

AIX Certification Checklist

Introduction:

This guide contains procedures that follow best practices in the security industry. Follow these steps to secure an AIX machine. These steps will help prevent threat agents from exploiting known vulnerabilities.

Procedure:

- Check for most recent updates that will need to be performed subsequent to installation.
 - Run `oslevel -r` to determine your maintenance level
 - Go to <http://techsupport.services.ibm.com/server/criticalfixes3/criticalfixes.html> and select your package
 - If your level is greater than what is listed on the site, there are no critical patches for your system at this time
- Install security patches retrieved before continuing.
- Check the Trusted Computing Base of the machine:
 - Use the `tcbck` command to check the security level of elements of the system: `tcbck -y ALL`
 - This causes the `tcbck` command to check the installation of each file in the `tcbck` database described by the `/etc/security/sysck.cfg` file.
 - Check the integrity of the file system tree with the `tchck` command: `tcbck -t tree`
 - Do **not** run `tcbck -y tree`. This will delete and disable devices that are not properly listed in the TCB and might disable your system.
- Set up login controls in the `/etc/security/login.cfg` file as follows:

Attribute	Applies to PtYs (Network)	Applies to TTYs	Recommended Value	Comments
sak_enabled	Y	Y	False	The Secure Attention key is rarely needed
logintimes	N	Y		Specify allowed login times here
logindisable	N	Y	4	Disable login on this terminal after 4 consecutive failed attempts
logininterval	N	Y	60	Terminal will be disabled when the specified invalid attempts have been made within 60 seconds
loginreenable	N	Y	30	Re-enable the terminal after it was automatically disabled after 30 minutes
logindelay	Y	Y	5	The time in seconds between login prompts. This will be multiplied with the number of failed attempts; for example, 5,10,15,20 seconds when 5 is the initial value

- For network logins, use explicit entries such as:

```
/dev/tty0:
    logintimes = 0600-2200
    logindisable = 5
    logininterval = 80
    loginreenable = 20
```
- Edit the `herald` parameter in the `/etc/security/login.cfg` file to something like:

```
Unauthorized use of this system is prohibited\n\nlogin:
```
- Edit the `/etc/security/.profile` file to enforce automatic logout with an entry such as:

```
TMOUT=600 ; TIMEOUT=600 ; export readonly TMOUT TIMEOUT
```
- Remove the `/etc/rc.dt` file
- Remove the `xwd` and `xwud` executables
- Unless “r” commands (i.e., `rsh`, `rlogin`) are required, remove or empty the file `/etc/hosts.equiv`.
- If “r” commands are required, consider replacing them with a secure alternative such as SSH.
- Configure `tcp_wrappers` in `/etc/inetd.conf` to provide greater access and logging on enabled services if using the `inetd` daemon.



- ❑ Edit /etc/hosts.allow to include this entry as the first uncommented line AFTER any configuration lines allowing connections for any specific services required: ALL:ALL:deny
- ❑ Edit /etc/hosts.deny to include this entry as the first uncommented line in the file: ALL:ALL
- ❑ After restarting the machine, check for running network services by issuing the command netstat -af inet. Ensure that only required services are running and listening for connections. This helps in preventing security compromises on possibly unknown and unpatched services.
- ❑ Restrict execution of xhost command to root-user authority only (chmod 744 /usr/bin/X11/xhost)
- ❑ Make sure the user root is the only user with a UID of 0
- ❑ Disable unnecessary default user and group IDs. Examples of users and groups that are unnecessary follow:
 - Unnecessary Users:
 - Uucp, nuucp
 - Lpd
 - Imnadm
 - Guest
 - Unnecessary Groups:
 - Uucp
 - Printq
 - Imnadm
- ❑ .netrc files contain usernames and passwords. Delete these files if you find them:
 - # find `awk -F: '{print \$6}' /etc/passwd` -name .netrc -ls
- ❑ Edit the /etc/security/users file to enable password checking (to enforce good passwords). This file is also where you can establish that root cannot log in remotely.
 - See http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm for details on this file
- ❑ Ensure that the file /etc/ftpusers or /etc/ftpd/ftpusers contains the names of all system accounts, as well as root.
- ❑ Prevent lpd and syslogd from listening for network connections if possible. Exercise caution to ensure outbound connections are still allowed, if required for your system configuration. This may be accomplished with command-line arguments and/or tcp_wrappers -- refer to your system's info or man pages.
- ❑ Clear /etc/hosts.lpd if not required. If the host is a print server, ensure that only fully qualified domain names are specified i.e., hostname.domainname.
- ❑ Ensure that passwords have been set and are strong for all users (crack).
- ❑ Ensure that openssl libraries are up to date "openssl version."
- ❑ Ensure that sudo is installed, configured and logging (visudo works).

Network Services

- ❑ Secure TCP/IP services. On AIX, the securetcip command will remove the following commands:
 - rlogin and rlogind
 - rcp, rsh, and rshd
 - tftp and tftpd
 - trpt
- ❑ Verify the /etc/security/services file – any service listed here is exempt from system ACLs.
- ❑ If the following two lines are in the /etc/services file, remove them:
 - sco_printer 7000/tcp sco_spooler # For System V print IPC
 - sco_s5_port 7001/tcp lpNet_s5_port # For future use
- ❑ Verify that packet forwarding has been disabled: /usr/sbin/no -o ipforwarding=0
- ❑ Verify that source routing is off: /usr/sbin/no -o nonlocsrcroute=0
- ❑ Verify that ntp (xntp) is running, configured, and starts on boot (/etc/rc.tcpip).
- ❑ Verify that sshd starts on boot (/etc/rc.d/rc2.d).
- ❑ Disable unneeded services from /etc/inetd.conf, /etc/inittab, /etc/rc.nfs, /etc/rc.tcpip

Service	Daemon	Started by	Function	Comments
inetd/bootps	Inetd	/etc/inetd.conf	Bootp services for diskless clients	Disable
inetd/chargen	Inetd	/etc/inetd.conf	Character generator	Disable
inetd/cmsd	Inetd	/etc/inetd.conf	Calendar service (as used by CDE)	Disable
inetd/comsat	Inetd	/etc/inetd.conf	Notifies incoming electronic mail	Disable
inetd/daytime	Inetd	/etc/inetd.conf	Obsolete time service (testing only)	Disable
inetd/discard	Inetd	/etc/inetd.conf	/dev/null service (testing only)	Disable
inetd/dtspc	Inetd	/etc/inetd.conf	CDE Subprocess Control	Disable



inetd/echo	Inetd	/etc/inetd.conf	Echo service (testing only)	Disable
inetd/exec	Inetd	/etc/inetd.conf	Remote execution service	Disable
inetd/finger	Inetd	/etc/inetd.conf	Finger peeking at users	Disable
inetd/ftp	Inetd	/etc/inetd.conf	File transfer protocol	Disable and use a secure protocol
inetd/imap2	Inetd	/etc/inetd.conf	Internet Mail Access Protocol	Disable unless you are running a mail server
inetd/klogin	Inetd	/etc/inetd.conf	Kerberos login	Disable unless your site uses Kerberos authentication
inetd/kshell	Inetd	/etc/inetd.conf	Kerberos shell	Disable unless your site uses Kerberos authentication
inetd/login	Inetd	/etc/inetd.conf	rlogin service	Disable and use ssh
inetd/netstat	Inetd	/etc/inetd.conf	Reporting of current network status	Disable
inetd/ntalk	Inetd	/etc/inetd.conf	Allows users to talk with each other	Disable
inetd/pcnfsd	Inetd	/etc/inetd.conf	PC NFS file services	Disable If you need a service similar to this, consider Samba, as the pcnfsd daemon predates Microsoft's release of SMB specifications
inetd/pop3	Inetd	/etc/inetd.conf	Post Office Protocol	Disable and use POP3s
inetd/rexd	Inetd	/etc/inetd.conf	Remote execution	Disable
inetd/quotad	Inetd	/etc/inetd.conf	Reports on file quotas (for NFS clients)	Disable
inetd/rstatd	Inetd	/etc/inetd.conf	Kernel statistics server	Disable
inetd/rusersd	Inetd	/etc/inetd.conf	Info about users logged in	Disable
inetd/rwalld	Inetd	/etc/inetd.conf	Write to all users	Disable
inetd/shell	Inetd	/etc/inetd.conf	Rsh service	Disable and use ssh
inetd/sprayd	Inetd	/etc/inetd.conf	RPC spray tests	Disable
inetd/systat	Inetd	/etc/inetd.conf	"ps - ef" status report	Disable
inetd/talk	Inetd	/etc/inetd.conf	Establish split screen between 2 users on the net	Disable
inetd/ntalk	Inetd	/etc/inetd.conf	"new talk" establish split screen between 2 users on the net	Disable
inetd/telnet	Inetd	/etc/inetd.conf	telnet service	Disable and use ssh
inetd/tftp	Inetd	/etc/inetd.conf	Trivial file transfer protocol	Disable
inetd/time	Inetd	/etc/inetd.conf	Obsolete time service	Disable and use ntpdate
inetd/ttdbserver	Inetd	/etc/inetd.conf	Tool-talk database server (for CDE)	Disable
inetd/uucp	Inetd	/etc/inetd.conf	UUCP network	Disable
inittab/dt	Init	/etc/rc.dt script in the /etc/inittab	Desktop login to CDE environment	Disable
inittab/dt_nogb	Init	/etc/inittab	Desktop login to CDE environment (NO graphic boot)	Disable
inittab/httpd-lite	Init	/etc/inittab	Web server for the docsearch command	Disable
inittab/i4ls	Init	/etc/inittab	License manager servers	Disable on production machines
inittab/imnss	Init	/etc/inittab	Search engine for the docsearch command	Disable
inittab/imqss	Init	/etc/inittab	Search engine for docsearch	Disable
inittab/lpd	Init	/etc/inittab	BSD line printer interface	Disable
inittab/nfs	Init	/etc/inittab	Network File System/Net Information Services	Disable unless using NFS
inittab/piobe	Init	/etc/inittab	Printer IO Back end	Disable if using a print server
inittab/qdaemon	Init	/etc/inittab	Queue daemon (for printing)	Disable if using a print server
inittab/uprintfd	Init	/etc/inittab	Kernel messages	Disable



inittab/writesrv	Init	/etc/inittab	Writing notes to ttys	Disable on servers, enable on workstations
inittab/xdm	Init	/etc/inittab	Traditional X11 display management	Disable on servers, enable on workstations
rc.nfs/automountd		/etc/rc.nfs	Automatic file systems	Disable on servers, enable on workstations using NFS
rc.nfs/biod		/etc/rc.nfs	Block IO daemon (required for NFS server)	If not an NFS server, then disable this along with nfsd and rpc.mountd
rc.nfs/keyserv		/etc/rc.nfs	Secure RPC key server	Disable this if you are not using NFS and NIS and NIS+
rc.nfs/nfsd		/etc/rc.nfs	NFS Services (required for NFS Server)	Enable if on NFS file servers If you disable this, then disable biod, nfsd, and rpc.mountd as well
rc.nfs/rpc.lockd		/etc/rc.nfs	NFS file locks	Disable if you are not using NFS
rc.nfs/rpc.mountd		/etc/rc.nfs	NFS file mounts (required for NFS server)	Should be enabled only on NFS file servers If you disable this, then disable biod and nfsd as well
rc.nfs/rpc.statd		/etc/rc.nfs	NFS file locks (to recover them)	Disable unless you are using NFS
rc.nfs/rpc.yppasswdd		/etc/rc.nfs	NIS password daemon (for NIS master)	Only required when the machine in question is the NIS master; disable in all other cases
rc.nfs/ypupdate		/etc/rc.nfs	NIS update daemon (for NIS slave)	Only required when the machine in question is a NIS slave to a Master NIS Server
rc.tcpip/autoconf6		/etc/rc.tcpip	IPv6 interfaces	Disable unless you are running IPV6
rc.tcpip/dhccpd		/etc/rc.tcpip	Dynamic host configure protocol (client)	If your host is not using DHCP, disable
rc.tcpip/dhcprd		/etc/rc.tcpip	Dynamic host configuration protocol (relay)	Disable this if you are not using DHCP or rely on passing information between networks
rc.tcpip/dhcpsd		/etc/rc.tcpip	Dynamic host configuration protocol (server)	Disable this if you are not a DHCP server
rc.tcpip/dpid2		/etc/rc.tcpip	Outdated SNMP service	Disable unless you need SNMP
rc.tcpip/gated		/etc/rc.tcpip	Gated routing between interfaces	Disable this service and use RIP or a router instead
rc.tcpip/mrouted		/etc/rc.tcpip	Multicast routing	Disable this service. Use a router instead
rc.tcpip/names		/etc/rc.tcpip	DNS name server	Use this only if your machine is a DNS name server
rc.tcpip/ndp-host		/etc/rc.tcpip	IPv6 host	Disable unless you use IPV6
rc.tcpip/ndp-router		/etc/rc.tcpip	IPv6 routing	Disable this unless you use IPV6.
rc.tcpip/routed		/etc/rc.tcpip	RIP routing between interfaces	Disable if you have a router for packets between networks
rc.tcpip/rwhod		/etc/rc.tcpip	Remote "who" daemon	Disable
rc.tcpip/sendmail		/etc/rc.tcpip	Mail services	Disable this service unless the machine is used as a mail server
rc.tcpip/snmpd		/etc/rc.tcpip	Simple network management protocol	Disable if you are not monitoring the system via SNMP tools



rc.tcpip/timed		/etc/rc.tcpip	Old Time daemon	Disable this service and use xntp instead
----------------	--	---------------	-----------------	---

Common Services

- Verify that sendmail is the latest version (executable and config); 'telnet <host> 25' to verify versions (if required). (Refer to www.sendmail.org)
 - o Version _____
- Verify that named is the latest version '(in)named version' (if required). (Refer to www.isc.org)
 - o Version _____
- Verify that sshd is the latest version; 'telnet <host> 22' to verify version. (Refer to www.openssh.org)
 - o Version _____
- Verify that sshd runs only Protocol 2 (check sshd_config)
- Verify that Apache is the latest version (if required). (Refer to www.apache.org)
 - o Version _____
- Verify that mod_ssl is the latest version (if required). (Refer to www.modssl.org)
 - o Version _____

Specific Services

Sendmail

- Confirm that relaying is turned off (promiscuous relay not set).
- Configure sendmail privacy flags (confPRIVACY_FLAGS set in sendmail.mc).
- If possible, configure sendmail to only queue/deliver mail, not accept outside connections.

BIND

- Verify that Dynamic updates are off.
 - o /etc/named.conf does not contain the 'allow-update' statement.
- Verify that recursion is off for external hosts.
 - o /etc/named.conf world view has 'recursion no' set.

Network Options

- If you wish to remotely administer your host, don't use unencrypted channels to do so (such as telnet). Configure your host to use encrypted communications with a utility such as SSH.

Final Updates

- Configure syslog to send system log output to a centralized logging servers.
- Verify that backup software has been installed and configured.

References:

http://www.cert.org/tech_tips/usc20_full.html#A114
http://colin.bitterfield.com/how_to_production_ready.html
http://www.menandmice.com/docs/DNS&BIND_security.pdf
<http://www.sendmail.org/m4/readme.html>
http://publib16.boulder.ibm.com/pseries/en_US/aixbman/security/securitytfrm.htm

