Global Information Assurance Certification Paper

AIX 4.3 Installation Checklist

This is an administrative checklist for a secure installation of AIX 4.3 on an IBM PCI RS/6000 B50 platform. The hardware includes one 375MHz processor, 512MB memory, and two 18.2GB SCSI disk drives. This particular server will host an Enterprise Application Integration (EAI) engine used to coordinate transactions between several application servers in a hospital environment. Users will be allowed to access the server remotely. Sendmail will be configured for operational reasons. DNS will not be installed, however the server will be a DNS client. All filesystems will be local.

*AIX supports a multitude of applications (each with their own unique requirements) in any number of conceivable environments making it impossible to create a single, default security environment that applies to all. Thus, the security level you set up in AIX needs to be tailored to the customer and application environment where the server is deployed.

**For security reasons this server will be built off-line, there will be instances when use of another AIX 4.3 server will be required for downloads. All commands will require an absolute path. We will be using an IBM-3153 ascii terminal attached to the first serial port. This checklist assumes the "driver" is comfortable with basic UNIX commands and the vi editor.*

Pre-Installation Information:

Basic information you will need prior to beginning the installation process.

Hostname: _____
IP Address: ____.____.____.____
Sub-net Mask: ____.____.____.____
Domain: _____
Primary DNS: ____.____.____.____
Secondary DNS: ____.____.____.____

AIX 4.3 Installation

Most IBM RS/6000 servers will arrive pre-built from the vendor. You will need to accomplish a complete reinstallation to enable the Trusted Computing Base (TCB) and minimize the amount of packages installed on the system. When you start-up the system for the first time it will boot into the Installation Assistant Menu, the following checklist assumes you are starting there.

Re-Install with Trusted Computing Base:

_____ 1. Type **0** to select system console
_____ 2. Set **Terminal Type** (*model # on monitor, if not listed pick closest; eg, ibm3151*)
_____ 3. **Set password** for administrator (root)
_____ 4. **Exit** the Configuration Assistant
_____ 5. **Login as root** using the password you just set
_____ 6. Place **Installation CD in CD-ROM** drive

_____ 7. **/usr/sbin/shutdown –Fr** to reboot system
**If the system does not boot from the CD you will need to edit the boot sequence, refer to the appendix for instructions*.
_____ 8. Type **1** then <**enter>** to use this device as the system console
_____ 9. Type **1** then <**enter>** to use English during install
_____ 10. Choose **#2 - Change/Show Installation Settings and Install**
_____ 11. Choose **#1 - System Settings**
_____ 12. Choose **#1 - New and Complete Overwrite**
_____ 13. Choose **Installation Disk** (*hdisk0*) then **0** to exit
_____ 14. Verify Primary Language is set to **English**
_____ 15. Choose **#3 - Install Trusted Computing Base (TCB)**
_____ 16. **Verify settings**
_____ 17. Type **0** to install AIX with current settings
**Installation will take approximately 20 minutes*

Basic System Configuration:

_____ 18. Set **Terminal Type** (*model # on monitor*) *deja vu!*
**You should now be at the Installation Assistant Menu*
_____ 19. Choose **Set Time and Date**
_____ 20. Choose **Change/Show Date and Time**
_____ 21. **Set current date and time** (use arrow keys to move through fields)
_____ 22. Press <**F3> twice** to return to Set Date and Time Menu
_____ 23. Choose **Change Time Zone Using System Default Values**
_____ 24. Choose **Yes for Daylight Savings Time**
_____ 25. Choose **your time zone**
_____ 26. Leave **all five options blank** for US DST default settings
_____ 27. Press <**F3> twice** to return to main Installation Assistant Menu
_____ 28. Choose **Set Root Password**
_____ 29. **Type and confirm pasword**

Network Configuration :

_____ 30. Choose **Configure Network Communications**
_____ 31. Choose **Further Configuration**
_____ 32. Choose **Hostname**
_____ 33. Choose **Set the Hostname**
_____ 34. Type in **Your_Hostname**
_____ 35. Choose **Network Interfaces**
_____ 36. Choose **Network Interface Selection**
_____ 37. Choose **Change/Show Characteristics of a Network Interface**
_____ 38. Choose **en0 Standard Ethernet Network Interface** *(on-board NIC)*
_____ 39. Type **host IP address and Subnet Mask** *(current state=down/use ARP=yes)*
_____ 40. Press <**F3> four times** to return to Further Configuration Menu
_____ 41. Choose **Name Resolution**
_____ 42. Choose **Domain Nameserver**

_____ 43. Choose **Start Using the Nameserver**
_____ 44. Choose **Create a New /etc/resolv.conf** File
_____ 45. Type **Primary DNS Server IP address** and **Domain Name**
_____ 46. Press <**F3> three times**
**If you are not adding a secondary DNS server skip to #50*
_____ 47. Choose **Add a Nameserver**
_____ 48. Type **IP address for secondary nameserver**
_____ 49. Press <**F3> four times** to return to main Installation Assistant Menu
_____ 50. Choose **Manage System Storage and Paging Space** (rootvg)
_____ 51. Choose **Add/Show Paging Space**
_____ 52. **Increase NEW paging space to 528MB** (real memory +16MB) **if real memory is less than 32MB you would increase paging space to 2X real memory*
_____ 53. Press <**F3> three** times to return to main menu
_____ 54. Choose **Tasks Completed – Exit to AIX Login**

Set Power-On and Privileged-Access Passwords

The power-on and privileged-access passwords are security features that help protect the information on a PCI RISC System/6000. Once set the power-on password is required to power on or start the system. Setting this password protects against an unauthorized break-in via a system reset or bootable media. The privileged-access password protects against the unauthorized starting of System Management Services (SMS). SMS is built-in firmware that provides system management tools that include setting or resetting power-on/privileged-access passwords. Your server will arrive with the power-on password enabled but unset, the privileged-access password is disabled by default. To set these passwords you must first change the jumper that controls the privileged-access password then go into the SMS program. Refer to the *Installing and Removing Options* chapter in your user guide for specific privileged-access password jumper setting information.

_____ 1. **/usr/sbin/shutdown –F** to bring down the server
_____ 2. **Turn-off server**, **remove power cable and cover**
_____ 3. Make appropriate **jumper setting changes**
_____ 4. **Replace cover**, **plug-in** and **power on** the server
_____ 5. Press <**F1> or 1** between keyboard and speaker icon – ***timing is everything, i****f you miss it you will have to reboot and try again! *Press* <**F4>** on *graphic displays*
_____ 6. Type **3**, Utilities
_____ 7. Type **1**, Set Passwords and Unattended Start Mode
_____ 8. Type **1**, Set Power On Password
_____ 9. **Select and confirm password**, up to eight characters (A-Z, a-z, and 0-9)
_____ 10. Type **4**, Set Privileged Access Password
_____ 11. **Select and confirm password**, up to eight characters (A-Z, a-z, and 0-9)
_____ 12. Continue typing **x** until you are out of the SMS program

NOTE: Both of these passwords are recommended for security reasons but *you must be careful.* If you forget the power-on password it can be removed and then re-added in the SMS program

providing you haven't lost power or rebooted. If you forget the privileged-access password you will have to power down the server and remove the NVRAM battery for at least 30 seconds; some models may require that they be returned to IBM for service!

Install bos.data and bos.txt.spell

Installation of these two base-level filesets will enable the use of a dictionary file for the local password policy. You will notice that eight filesets will actually be installed during this process due to dependencies/prerequisites. The additional six filesets are: bos.msg.en_US.txt.tfs, printers.msg.en_US.rte, bos.txt.spell.data, bos.txt.tfs, bos.txt.tfs.data, and printers.rte. This information will be displayed during the installation process.

_____ 1. Insert **Volume 1** of installation media in the **CD-ROM** drive
_____ 2. **/usr/bin/smit install**
_____ 3. Select **Install and Update Software**
_____ 4. Select **Install and Update from LATEST Available Software**
_____ 5. Press <**F4>** then select **/dev/cd0** as input device
_____ 6. Press <**F4>** to pull up a list of available software
_____ 7. Type **/bos.data** then <**ENTER>**
_____ 8. Press <**F7>** to select
_____ 9. Type **/bos.txt.spell** then <**ENTER>**
_____10. Press <**F7>** to select (*may display as Writer's Tools Commands*)
_____11. **Accept** remaining **defaults**
_____12. Press <**ENTER> twice** to install
_____13. Insert **Volume 2** when prompted then press <**ENTER**>
_____14. Insert **Volume 3** when prompted then press <**ENTER>**
_____15. Press <**F10>** to exit once installation is complete

Installation Summary

Name	Level	Part	Event	Result
ipfx.msg.en_US.rte	2.2.0.0	USR	APPLY	SUCCESS
bos.data	4.3.0.0	SHARE	APPLY	SUCCESS
ifor_ls.msg.en_US.compat.gu	4.3.2.0	USR	APPLY	SUCCESS
ifor_ls.msg.en_US.compat.cl	4.3.2.0	USR	APPLY	SUCCESS
ifor_ls.msg.en_US.base.gui	4.3.3.0	USR	APPLY	SUCCESS
bos.txt.spell	4.3.3.0	SHARE	APPLY	SUCCESS

Install AIX System Backup and Recovery/6000 (Sysback)

Prior to system customization it is a good idea to perform a backup, this will ease the pain of backing out of any changes that don't go quite as smoothly as you may have liked. Sysback is a menu-driven application that provides system administrators with a simple, efficient way to backup data and recover from hardware failures. A nice feature with this product is that it is flexible enough to allow a system backup created on one system to be installed (or reinstalled) onto another system with either an identical or dissimilar hardware configuration. *This is*

product does not come standard with the OS, if you are unable to purchase Sysback refer to the appendix for instructions on using mksysb as an alternative.

_____ 1. Place the **AIX Sysback/6000 Installation Diskette** into the floppy drive
_____ 2. **/usr/sbin/installp –ac all**

Installation Summary

Name	Level	Part	Event	Result
sysback.rte	4.2.1.30	USR	APPLY	SUCCESS

Perform Initial System Backup

Now that Sysback has been successfully installed we can perform a system backup prior to customizing the system. This backup can be used as a starting base for all future secure AIX system installations and will also allow us to back out of any changes that may have adverse effects on the system. This particular system will be using an enterprise backup solution once installed on the network and for that reason there are no tape drives installed. For our purposes we will backup the system to a file.

_____ 1. **/usr/bin/smit sysback**
_____ 2. Select **Backup & Recover Options**
_____ 3. Select **Backup Options**
_____ 4. Select **Backup the System** (Installation Image)
**Since there are no backup devices defined the only option given is to backup to an image directory*
_____ 5. <**ENTER>** to select "Dir /usr/lpp/sysback/images/local"
_____ 6. Change **Backup file ID** to **OrigSysConf**
_____ 7. Press <**TAB> twice** to change **Report output** type to **errors only**
_____ 8. Press <**TAB>** to change **Include non-JFS** logical volumes to **no**
_____ 9. Type **Fresh Install Backup** in the **User description**
_____ 10. Press <**TAB>** to change **Host read** permission to **same host only**
_____ 11. Press <**TAB>** to change **User read** permission to **same user only** (root)
_____ 12. **Accept remaining defaults**
_____ 13. **<ENTER>** to start backup
***If the backup errors because it ran out of space refer to the appendix for instruction on expanding a Journaled Filesystem*

System Customization:

Backup copy of system files

Backup the following files prior to modification. Place them in root for now just incase you have to boot the system with your installation cd (*rootvg is the only place you can go!*)

_____ 1. **/usr/bin/mkdir /origsysfiles**
_____ 2. **/usr/bin/cp [path/file] /origsysfiles**
/etc/security/.profile /etc/ rc.net

/etc/environment	/etc/rc.nfs
/etc/inetd.conf	/etc/rc.tcpip
/etc/inittab	/etc/security/login.cfg
/etc/motd	/etc/security/sysck.cfg
/etc/netsvc.conf	/etc/security/user
/etc/profile	/etc/sendmail.cf

Remove unnecessary entries from /etc/inittab

The following default entries are good candidates for removal since they are usually not required. Removing the entries from /etc/inittab will disable them from automatically starting. We will also alter the permissions and rename the executables to further disable the services.

_____ 1. **/usr/sbin/rmitab httpdlite writesrv uprintfd pmd rcnfs**
_____ 2. **/usr/sbin/shutdown -Fr** (Reboot the system to confirm changes)
_____ 3. **/usr/bin/cd /usr/bin**
_____ 4. **/usr/bin/chmod 0000 httpdlite pmd**
_____ 5. **/usr/bin/mv pmd Xpmd**
_____ 6. **/usr/bin/mv /usr/IMNSearch/httpdlite /usr/IMNSearch/Xhttpdlite**
_____ 7. **/usr/bin/cd /usr/sbin**
_____ 8. **/usr/bin/chmod 0000 writesrv uprintfd nfsd**
_____ 9. **/usr/bin/mv writesrv Xwritesrv**
_____10. **/usr/bin/mv uprintfd Xuprintfd**
_____11. **/usr/bin/mv nfsd Xnfsd**

Remove unnecessary services from /etc/inetd.conf

There are many services included in inetd that are unnecessary. For maximum security you should not have any services running that are not necessary for operation. IBM recommends that you comment out services in inetd but that makes it too easy for a hacker to change. For that reason we will completely delete the services from inetd and also rename and change the permissions on the executables called by these services.

_____ 1. **/usr/bin/vi /etc/inetd.conf**
_____ 2. **Remove** the following entries: **shell**, **login**, **kshell, klogin, exec, rstatd, rusersd, rwalld, rquotad, comsat, uucp, bootps, tftp, finger, systat, netstat, talk, ntalk, rexd, sprayd, pcnfsd, echo, chargen, time, daytime, discard, ttdbserver, dtspc, cmsd, imap2, pop3**
_____ 3. **/usr/bin/refresh –s inetd**
_____ 4. **/usr/bin/cd /usr/sbin**
_____ 5. **/usr/bin/chmod 0000 rshd krshd rlogind krlogind rexecd comsat bootpd fingerd tftpd talkd rpc.rquotad rpc.rexd rpc.rstatd rpc.pcnfsd**
_____ 6. **/usr/bin/mv rshd Xrshd *** *repeat for all in #6*
_____ 7. **/usr/bin/cd /usr/lib/netsvc**
_____ 8. **/usr/bin/chmod 0000 rusers/rpc.rusersd rwall/rpc.rwalld spray/rpc.sprayd**
_____ 9. **/usr/bin/mv rusers/rpc.rusersd rusers/Xrpc.rusersd**
_____ 10. **/usr/bin/mv rwall/rpc.rwalld rwall/Xrpc.rwalld**
_____ 11. **/usr/bin/mv spray/rpc.sprayd spray/Xrpc.sprayd**

Remove unnecessary services from /etc/rc.tcpip

As with inetd there are several unnecessary and vulnerable services within the rc.tcpip startup script. Once again we will remove them, then change permissions and rename the associated binaries.

_____ 1. **/usr/bin/vi /etc/rc.tcpip**
_____ 2. **Remove: dhcpcd autoconf6 ndpd-host ndpd-router routed gated portmap named timed rwhod snmpd dhcpsd dhcprd dpid2 mrouted**
_____ 3. **Add –s** to the end of the **syslog** entry *(suppress logging for remote hosts)*
_____ 4. **/usr/bin/cd /usr/sbin**
_____ 5. **/usr/bin/chmod 0000 dhcpcd autoconf6 ndpd-host ndpd-router portmap rwhod snmpd dpid2**
_____ 6. **/usr/bin/mv dhcpcd Xdhcpcd** ***repeat for all in #5**
_____ 7. **/etc/tcp.clean** to commit changes

Rename startup scripts for dangerous services

Rename and change permissions on vulnerable startup scripts**.**

_____ 1. **/usr/bin/cd /etc**
_____ 2. **/usr/bin/chmod 0000 rc.net.serial rc.nfs**
_____ 3. **/usr/bin/mv rc.net.serial Xrc.net.serial**
_____ 4. **/usr/bin/mv rc.nfs Xrc.nfs**

Tighten Sendmail Configuration

Sendmail is the default SMTP server software for AIX. The version of sendmail included with AIX 4.3.3 is version 8.9.3, the following steps will further secure the program. Be sure to check www.sendmail.org for the latest sendmail security information as well as additional methods for securing it.

_____ 1. **/usr/bin/vi /etc/sendmail.cf**
_____ 2. Make the following changes:
set **PrivacyOptions=goaway,restrictmailq,restrictqrun**
set **SmtpGreetingMessage=$j Sendmail; $b**
set **SafeFileEnvironment=/**
_____ 3. **/usr/sbin/sendmail –v –bi** (verify configuration changes)

Set Network Options with "no" command

Network options control how TCP, UDP, and ICMP behave on an AIX machine. Many of the default settings are insufficient for the Internet World. Use the **no –a** command to display the current network options. The **no** command only operates on the currently running kernel so we'll have to add the following entry to /etc/rc.net to make the changes permanent.

_____ 1. **/usr/bin/vi /etc/rc.net**
_____ 2. **Add** the following **to** the **end** of the file:

```
############################################################
# Additional security network options.
############################################################
```

```
if [ -f /usr/sbin/no ] ; then
        /usr/sbin/no –o clean_partial_conns=1#SYN attack protection
        /usr/sbin/no –o directed_broadcast=0 # directed packets can't
                                             reach broadcast address
        /usr/sbin/no –o ipignoreredirects=1    #prevent source routing
        /usr/sbin/no –o ipsendredirects=0
        /usr/sbin/no –o ipsrcroutesend=0
        /usr/sbin/no –o ipsrcrouteforward=0
        /usr/sbin/no –o ip6srcrouteforward=0
        /usr/sbin/no –o tcp_pmtu_discover=0
        /usr/sbin/no –o udp_pmtu_discover=0
    fi
```

_____ 3. **/usr/sbin/shutdown –Fr**
_____ 4. **/usr/sbin/no –a** (verify changes)

Remove Unnecessary Default Accounts/Groups

Remove the following default accounts and groups. If your server doesn't require print capabilities add the lpd user and printq group to this list.

_____ 1. /**usr/sbin/rmuser uucp imnadm guest**
_____ 2. **/usr/sbin/rmgroup uucp imnadm**

Remove banner from ftp login screen

The standard ftp login banner gives the version number which could be useful to a hacker. The following steps will diminish this information.

_____ 1. **/usr/bin/dspcat –g /usr/lib/nls/msg/en_US/ftpd.cat > /tmp/ftpd.msg**
_____ 2. **/usr/bin/vi /tmp/ftpd.msg**
_____ 3. **change 9** to read "**%s FTP server ready" vs "%s FTP server (%s) ready**"
_____ 4. **/usr/bin/gencat /tmp/ftpd.cat /tmp/ftpd.msg**
_____ 5. **/usr/bin/cp –p /tmp/ftpd.cat /usr/lib/nls/msg/en_US/ftpd.cat**

Restrict access to crontab and at command:

Use configuration files to limit access to root only for these services.

_____ 1. **/usr/bin/touch /var/adm/cron/cron.allow**
_____ 2. **/usr/bin/echo "root" /var/adm/cron/cron.allow**
_____ 3. **/usr/bin/chown root:root /var/adm/cron.allow**
_____ 4. **/usr/bin/chmod 600 /var/adm/cron/cron.allow**
_____ 5. **/usr/bin/touch /var/adm/cron/at.allow**
_____ 6. **/usr/bin/echo "root" /var/adm/cron/at.allow**
_____ 7. **/usr/bin/chown root:root /var/adm/at.allow**
_____ 8. **/usr/bin/chmod 600 /var/adm/cron/at.allow**
_____ 9. **/usr/bin/ps –ef |grep cron**
_____10. **/usr/bin/kill –HUP <PID>**

Set User Attributes

User attributes are set in the */etc/security/user* file on AIX. The settings can be global (default stanza) or individual (user stanza), individual settings override global.

_____ 1. **/usr/bin/vi /etc/security/user**

_____ 2. **add/set the following attributes** to the specified stanza:

DEFAULT

umask = **077** (tightens umask to rw-------)
pwdwarntime = **7** (begins warning 7days prior to pwd expiring)
loginretries = **3** (#failed logins before acct locked)
histexpire = **26** (# weeks before pwd can be reused)
histsize = **8** (#pwd iterations before pwd can be reused)
minage = **1** (min #wks before pwd can be reset)
maxage = **12** (#wks before pwd must be changed)
maxexpired = **2** (max #wks beyond maxage that pwd can be changed)
minalpha = **4** (min# alpha characters)
minother = **1** (min# non-alpha characters)
minlen = **6** (min characters pwd must contain)
mindiff = **3** (min# different characters from old to new pwd)
maxrepeats = **3** (max# repeated characters)
dictionlist = **/usr/share/dict/words** (prevents dictionary word as password)
registry = **files** (acct administered using local files)

ROOT

rlogin = **false**
ttys = **/dev/tty0** (direct root login permitted at console only)
maxage = **5**
minlen = 8

Other attributes

/etc/security/.profile: (root's profile)

_____ 1. **/usr/bin/vi /etc/security/.profile**

_____ 2. remove **/sbin /usr/sbin /usr/bin** and "**.**" from PATH

/etc/security/login.cfg:

_____ 1. **/usr/bin/vi /etc/security/login.cfg**

_____ 2. add **herald = "\r\n\n\n\n\n\n\n\n\ NOTICE TO USERS\r\n\r\nUse of this machine waives all rights to your privacy,\r\n\r\n and is consent to being monitored.\r\n\r\nUnauthorized use prohibited.\r\n\r\n\r\nlogin: "**to default stanza

_____ 3. add **/bin/false** to **usw shells**

_____ 4. **/usr/bin/chsh daemon sys bin adm nobody /bin/false**

/etc/environment:

_____ 1. **/usr/bin/vi /etc/environment**

_____ 2. **remove /sbin, /usr/sbin, /usr/bin** and "**.**" from the end of the **PATH**

_____ 3. add **EDITOR=/usr/bin/vi**

/etc/profile:

_____ 1. **/usr/bin/vi /etc/profile**
_____ 2. uncomment **TMOUT = 600**
_____ 3. uncomment **TIMEOUT = 600**
_____ 4. add **EDITOR=/usr/bin/vi**
_____ 5. add **TMOUT TIMEOUT EDITOR** to export line

/etc/motd:

_____ 1. **/usr/bin/vi /etc/motd**
_____ 2. add login banner "**Use of this machine is consent to being monitored. Unauthorized use is prohibited**."

Create non-root user account

You will need a non-root account for the TCPWrapper and SSH installations. The following fast path will put you into a simple, menu driven interface for adding users. Any attributes left blank will be picked up from those set in /etc/security/user.

_____ 1. **/usr/bin/smit mkuser**
_____ 2. **Set:** username, primary group, home directory, login program and user information
_____ 3. **F10** to exit
_____ 4. **/usr/bin/smit passwd**
_____ 5. Type **username**
_____ 6. **Type and confirm password**

Install TCP Wrappers

TCP Wrappers can be downloaded from the IBM Bull site in installp format eliminating the need for a compiler on the system. Since the server is still not on the network we will download the files from another system and then copy them to removable media.

_____ 1. **Download tcp_wrappers-7.6.1.0.exe** from www-frec.bull.com/cgi-bin/list_dir.cgi/download/out/
_____ 2. **Copy to removable media**
_____ 3. **Login** to server as **root**
_____ 4. **/usr/bin/mkdir /floppy**
_____ 5. **/usr/bin/mkdir /usr/local**
_____ 6. **/usr/sbin/mount /dev/fd0 /floppy**
_____ 7. **/usr/bin/cp /floppy/*.exe /usr/local**
_____ 8. **/usr/bin/chmod 744 /usr/local/tcp_wrappers-7.6.1.0.exe**
_____ 9. **/usr/bin/chown *non-root-user* /usr/local/tcp_wrappers-7.6.1.0.exe**
_____10. **/usr/bin/su *non-root-user***
_____11. **/usr/bin/cd /usr/local**
_____12. **/usr/local/tcp_wrappers-7.6.1.0.exe**
_____13. **/usr/bin/more tcp_wrappers-7.6.1.0.bff.asc** (*annotate the sum hash*)

_____14. **/usr/bin/sum tcp_wrappers-7.6.1.0.bff** (*result should match # in .asc file*)
_____15. **exit** (return to root user)
_____16. **/usr/sbin/installp –acqX –d . freeware.tcp_wrappers.rte**

Installation Summary

Name	Level	Part	Event	Result
freeware.tcp_wrappers.rte	7.6.1.0	USR	APPLY	SUCCESS

_____17. **/usr/bin/rm .toc**

Install OpenSSH2

SSH installation requires four additional filesets due to application prerequisites. SSH and its prerequisites can also be downloaded from the IBM Bull site using a networked computer; the files will then be placed on removable media. ***The egd fileset must be installed first*** because it creates the local socket (/dev/entropy) which must be present for the remaining SSH installation.

_____ 1. **Download** the following installp packages from www-frec.bull.com/cgi-bin/list_dir.cgi/download/out/:
openssh-2.5.1.0.exe
openssl-0.9.6.0.exe
zlib-1.1.3.2.exe
egd-0.8.0.0.exe
perl.md5-2.12.0.0.exe
_____ 2. **Copy to removable media**
_____ 3. **Login** to server as **root**
_____ 4. **/usr/sbin/mount /dev/fd0 /floppy**
_____ 5. **/usr/bin/cp /floppy/*.exe /usr/local**
_____ 6. **/usr/bin/cd /usr/local**
_____ 7. **/usr/bin/chmod 744 *.exe**
_____ 8. **/usr/bin/chown *non-root-user* *.exe**
_____ 9. **su *non-root-user***
_____10. **/usr/local/egd-0.8.0.0.exe** **repeat for all .exe files*
_____11. **/usr/bin/more egd-0.8.0.0.bff.asc**, annotate sum hash ***repeat for all .asc files*
_____12. **/usr/bin/sum egd-0.8.0.0.bff**, result should match .asc ** repeat for all .bff files*
_____13. **exit** (return to root)
_____14. **/usr/sbin/installp –acgX –d . freeware.egd.rte** (*perl.md5 is a prerequisite for egd*)

Installation Summary

Name	Level	Part	Event	Result
freeware.perl.md5.rte	2.12.0.0	USR	APPLY	SUCCESS
freeware.egd.rte	0.8.0.0	USR	APPLY	SUCCESS

freeware.egd.rte	0.8.0.0	ROOT	APPLY	SUCCESS

_____15. **rm .toc**

Create and load the local socket file that will be used to create the necessary SSH DSA keys automatically: **Added to /etc/rc.tcpip during the egd fileset installation*

_____16. **/usr/bin/perl –w /usr/local/bin/egd.pl /dev/entropy**

Install remaining filesets:

_____17. **/usr/sbin/installp –acgX –d . freeware.openssh.rte** (*openssl and zlib are prerequisites*)

Installation Summary

Name	Level	Part	Event	Result
freeware.zlib.rte	1.1.3.2	USR	APPLY	SUCCESS
freeware.openssl.rte	0.9.6.0	USR	APPLY	SUCCESS
freeware.openssl.rte	0.9.6.0	ROOT	APPLY	SUCCESS
freeware.openssh.rte	2.5.1.0	USR	APPLY	SUCCESS
freeware.openssh.rte	2.5.1.0	ROOT	APPLY	SUCCESS

_____18. **rm .toc**

Configure TCP Wrappers

Protect the telnet and ftp programs with TCP Wrappers. Change location of the log file to something other than /var/adm/syslog then lock it down with strict permissions. Configure the TCP Wrapper access control lists to allow/deny access via telnet and ftp.

_____ 1. **/usr/bin/vi inetd.conf**
_____ 2. **Replace /usr/sbin/telnetd** with /usr/local/bin/tcpd
_____ 3. **Replace /usr/sbin/ftpd** with /usr/local/bin/tcpd
_____ 4. **/usr/bin/refresh –s inetd**
_____ 5. **/usr/bin/vi /etc/syslog.conf**
_____ 6. **Change mail.debug** to /var/adm/tcp_wrapper.log
_____ 7. **/usr/bin/touch /var/adm/tcp_wrapper.log**
_____ 8. **/usr/bin/chmod 600 /var/adm/tcp_wrapper.log**
_____ 9. **/usr/bin/refresh –s syslogd**
_____10. **/usr/bin/touch /etc/hosts.allow**
_____11. **/usr/bin/chown root:root /etc/hosts.allow**
_____12. **/usr/bin/chmod 600 /etc/hosts.allow**
_____13. **/usr/bin/echo "ssh : ALL : allow" > /etc/hosts.allow**
_____14. **/usr/bin/touch /etc/hosts.deny**
_____15. **/usr/bin/chown root:root /etc/hosts.deny**
_____16. **/usr/bin/chmod 600 /etc/hosts.deny**
_____17. **/usr/bin/echo "ALL : ALL : deny" > /etc/hosts.deny**

**Refer to man/man5/hosts_access.5 for more examples*

Configure OpenSSH2/Reconfigure sshd

The OpenSSH client is set up to support both SSH1 and SSH2 by default; however, the OpenSSH server daemon (sshd) is only configured for SSH1. The following steps will reconfigure sshd to support SSH2. */etc/rc.openssh was created during OpenSSH installation then added to /etc/inittab, the daemon will start automatically during the next system startup*.

_____ 1. **/usr/bin/cd /etc/openssh**
_____ 2. **/usr/bin/mv ssh_host_key ssh_host_key.orig**
_____ 3. **/usr/bin/mv ssh_host_key.pub ssh_host_key.pub.orig**
_____ 4. **/usr/bin/vi sshd_config**
_____ 5. **Uncomment Protocol 2,1**
_____ 6. **kill `cat /var/openssh/sshd.pid`**
_____ 7. **/usr/local/bin/opensshd –f /etc/openssh/sshd_config –Q**
**there will be errors regarding ssh_host_key, this is normal*

.

Configure Trusted Computing Base (TCB)

The TCB is responsible for enforcing the information security policies of the system. It consists of the kernel, configuration files that control system operation, and any program that is run with the privilege or access rights to alter the kernel or configuration files. The TCB contains the following trusted programs: all setuid root programs, all setgid to admin group(s) programs, any program exclusively run by root or a member of the system group, and any program that must be run by the administrator while on the trusted communication path. This is also the time to add all of the previously locked down services and files to the TCB.

_____ 1. **/usr/bin/vi /etc/security/login.cfg**
_____ 2. **Add sak_enabled = true** to /dev/tty0 stanza
_____ 3. **/usr/bin/vi /etc/security/user**
_____ 4. **Add tpath = on** to root stanza
_____ 5. **Add tpath = notsh** to default stanza

Add all "locked down" binaries and files to the TCB:

_____ 6. **/usr/sbin/chtcb on [path] [command/file]**

/usr/sbin:

Xdhcpd	Xautoconf6	Xndpd-host	Xndpd-router	Xrouted	Xrshd
Xgated	Xportmap	Xnamed	Xtimed	Xdpid2	
Xrpc.rstatd					
Xrwhod	Xsnmpd	Xdhcpsd	Xdhcprd	Xmrouted	Xbootpd
Xkrshd	Xrlogind	Xkrlogind	Xrexecd	Xcomsat	
Xfingerd	Xtftpd	Xtalkd	Xrpc.rquotad	Xrpc.rexd	
Xwritesrv	Xrpc.pcnfsd	Xuprintfd	Xnfsd		

/usr/bin:

Xpmd	ls

***/etc**:*
Xrc.net.serial Xrc.nfs rc.net inetd.conf inittab sendmail.cf
hosts.allow hosts.deny motd profile

***/etc/security**:*
.profile login.cfg users

***/etc/openssh**:*
sshd_config ssh_known_hosts ssh_config

***/usr/lib/netsvc**: *commands are in sub-directories*
rusers/Xrpc.rusersd rwall/Xrpc.rwalld spray/Xrpc.sprayd

***/usr/lib/nls/msg/en_US**:*
ftpd.cat

***/usr/IMNSearch**:*
Xhttpdlite

/var/adm/cron:
cron.allow at.allow

_____ 7. **/usr/bin/ls –le [directory]** *verify all above command were added to the TCB, should have a **"+" in the 11th perm bit***
_____ 8. **/usr/sbin/tcbck –y ALL**
_____ 9. **Download copy of /etc/sysck.cfg to removable media**, write protect it and store in a safe place **this copy will be used to run sanity checks against all TCB files, any time*
changes are made to the system you will need to make a new copy of sysck.cfg

Configure xntpd

For our purposes we will configure the system as an NTP client with an existing, in-house NTP server and two external secondary servers.

_____ 1. **Get hostname** of in-house NTP server
_____ 2. **Go to** www.eeics.udel.edu/~mills/ntp/servers.htm from a networked computer
_____ 3. **Find two additional NTP servers** and annotate their administrator's information
_____ 4. **Contact administrator for each** NTP server and request permission to connect

Once you have permission add each server to /etc/ntp.conf in the form *server FQDN version 3*

_____ 5. **/usr/bin/vi /etc/ntp.conf**
_____ 6. **Comment out broadcastclient entry**
_____ 7. **Add three NTP server entries**
_____ 8. **/usr/bin/startsrc –s xntpd**

Remove copy of "backup" system files

Prior to customizing the system we made a backup copy of several system files and moved them to a directory on the root volume group for "backing out" purposes; it is now safe to remove these.

_____ 1. **/usr/bin/rm –r /origsysfiles**

Testing:

Place the server on the network. Verify connectivity and ensure results of the following checks match the restrictions imposed by this checklist. If any of these tests should fail take the server off-line immediately.

_____ 1. Power-On Password required for reboot
_____ 2. Power-On Password required for boot from media
_____ 3. Privileged-Access password required for SMS access
_____ 4. No direct root logins allowed other than at console
_____ 5. Correct "message of the day" is displayed upon login
_____ 6. Absolute path required for execution of all binaries
_____ 7. Can SSH out
_____ 8. Can SSH in
_____ 9. Cannot telnet/ftp/rlogin/rsh in
_____10. Can sendmail out
_____11. Can receive inbound mail
_____12. Cannot set password to dictionary words
_____13. Only root is allowed to schedule cron and at jobs
_____14. Scan with IDT of your choice

Customized Backup

Now that the system has been locked down we should perform another backup prior to installing the application. Once again we will backup the system to a file, refer to steps on page 5 of this checklist. (***Backup File ID=CustSysConf***; ***User Description=Customized System Backup***)
**Use mksysb if sysback was not purchased*

_____ **1.** Perform Customized System Backup

Appendix:

SMIT Menus:

Much of the system installation and configuration is done within the System Management Interface Toot (SMIT). Menus can be reached via "fastpaths" (smit mkuser) or by typing "smit" and using conventional menu navigation. (All examples in this checklist make use of fastpaths) Depending on your console these menus will either display graphically (point-and-click) or ASCII-based (up/down arrow keys/Function keys). At the bottom of each menu screen are self-explanatory function keys. A "#" indicates that SMIT is expecting a number as input, a "+" indicates a drop down menu is present and can be accessed by pressing <F4>. A SMIT "OK"

prompt will indicate the successful completion of a process.

Editing Boot Sequence (SMS):

To edit the boot sequence you must go into the System Management Services (SMS) section.

_____ 1. **/usr/sbin/shutdown –Fr** to reboot
_____ 2. Press **F4** (*graphic*), **F1 or 1** (*ascii) ***between the keyboard and speaker icon***
_____ 3. Choose **2**, Multiboo**t**
_____ 4. Choose **4**, Select Boot Devices
_____ 5. Choose **3**, Configure 1st Boot Device
_____ 6. Select **CD-ROM** (displays current boot sequence) then type **x** to exit
_____ 7. Choose **4**, Configure 2nd Boot Device
_____ 8. Select **Hard Disk**, ie hdisk0 (displays current boot sequence) type **x** to exit
_____ 9. Continue typing **x** until you are completely out of the SMS section, system will now reboot

Expanding a Journaled File System:

AIX provides you with the ability to increase the size of a file system dynamically provided you have enough free space available on your disk.

_____ 1. **/usr/bin/smit chfs**
_____ 2. Select **Change/Show Characteristics of a Journaled File System**
_____ 3. **Highlight filesystem** then **enter** to select
_____ 4. **Enter the new file system size** that you calculated in *512-byte blocks*
_____ 5. **Enter**

Backup using mksysb:

mksysb comes standard with AIX 4.3.3 and is part of the bos.sysmgt package. mksysb can be used to backup rootvg. It will create a bootable system image on either tape or cd, it can also save the image to disk. For our purposes we will choose the latter since we do not have a tape drive or writeable cd-rom drive installed on the system.

_____ 1. **/usr/bin/smit mksysb**
_____ 2. **Add path/filename** to Backup DEVICE or FILE
_____ 3. **<ENTER>**

Snapshot of SMIT mksysb menu

Back Up the System

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

WARNING: Execution of the mksysb command will result in the loss of all material previously stored on the selected output medium. This command backs up only rootvg volume group.

*Backup DEVICE or FILE	[**/usr/init_backup**]	+/
Create MAP files?	no	+
EXCLUDE files?	no	+
List files as they are backed up?	no	+
Generate new /image.data file?	yes	+
EXPAND /tmp if needed?	no	+
Disable software packing of backup?	no	+
Number of BLOCKS to write in a single output (Leave blank to use a system default)	[ ]	#

F1=Help F2=Refresh F3=Cancel F4=List
F5=Reset F6=Command F7=Edit F8=Image
F9=Shell F10=Exit Enter=Do

Command: **OK** stdout: yes stderr: no
Before command completion, additional instructions may appear below.

Creating information file (/image.data) for rootvg..
0512-039 mksysb: WARNING: /usr/init_backup does not appear to be a tape device and will NOT have a bootable image.

Creating list of files to back up.
Backing up 13483 files.....

0512-038 mksysb: Backup Completed Successfully.
0512-040 mksysb: WARNING: /usr/init_backup does not appear to be a tape device and does NOT have a bootable image.

References:

AIX Support Family, AIX System Backup & Recovery/6000 Version 4 (User Reference Manual), Second Edition, IBM Global Services, April 1998

Farazdel, Abbas, Additional Security Tools on IBM e-server pSeries, IBM RS/6000, and SP/Cluster, Fatbrain, December 2000

Garfinken, Simson & Spafford, Gene, Practical UNIX and Internet Security, Second Edition, Sebastopol: O'Reilly and Associates, Inc., 1996

IBM Learning Services, AIX Ver. 4 System Administration (Student Notebook), IBM Global Services, December 1999

IBM Education and Training, AIX V4 Advanced System Administration (Student Notebook), IBM Global Services, June 1998

Siegert, Andreas, The AIX Survival Guide, Reading: Addison Wesley Longman, Inc., 1999

Yashimichi, Kosuge, AIX 4.3 Elements of Security Effective and Efficient Implementation, Fatbrain, August 2000

Last Updated: May 25th, 2017

Upcoming Training

SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**