpm
./DEVEL-KIT/db-3.3.11-3.aix4.3.ppc.rpm
```

```
./DEVEL-KIT/fileutils-4.1-4.aix4.3.ppc.rpm
./DEVEL-KIT/findutils-4.1-3.aix4.3.ppc.rpm
./DEVEL-KIT/flex-2.5.4a-6.aix4.3.ppc.rpm
./DEVEL-KIT/gawk-3.1.0-2.aix4.3.ppc.rpm
./DEVEL-KIT/gcc-2.9.aix51.020209-4.aix5.2.ppc.rpm
./DEVEL-KIT/gdbm-1.8.0-5.aix4.3.ppc.rpm
./DEVEL-KIT/gdbm-devel-1.8.0-5.aix4.3.ppc.rpm
./DEVEL-KIT/gettext-0.10.39-2.aix4.3.ppc.rpm
./DEVEL-KIT/libtool-1.4.2-1.aix4.3.ppc.rpm
./DEVEL-KIT/m4-1.4-14.aix4.3.ppc.rpm
./DEVEL-KIT/make-3.79.1-3.aix4.3.ppc.rpm
./DEVEL-KIT/popt-1.7-1.aix4.3.ppc.rpm
./DEVEL-KIT/readline-devel-4.2a-1.aix4.3.ppc.rpm
./DEVEL-KIT/texinfo-4.0-8.aix4.3.ppc.rpm
./DEVEL-KIT/zlib-devel-1.1.4-3.aix4.3.ppc.rpm
./DEVEL-KIT/openssl-devel-0.9.6m-1.aix5.1.ppc.rpm
./INSTALL
./LPP
./LPP/bos.content_list
./LPP/bos.content_list/bos.content_list.5.2.0.0.I
./LPP/bos.content_list/.toc
./LPP/tsm
./LPP/tsm/README
./LPP/tsm/README.FTP
./LPP/tsm/TSM520_GA.README.32bit
./LPP/tsm/TSM520_GA.README.API.32bit
./LPP/tsm/TSM520_GA.README.GUID
./LPP/tsm/TSM520_GA.tivoli.tivguid
./LPP/tsm/TSM520_GA.tivoli.tsm.books.en_US.client
./LPP/tsm/TSM520_GA.tivoli.tsm.client.api.32bit
./LPP/tsm/TSM520_GA.tivoli.tsm.client.ba.32bit
./LPP/tsm/.toc
./LPP/bos.dosutil
./LPP/bos.dosutil/bos.dosutil.5.2.0.0.I
./LPP/bos.dosutil/.toc
./LPP/perf_monitor
./LPP/perf_monitor/installp
./LPP/perf_monitor/installp/ppc
./LPP/perf_monitor/installp/ppc/bos.vendor.profile
./LPP/perf_monitor/installp/ppc/bos.sysmgt.5.2.0.0.I
./LPP/perf_monitor/installp/ppc/bos.perf.5.2.0.0.I
./LPP/perf_monitor/installp/ppc/perfagent.tools.5.2.0.0.I
./LPP/perf_monitor/installp/ppc/.toc
./LPP/perf_monitor/usr
./LPP/perf_monitor/usr/swlag
./LPP/perf_monitor/usr/swlag/Ja_JP
./LPP/perf_monitor/usr/swlag/Ja_JP/BOS.la
./LPP/perf_monitor/usr/swlag/Zh_TW
./LPP/perf_monitor/usr/swlag/Zh_TW/BOS.la
./LPP/perf_monitor/usr/swlag/de_DE
./LPP/perf_monitor/usr/swlag/de_DE/BOS.la
./LPP/perf_monitor/usr/swlag/en_US
./LPP/perf_monitor/usr/swlag/en_US/BOS.la
./LPP/perf_monitor/usr/swlag/es_ES
./LPP/perf_monitor/usr/swlag/es_ES/BOS.la
./LPP/perf_monitor/usr/swlag/fr_FR
./LPP/perf_monitor/usr/swlag/fr_FR/BOS.la
```

```
./LPP/perf_monitor/usr/swlag/it_IT
./LPP/perf_monitor/usr/swlag/it_IT/BOS.la
./LPP/perf_monitor/usr/swlag/ja_JP
./LPP/perf_monitor/usr/swlag/ja_JP/BOS.la
./LPP/perf_monitor/usr/swlag/ko_KR
./LPP/perf_monitor/usr/swlag/ko_KR/BOS.la
./LPP/perf_monitor/usr/swlag/pt_BR
./LPP/perf_monitor/usr/swlag/pt_BR/BOS.la
./LPP/perf_monitor/usr/swlag/ru_RU
./LPP/perf_monitor/usr/swlag/ru_RU/BOS.la
./LPP/perf_monitor/usr/swlag/zh_CN
./LPP/perf_monitor/usr/swlag/zh_CN/BOS.la
./LPP/perf_monitor/usr/swlag/zh_TW
./LPP/perf_monitor/usr/swlag/zh_TW/BOS.la
./LPP/diagnostics
./LPP/diagnostics/installp
./LPP/diagnostics/installp/ppc
./LPP/diagnostics/installp/ppc/.toc
./LPP/diagnostics/installp/ppc/bos.vendor.profile
./LPP/diagnostics/installp/ppc/devices.chrp.base.5.2.0.0.I
./LPP/diagnostics/installp/ppc/devices.common.IBM.modemcfg.5.2.0.0.I
./LPP/diagnostics/installp/ppc/devices.common.base.5.2.0.0.I
./LPP/diagnostics/usr
./LPP/diagnostics/usr/swlag
./LPP/diagnostics/usr/swlag/Ja_JP
./LPP/diagnostics/usr/swlag/Ja_JP/BOS.la
./LPP/diagnostics/usr/swlag/Zh_TW
./LPP/diagnostics/usr/swlag/Zh_TW/BOS.la
./LPP/diagnostics/usr/swlag/de_DE
./LPP/diagnostics/usr/swlag/de_DE/BOS.la
./LPP/diagnostics/usr/swlag/en_US
./LPP/diagnostics/usr/swlag/en_US/BOS.la
./LPP/diagnostics/usr/swlag/es_ES
./LPP/diagnostics/usr/swlag/es_ES/BOS.la
./LPP/diagnostics/usr/swlag/fr_FR
./LPP/diagnostics/usr/swlag/fr_FR/BOS.la
./LPP/diagnostics/usr/swlag/it_IT
./LPP/diagnostics/usr/swlag/it_IT/BOS.la
./LPP/diagnostics/usr/swlag/ja_JP
./LPP/diagnostics/usr/swlag/ja_JP/BOS.la
./LPP/diagnostics/usr/swlag/ko_KR
./LPP/diagnostics/usr/swlag/ko_KR/BOS.la
./LPP/diagnostics/usr/swlag/pt_BR
./LPP/diagnostics/usr/swlag/pt_BR/BOS.la
./LPP/diagnostics/usr/swlag/ru_RU
./LPP/diagnostics/usr/swlag/ru_RU/BOS.la
./LPP/diagnostics/usr/swlag/zh_CN
./LPP/diagnostics/usr/swlag/zh_CN/BOS.la
./LPP/diagnostics/usr/swlag/zh_TW
./LPP/diagnostics/usr/swlag/zh_TW/BOS.la
./MAINT
./MAINT/5200-02
./MAINT/5200-02/U482897.bff
./MAINT/5200-02/U476795.bff
./MAINT/5200-02/U482895.bff
./MAINT/5200-02/U485377.bff
./MAINT/5200-02/U482893.bff
```

```
./MAINT/5200-02/U485143.bff
./MAINT/5200-02/U482901.bff
./MAINT/5200-02/U485381.bff
./MAINT/5200-02/U485379.bff
./MAINT/5200-02/U485384.bff
./MAINT/5200-02/U485383.bff
./MAINT/5200-02/U485401.bff
./MAINT/5200-02/U485189.bff
./MAINT/5200-02/U485418.bff
./MAINT/5200-02/U485423.bff
./MAINT/5200-02/U485422.bff
./MAINT/5200-02/U485371.bff
./MAINT/5200-02/U485438.bff
./MAINT/5200-02/U485126.bff
./MAINT/5200-02/U485412.bff
./MAINT/5200-02/U485429.bff
./MAINT/5200-02/U485121.bff
./MAINT/5200-02/U485179.bff
./MAINT/5200-02/U485138.bff
./MAINT/5200-02/U485186.bff
./MAINT/5200-02/U485135.bff
./MAINT/5200-02/U485369.bff
./MAINT/5200-02/U485122.bff
./MAINT/5200-02/U485152.bff
./MAINT/5200-02/U485191.bff
./MAINT/5200-02/U485155.bff
./MAINT/5200-02/U485426.bff
./MAINT/5200-02/U485147.bff
./MAINT/5200-02/U485424.bff
./MAINT/5200-02/U485427.bff
./MAINT/5200-02/U485130.bff
./MAINT/5200-02/U485425.bff
./MAINT/5200-02/U485129.bff
./MAINT/5200-02/U485415.bff
./MAINT/5200-02/U485409.bff
./MAINT/5200-02/U485158.bff
./MAINT/5200-02/U485445.bff
./MAINT/5200-02/U485428.bff
./MAINT/5200-02/.toc
./MAINT/5200-02/U485430.bff
./MAINT/5200-02/U485160.bff
./MAINT/5200-02/U485437.bff
./MAINT/5200-02/U485162.bff
./MAINT/5200-02/U485413.bff
./MAINT/5200-02/U485433.bff
./MAINT/5200-02/U485133.bff
./MAINT/5200-02/U485408.bff
./MAINT/5200-02/U485188.bff
./MAINT/5200-02/U485391.bff
./MAINT/5200-02/U485153.bff
./MAINT/5200-02/U485372.bff
./MAINT/5200-02/U485169.bff
./MAINT/5200-02/U485374.bff
./MAINT/5200-02/U485373.bff
./MAINT/5200-02/U485159.bff
./MAINT/5200-02/U485406.bff
./MAINT/5200-02/U485441.bff
```

```
./MAINT/5200-02/U485166.bff
./MAINT/5200-02/U485131.bff
./MAINT/5200-02/U485411.bff
./MAINT/5200-02/U485132.bff
./MAINT/5200-02/U485393.bff
./MAINT/5200-02/U485170.bff
./MAINT/5200-02/U485443.bff
./MAINT/5200-02/U485392.bff
./MAINT/5200-02/U485452.bff
./MAINT/5200-02/U485453.bff
./MAINT/5200-02/U485454.bff
./MAINT/5200-02/U485461.bff
./MAINT/5200-02/U485462.bff
./MAINT/5200-02/U485463.bff
./MAINT/5200-02/U485762.bff
./MAINT/5200-02/U485768.bff
./MAINT/5200-02/U485891.bff
./MAINT/5200-02/U485892.bff
./MAINT/5200-02/U485893.bff
./MAINT/5200-02/U485975.bff
./MAINT/5200-02/U485976.bff
./MAINT/5200-02/U485978.bff
./MAINT/5200-02/U485979.bff
./MAINT/5200-02/U485984.bff
./MAINT/5200-02/U485985.bff
./MAINT/5200-02/U485986.bff
./MAINT/5200-02/U485989.bff
./MAINT/5200-02/U485991.bff
./MAINT/5200-02/U485994.bff
./MAINT/5200-02/U485995.bff
./MAINT/5200-02/U485996.bff
./MAINT/5200-02/U485997.bff
./MAINT/5200-02/U485998.bff
./MAINT/5200-02/U485999.bff
./MAINT/5200-02/U486001.bff
./MAINT/5200-02/U486004.bff
./MAINT/5200-02/U486005.bff
./MAINT/5200-02/U486007.bff
./MAINT/5200-02/U486008.bff
./MAINT/5200-02/U486009.bff
./MAINT/5200-02/U486010.bff
./MAINT/5200-02/U486014.bff
./MAINT/5200-02/U486015.bff
./MAINT/5200-02/U486018.bff
./MAINT/5200-02/U486019.bff
./MAINT/5200-02/U486020.bff
./MAINT/5200-02/U486021.bff
./MAINT/5200-02/U486022.bff
./MAINT/5200-02/U486027.bff
./MAINT/5200-02/U486028.bff
./MAINT/5200-02/U486029.bff
./MAINT/5200-02/U486032.bff
./MAINT/5200-02/U486034.bff
./MAINT/5200-02/U486035.bff
./MAINT/5200-02/U486037.bff
./MAINT/5200-02/U486042.bff
./MAINT/5200-02/U486045.bff
```

```
./MAINT/5200-02/U486046.bff
./MAINT/5200-02/U486048.bff
./MAINT/5200-02/U486049.bff
./MAINT/5200-02/U486050.bff
./MAINT/5200-02/U486052.bff
./MAINT/5200-02/U486054.bff
./MAINT/5200-02/U486055.bff
./MAINT/5200-02/U486056.bff
./MAINT/5200-02/U486062.bff
./MAINT/5200-02/U486063.bff
./MAINT/5200-02/U486064.bff
./MAINT/5200-02/U486033.bff
./MAINT/5200-02/U486006.bff
./MAINT/5200-02/U485993.bff
./MAINT/5200-02/U486060.bff
./MAINT/5200-02/U486000.bff
./MAINT/5200-02/U486031.bff
./MAINT/5200-02/U486003.bff
./MAINT/5200-02/U486025.bff
./MAINT/5200-02/U486024.bff
./MAINT/5200-02/U485990.bff
./MAINT/5200-02/U486053.bff
./MAINT/5200-02/U486051.bff
./MAINT/5200-02/U485981.bff
./MAINT/5200-02/U486016.bff
./MAINT/5200-02/U485982.bff
./MAINT/5200-02/U486012.bff
./MAINT/5200-02/U486011.bff
./MAINT/5200-02/U485987.bff
./MAINT/5200-02/U486039.bff
./MAINT/5200-02/U486067.bff
./MAINT/5200-02/U486072.bff
./MAINT/5200-02/U486074.bff
./MAINT/5200-02/U486435.bff
./MAINT/5200-02/U486466.bff
./MAINT/5200-02/U486483.bff
./MAINT/5200-02/U486485.bff
./MAINT/5200-02/U486486.bff
./MAINT/5200-02/U486513.bff
./MAINT/5200-02/U486522.bff
./MAINT/5200-02/U486523.bff
./MAINT/5200-02/U486525.bff
./MAINT/5200-02/U486526.bff
./MAINT/5200-02/U486527.bff
./MAINT/5200-02/U486528.bff
./MAINT/5200-02/U486529.bff
./MAINT/5200-02/U486530.bff
./MAINT/5200-02/U488347.bff
./MAINT/5200-02/U488779.bff
./MAINT/5200-02/U488785.bff
./MAINT/5200-02/U488789.bff
./MAINT/5200-02/U488820.bff
./MAINT/5200-02/U488823.bff
./MAINT/5200-02/U488831.bff
./MAINT/5200-02/U488832.bff
./MAINT/5200-02/U488834.bff
./MAINT/5200-02/U488863.bff
```

```
./MAINT/5200-02/U488864.bff
./MAINT/5200-02/U488865.bff
./MAINT/5200-02/U488866.bff
./MAINT/5200-02/U488869.bff
./MAINT/5200-02/U488871.bff
./MAINT/5200-02/U488872.bff
./MAINT/5200-02/U488361.bff
./MAINT/5200-02/U488356.bff
./MAINT/5200-02/U487959.bff
./MAINT/5200-02/U487973.bff
./MAINT/5200-02/U487970.bff
./MAINT/5200-02/U487955.bff
./MAINT/5200-02/U487972.bff
./MAINT/5200-02/U487965.bff
./MAINT/5200-02/U487971.bff
./MAINT/5200-02/U487977.bff
./MAINT/5200-02/U487975.bff
./MAINT/5200-02/U486487.bff
./MAINT/5200-02/U486495.bff
./MAINT/5200-02/U486068.bff
./MAINT/5200-02/U488794.bff
./MAINT/5200-02/U488795.bff
./MAINT/5200-02/U488797.bff
./MAINT/5200-02/U488791.bff
./MAINT/5200-02/U488796.bff
./MAINT/5200-02/U486467.bff
./MAINT/5200-02/U488798.bff
./MAINT/5200-02/U486491.bff
./MAINT/5200-02/U488870.bff
./MAINT/5200-02/U488814.bff
./MAINT/5200-02/U488349.bff
./MAINT/5200-02/U487958.bff
./MAINT/5200-02/U486505.bff
./MAINT/5200-02/U487957.bff
./MAINT/5200-02/U486446.bff
./MAINT/5200-02/U486474.bff
./MAINT/5200-02/U486502.bff
./MAINT/5200-02/U486501.bff
./MAINT/5200-02/U486510.bff
./MAINT/5200-02/U486462.bff
./MAINT/5200-02/U488858.bff
./MAINT/5200-02/U486504.bff
./MAINT/5200-02/U486521.bff
./MAINT/5200-02/U488818.bff
./MAINT/5200-02/U488353.bff
./MAINT/5200-02/U486431.bff
./MAINT/5200-02/U488359.bff
./MAINT/5200-02/U488354.bff
./MAINT/5200-02/U488867.bff
./MAINT/5200-02/U488837.bff
./MAINT/5200-02/U486432.bff
./MAINT/5200-02/U487953.bff
./MAINT/5200-02/U488830.bff
./MAINT/5200-02/U486073.bff
./MAINT/5200-02/U487981.bff
./MAINT/5200-02/U488810.bff
./MAINT/5200-02/U486071.bff
```

```
./MAINT/5200-02/U488358.bff
./MAINT/5200-02/U488827.bff
./MAINT/5200-02/U488844.bff
./MAINT/5200-02/U488835.bff
./MAINT/5200-02/U486454.bff
./MAINT/5200-02/U488868.bff
./MAINT/5200-02/U486493.bff
./MAINT/5200-02/U486519.bff
./MAINT/5200-02/U488857.bff
./MAINT/5200-02/U488786.bff
./MAINT/5200-02/U488357.bff
./MAINT/5200-02/U488792.bff
./MAINT/5200-02/U486503.bff
./MAINT/5200-02/U487979.bff
./MAINT/5200-02/U487976.bff
./MAINT/5200-02/U488360.bff
./MAINT/5200-02/U487968.bff
./MAINT/5200-02/U487978.bff
./MAINT/5200-02/U487980.bff
./MAINT/5200-02/U487967.bff
./MAINT/5200-02/U486492.bff
./MAINT/5200-02/U487960.bff
./MAINT/5200-02/U488824.bff
./MAINT/5200-02/U487962.bff
./MAINT/5200-02/U487956.bff
./MAINT/5200-02/U487974.bff
./MAINT/5200-02/U487964.bff
./MAINT/5200-02/U487961.bff
./MAINT/5200-02/U488851.bff
./MAINT/5200-02/U488348.bff
./MAINT/5200-02/U486456.bff
./MAINT/5200-02/U486496.bff
./MAINT/5200-02/U487963.bff
./MAINT/5200-02/U488784.bff
./MAINT/5200-02/U487966.bff
./MAINT/5200-02/U488873.bff
./MAINT/5200-02/U488877.bff
./MAINT/5200-02/U489150.bff
./MAINT/5200-02/U489151.bff
./MAINT/5200-02/U489152.bff
./MAINT/5200-02/U489867.bff
./MAINT/5200-02/U489869.bff
./MAINT/5200-02/U489870.bff
./MAINT/5200-02/U489874.bff
./MAINT/5200-02/U489875.bff
./MAINT/5200-02/U489877.bff
./MAINT/5200-02/U489885.bff
./MAINT/5200-02/U489896.bff
./MAINT/5200-02/U489897.bff
./MAINT/5200-02/U489898.bff
./MAINT/5200-02/U489899.bff
./MAINT/5200-02/U489900.bff
./MAINT/5200-02/U489901.bff
./MAINT/5200-02/U489902.bff
./MAINT/5200-02/U489903.bff
./MAINT/5200-02/U489904.bff
./MAINT/5200-02/U489905.bff
```

```
./MAINT/5200-02/U489911.bff
./MAINT/5200-02/U489912.bff
./MAINT/5200-02/U489913.bff
./MAINT/5200-02/U489915.bff
./MAINT/5200-02/U489920.bff
./MAINT/5200-02/U489921.bff
./MAINT/5200-02/U489922.bff
./MAINT/5200-02/U489923.bff
./MAINT/5200-02/U489924.bff
./MAINT/5200-02/U489925.bff
./MAINT/5200-02/U489926.bff
./MAINT/5200-02/U489927.bff
./MAINT/5200-02/U489928.bff
./MAINT/5200-02/U489929.bff
./MAINT/5200-02/U489930.bff
./MAINT/5200-02/U489931.bff
./MAINT/5200-02/U489932.bff
./MAINT/5200-02/U489933.bff
./MAINT/5200-02/U489934.bff
./MAINT/5200-02/U489935.bff
./MAINT/5200-02/U489936.bff
./MAINT/5200-02/U489937.bff
./MAINT/5200-02/U489938.bff
./MAINT/5200-02/U489939.bff
./MAINT/5200-02/U489940.bff
./MAINT/5200-02/U489942.bff
./MAINT/5200-02/U489943.bff
./MAINT/5200-02/U489944.bff
./MAINT/5200-02/U489945.bff
./MAINT/5200-02/U489946.bff
./MAINT/5200-02/U489947.bff
./MAINT/5200-02/U489950.bff
./MAINT/5200-02/U489952.bff
./MAINT/5200-02/U489953.bff
./MAINT/5200-02/U495551.bff
./MAINT/5200-02/U495552.bff
./MAINT/5200-02/U495553.bff
./MAINT/5200-02/U495932.bff
./MAINT/5200-02/U489954.bff
./MAINT/5200-02/U489910.bff
./MAINT/5200-02/U495933.bff
./MAINT/5200-02/U489908.bff
./MAINT/5200-02/U489948.bff
./MAINT/5200-02/U489873.bff
./MAINT/5200-02/U488914.bff
./MAINT/5200-02/U489893.bff
./MAINT/5200-02/U495934.bff
./MAINT/5200-02/U495935.bff
./MAINT/5200-02/U495936.bff
./MAINT/5200-02/U495937.bff
./MAINT/5200-02/U489916.bff
./MAINT/5200-02/U489895.bff
./MAINT/5200-02/U489917.bff
./MAINT/5200-02/U489907.bff
./MAINT/5200-02/U489918.bff
./MAINT/5200-02/U489887.bff
./MAINT/5200-02/U495938.bff
```

```
./MAINT/5200-02/U489892.bff
./MAINT/5200-02/U489919.bff
./MAINT/5200-02/U495939.bff
./MAINT/5200-02/U489888.bff
./MAINT/5200-02/U495940.bff
./MAINT/5200-02/U489914.bff
./MAINT/5200-02/U489941.bff
./MAINT/5200-02/U489909.bff
./MAINT/5200-02/U495941.bff
./MAINT/5200-02/U489951.bff
./MAINT/5200-02/U489884.bff
./MAINT/5200-02/U489883.bff
./MAINT/5200-02/U489949.bff
./MAINT/5200-02/U489906.bff
./MAINT/5200-02/U495907.bff
./MAINT/5200-02/U495908.bff
./MAINT/5200-02/U495909.bff
./MAINT/5200-02/U495910.bff
./MAINT/5200-02/U495911.bff
./MAINT/5200-02/U489854.bff
./MAINT/5200-02/U495556.bff
./MAINT/5200-02/U489846.bff
./MAINT/5200-02/U489857.bff
./MAINT/5200-02/U489852.bff
./MAINT/5200-02/U489850.bff
./MAINT/5200-02/U489844.bff
./MAINT/5200-02/U495554.bff
./MAINT/5200-02/U495555.bff
./MAINT/5200-02/U495550.bff
./MAINT/5200-02/U495942.bff
./MAINT/5200-02/U489843.bff
./MAINT/5200-02/U495943.bff
./MAINT/5200-02/U489395.bff
./PATCHES
./PATCHES/5200-02
./PATCHES/5200-02/bos.adt.include.5.2.0.15.bff
./PATCHES/5200-02/bos.mp.5.2.0.19.bff
./PATCHES/5200-02/bos.mp64.5.2.0.19.bff
./PATCHES/5200-02/bos.net.nisplus.5.2.0.15.bff
./PATCHES/5200-02/bos.net.tcp.client.5.2.0.17.bff
./PATCHES/5200-02/bos.net.tcp.server.5.2.0.17.bff
./PATCHES/5200-02/bos.perf.diag_tool.5.2.0.12.bff
./PATCHES/5200-02/bos.perf.perfstat.5.2.0.14.bff
./PATCHES/5200-02/bos.perf.tools.5.2.0.17.bff
./PATCHES/5200-02/bos.perf.tune.5.2.0.16.bff
./PATCHES/5200-02/bos.rte.5.2.0.12.bff
./PATCHES/5200-02/bos.rte.archive.5.2.0.14.bff
./PATCHES/5200-02/bos.rte.boot.5.2.0.14.bff
./PATCHES/5200-02/bos.rte.filesystem.5.2.0.15.bff
./PATCHES/5200-02/bos.rte.install.5.2.0.15.bff
./PATCHES/5200-02/bos.rte.libc.5.2.0.17.bff
./PATCHES/5200-02/bos.rte.libpthreads.5.2.0.15.bff
./PATCHES/5200-02/bos.rte.shell.5.2.0.17.bff
./PATCHES/5200-02/bos.sysmgt.serv_aid.5.2.0.17.bff
./PATCHES/5200-02/bos.sysmgt.sysbr.5.2.0.16.bff
./PATCHES/5200-02/bos.up.5.2.0.19.bff
./PATCHES/5200-02/devices.chrp.base.rte.5.2.0.14.bff
```

```
./PATCHES/5200-02/devices.chrp.pci.rte.5.2.0.13.bff
./PATCHES/5200-02/devices.common.IBM.ethernet.rte.5.2.0.14.bff
./PATCHES/5200-02/dlmgr.pro
./PATCHES/5200-02/.toc
```

References

Batten, David. Joglar, Antonio. St. Clair, Linda. Schreitmueller, Susan. Sanchez, Rebecca. International Business Machines. "Strengthening AIX Security: A System Hardening Approach". 26 March 2002. URL: http://www-1.ibm.com/servers/aix/whitepapers/aix_security.pdf (3 May 2004).

Jenkinson, John. "Securing Unix GCUX Practical Assignment". URL: http://www.giac.org/practical/John_Jenkinson_GCUX.doc (3 May 2004).

Gresham, Austin. "Securing AIX5L, Version 5.1 on an RS/6000 E30". URL: http://www.giac.org/practical/Austin_Gresham_GCUX.doc (3 May 2004).

Lee, Kenneth. "AIX 4.3 Installation Checklist". URL: http://www.giac.org/practical/Kenneth_H_Lee_GCUX.zip (3 May 2004).

Hardcastle, Jodi. "AIX 4.3 Installation Checklist". URL: http://www.giac.org/practical/Jodi_Hardcastle_GCUX.zip (3 May 2004).

Caines, Devon. "A Guide to Building and Securing an Intranet Mail Server/Hub with AIX 5L Version 5.1". URL: http://www.giac.org/practical/Devon_Caines_GCUX.doc (3 May 2004).

ThinkSec AS and Network Associates Laboratories. "Pluggable Authentication Modules". Version 1.27. 12 December 2003. URL: http://www.freebsd.org/doc/en_US.ISO8859-1/articles/pam/article.html (3 May 2004).

International Business Machines. "Security Guide – AIX 5L Version 5.2". Third Edition. July 2003. URL: http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm (3 May 2004)

Tucker, Darren. "Darren Tucker's OpenSSH Page". URL: http://www.zip.com.au/~dtucker/openssh/ (3 May 2004).

Poirier, Dan. International Business Machines. "Packaging software with RPM, Part 1". 1 November 2001. URL: http://www-106.ibm.com/developerworks/linux/library/l-rpm1/ (3 May 2004).

Poirier, Dan. International Business Machines. "Packaging software with RPM, Part 2". 1 December 2001. URL: http://www-106.ibm.com/developerworks/linux/library/l-rpm2/ (3 May 2004).

Poirier, Dan. International Business Machines. “Packaging software with RPM, Part 3”. 1 February 2002. URL: http://www-106.ibm.com/developerworks/linux/library/l-rpm3.html (3 May 2004).