



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering  
"Securing Linux/Unix (Security 506)"  
at <http://www.giac.org/registration/gcux>

# United States Department of \_\_\_\_\_

## Office of \_\_\_\_\_

### **Instructions For Installing and Configuring a Hardened Version of the Solaris 8 Operating System for Use as an Oracle Database Server**

(provided by Tony Schloss)

This instruction document is specific to Sun Microsystems Enterprise-level hardware (not including the Starfire E10000), and for the Sun Operating System Solaris, version 8. While most of the instructions will readily apply also to Solaris 7, and possibly to later versions, it has been written explicitly for Solaris 8 and should be taken as such if there is a need or desire to use it with another version of the Operating System.

#### **Hardware:**

These instructions were performed and tested on a Sun E250 server (sun4u architecture), with 256MB of RAM, and a single internal 9GB hard drive. Obviously, some consideration will need to be taken with other hardware platforms, especially if the architecture is different, but by and large these instructions should well suffice.

This document assumes that the hardware decisions for your requirements & environment have already been made, and that the system is in-place and ready to be installed. Server sizing, capacity planning, load & load balancing considerations are beyond the scope of this document, and are the responsibility of the individual system manager(s), along with his/her case management team.

#### **Network Installation**

A word about installation while connected to a network: don't. That is, unless you absolutely have to do so, don't. There is normally no real need to be connected to a network at this stage of an installation, and doing so can put in you harm's way. However slight that may be, it's still an unnecessary risk, and one that you shouldn't take unless circumstances dictate. However, you are the system administrator or systems manager for this server, and should make the decision based on your experience and the situation at hand.

If you feel you need to do this installation while connected to a network, you need to get approval from the Office of \_\_\_\_\_. The request must include a justification as to why you

feel you need to do an on-network installation, and a detailed step-by-step Install Plan with a realistic timeline.

If you choose not to do a network-connected installation, be prepared to transfer files (e.g., the Recommended Patch Cluster) from a machine that does have Internet connectivity, to this one. The most logical method is via tape.

### **How to Use This Document**

While these instructions are not explicitly formatted as a checklist, per se, it is easy to use the document as such. The outline of the document is generally sequential, in that you can (should) start at the beginning and work your way through step-by-step. I recommend you read through the entire document before beginning, however; it will help to be prepared if you encounter a question or need explanation whilst in the middle of something.

The installation and configuration detailed here is meant to be done at one sitting, but in theory could be spread out over a day or so. It truly should not take more than a couple of hours. If for some reason you must leave and come back, make sure that the physical security for the server is high – in other words, it needs to be locked up tight in a controlled-access room. Otherwise, when you return to the machine after being away for any period of time, you should assume the machine is compromised and start over.

Remember, this instruction set, and the changes that will be made to the machine as a result of following them, are not a panacea – this will not magically declare your sever to be “A Secure Server of the Realm,” or any such nonsense. It’s simply a set of tools, among many others, that will *help* you maintain a secure environment. It’s still up to you to monitor and stay current.

© SANS Institute. Author retains full rights.

## Step-by-Step Instructions for Solaris 8 Installation & Configuration

### Boot the machine:

Boot from the Software (1 of 2) CD, \*not\* the Solaris Installation CD. As the machine boots, go through the language & locale selection; it will then take you into OpenWindows and then start the Solaris installation program.

### Identify the System:

1. Network Connectivity:  
Choose "Yes"
2. DHCP:  
Choose "No"
3. Hostname  
Enter the machine's hostname as provided by the Office of \_\_\_\_\_.
4. IP Address:  
Enter the machine's IP address as provided by the Office of \_\_\_\_\_.
5. Enable IPv6?  
I recommend choosing yes. Enabling IPv6 will add no additional processing requirements at this time, and will in essence have no effect on a non-IPv6 network. However, when in the future the Office of \_\_\_\_\_ begins to migrate to IPv6, you will have a much easier time if it's enabled from the beginning. IPv6 will require no additional administration while not in use. Choose your response accordingly, or based on guidance from the Office of \_\_\_\_\_.
6. Confirm Information:  
Confirm the information presented there, and click "Continue," or "Change" if changes are required.
7. Configure Kerberos Security:  
Choose "No" unless explicitly informed to do so by the Office of \_\_\_\_\_. They should be able to provide you with detailed implementation instructions if they require Kerberos.
8. Confirm Information:  
Confirm the information presented there, and click "Continue," or "Change" if changes are required.
9. Name service:  
Choose "None." You will modify this manually to your specific requirements later.
10. Confirm Information:  
Confirm the information presented there, and click "Continue," or "Change" if changes are required.
11. System part of a subnet?  
Choose "Yes."

12. Netmask:  
Enter the appropriate netmask.
13. Specify timezone by:  
Choose your preferred method of selecting the timezone (if unsure, select "Geographic Region;" it's the easiest), and click "Set..."
14. Set the timezone based on your choice above.
15. Date and Time:  
Set the date and time. If the machine is new from the factory, it will most likely have Pacific time preset. Simply correct the date & time, and click "Continue."
16. Confirm Information:  
Confirm the information presented there, and click "Continue," or "Change" if changes are required.

This completes System Identification. At this point the installation program will configure the system and begin execution of install scripts. After a short hiatus, the install program comes back and begins asking more questions.

### **Solaris Interactive Installation**

You will probably be informed that the system is upgradeable, and you will be asked if you want to Upgrade the existing installation, or begin an Initial Install.  
Choose "Initial"

### **Select Geographic Region**

There should be no reason to install support for any region other than the United States.

Choose North America, then U.S.A.

### **Select Software**

Here's where you will select the cluster, or Software Group, for installation, and begin the customization of that selection. Normally for a hardened Solaris box, you would choose the Core System Support only. However, you eventually will be installing Oracle and related products; Oracle no longer has a CLI (Command Line Interface) installation program, and you must install Oracle using their Java-based installer. Because of this, you need to install an X windows system on the Solaris box.

As such, select "End User System Support," ensure that Solaris 64 Bit Support is checked, and click "Customize."

1. Having selected the End User System Support cluster, a number of packages will be preselected for you. The following table indicates which preselected packages (or clusters) that you should deselect, and a few unselected packages (or clusters) that you should select. Again, use your judgment: look at each of the packages (not just those listed here), and make sure that you either need them or don't need them, as appropriate to your situation. Packages listed should be deselected unless otherwise noted.

Select	Full Package Name	Package <sup>(1)</sup>
	64-bit incov conversion for Eastern European Locales	SUNWislcx
	64-bit incov conversion for ISO Latin Character Sets	SUNWisolx
	Audio Drivers (64-bit)	SUNWauddx
	Authentication Management Infrastructure	SUNWami
	Authentication Management Infrastructure (64-bit)	SUNWamix
	CDE End User Software	
	CDE Help Runtime	SUNWdthe
	CDE Help Volumes	SUNWdtev
	CDE Release Documentation	SUNWtrme
	Java Media Framework Player	SUNWjmfp
	PDA Synchronization for Solaris	SUNWpdas
	Solaris CDE Image Viewer	SUNWdtim
	Solaris Desktop Extensions Applications	SUNWdtezt
	Solaris Smart Card Administration GUI	SUNWscgui
	Configuration Files for Authentication Management Infrastructure	SUNWamir
	Font Downloader	SUNWfdl
	Font Server Cluster	
	Font Server	SUNWxwfs
	X Window System optional fonts	SUNWxwoft
	Frame Buffer Configuration Utility	SUNWfbc
	Freeware Compression Utilities	
Select	The GNU Zip (gzip) compression utility	SUNWgzip
Select	The INFO-Zip (zip) compression utility	SUNWzip
	Freeware Other Utilities	
Select	The GNU Patch utility	SUNWgpch
Select	The GNU pager (less)	SUNWless
Select	Freeware Shells	SUNWCfwshl
	Install Software	SUNWinst
	Java VM	
	JDK 1.2 demo programs	SUNWj2dem
	Locale Conversion Library	SUNWlcl
	Locale Conversion Library (64-bit)	SUNWlclx
	Localization Common Files	SUNWlccom
Select	On-Line Manual Pages	SUNWman
	On-Line Open Issues Readme	SUNWrdrd
	OpenWindows Version 3	

Select	Full Package Name	Package <sup>(1)</sup>
	OPEN LOOK Audio applications	SUNWolaud
	OpenWindows online Handbooks	SUNWolbk
Select	X Window System online user man pages	SUNWxwman
	Perl 5	
Select	Perl 5.005_03 (POD Documentation)	SUNWplp5
Select	Perl 5 On-Line Manual Pages	SUNWpl5m
	Power Management OW Utilities	SUNWCpmon
	Power Management Software	SUNWCpm
	Power Management Software (64-bit)	SUNWCpmx
	Print Utilities for CTL Locales	SUNWctlu
	Russian 1251 fonts	SUNW1251f
	Solaris Product Registry & Web Start runtime support	SUNWwsr
<sup>(2)(3)</sup>	Sparc Storage Array Drivers	SUNWssad
<sup>(2)(3)</sup>	Sparc Storage Array Drivers (64-bit)	SUNWssadx
<sup>(2)</sup>	Sun Fibre Channel Transport Software	SUNWCfct
<sup>(2)</sup>	Sun Fibre Channel Transport Software (64-bit)	SUNWCfctx
Select	System Accounting	SUNWacc
Select	Terminal Information	SUNWter
	Web-based Enterprise Management (WBEM) Services	SUNWCwbem
	X Window System Minimum Required Fonts for Multibyte Locales	SUNWCxmft
	X11 Arabic required fonts	SUNWarrf
	X11 ISO-8859-x optional fonts	SUNWCiof
	X11 ISO-8859-x required fonts	SUNWCirf
	X11 sun_eu_greek fonts	SUNWeugrf
	XCU4 Utilities	SUNWxcu4
	XCU4 Utilities (64-bit)	SUNWxcu4x
	XSH4 Conversion for Eastern European Locales	SUNWislcc
	XSH4 Conversion for ISO Latin Character Sets	SUNWisloc
	en_US.UTF-8	SUNWCutf8
	en_US.UTF-8 (64-bit)	SUNWCutf8x

- <sup>(1)</sup> Packages with a "C" in the fifth position (SUNWC....) indicate a software cluster. Individual packages that comprise the cluster are listed in the file `/cdrom/Solaris_8/Product/.clustertoc` (assuming the CD is mounted on `/cdrom`).
- <sup>(2)</sup> Package may be required, depending on your hardware configuration
- <sup>(3)</sup> Deselection of this package may show broken dependencies when first deselected, but will be resolved as you progress through the list.

- From the Customize Software screen, once done selecting packages, click "OK," which brings you back to the Software Group selection screen.  
Click "Continue" to go on from here.

### 3. Select Disks

Select the disk or disks on which you want to configure filesystems. At this point I recommend you work solely on the boot disk, unless your install plan uses any secondary disks for OS-required filesystems (e.g., /opt, /var, et cetera). The primary (boot) disk should be labeled as such on the listing displayed, and pre-selected.

### 4. Preserve Data?

You should be asked if you want to preserve any existing data. There should be no reason to preserve any of the filesystems preloaded at the factory.

Select "Continue."

### 5. Automatically Layout File Systems

Choose "Manual Layout."

### 6. File System and Disk Layout

You will be presented with a summary of the current filesystem & disk layout; there should be only one partition listed – the overlap (slice 2).

Choose "Customize."

### 7. Lay Out File Systems

I'm not going to get into the philosophical & near-metaphysical argument over filesystem sizes here. Presumably you have some experience as a system administrator of a \*NIX system, or you wouldn't be here doing this now. I will make recommendations based on my experience with this client (Department of \_\_\_\_\_, Office of \_\_\_\_\_) and the specifics of Oracle database servers within this environment; you will need to make the final choices as to what to do.

Beginning with Solaris 8, the Installer program seems to want to minimize the number of system filesystems, putting most everything under the root (/) filesystem itself. For various reasons, I recommend against this.

Below are my recommendations for the minimum filesystems you should create:

<u>Slice</u>	<u>Filesystem</u>	<u>Minimum Size</u>
s0	/	100MB
s1	(swap)	(1)
s2	--	(overlap - entire disk)
s3	/usr	200MB
s4	/var <sup>(2)</sup>	500MB
s5	/opt <sup>(3)</sup>	500MB
s6	/extra	remainder of disk <sup>(4)</sup>
s7	(unused) <sup>(5)</sup>	

(1) the old rule of thumb of having a swap size equal to twice the amount of physical memory is becoming less necessary. I



make the assumption here that since this will be an Oracle server, you more than likely have 512MB or more of physical memory. If this is the case, I recommend simply having 512MB of swap space, unless you explicitly need more (e.g., if this will be a development Oracle server on which you will do core file analysis), and depending on your available disk space.

- (2) the more log information you expect, the larger this should be.
- (3) with Solaris, I recommend keeping this; too many third-party applications (as well as Sun apps) require this, and it helps significantly having it as its own filesystem. Also note that `/opt` is easy to put on another disk, if you are short on space or on available disk partitions (Sun only gives you 7).
- (4) I normally leave the remainder of the disk "unused" and mounted as `/extra` -- this simply gives you a place for some empty filesystem space for when you need it -- I've never regretted having it.
- (5) I recommend you leave between 5 and 10 megabytes free (unformatted) to give you some working room should you decide in the future to use Online Disk Suite or another disk management product. Note also that Veritas Volume Manager requires two free partitions to encapsulate the root drive.

Note: If you intend to use Veritas Volume manager (or any other disk management product), I **highly** recommend that you be very familiar with its requirements before beginning the process of disk partitioning & filesystem layout.

Optional:

`/usr/local`

Usually should not be required on a production Oracle server, but if this will be a database/development server and you expect to use a lot of 3rd-party development tools installed in `/usr/local`, then I recommend this be a separate filesystem (on another disk, normally)

Once you are done and satisfied with the filesystem layout as you have it, click "Continue."

8. Mount Remote Filesystems?

Select "Continue."

9. Profile

Here you are presented with the profile, or summary, of all the choices you just made. Verify that all is as you wish them to be for the installation.

Click "Begin Installation."

10. Auto Reboot / Manual Reboot

Select "Auto reboot."

11. Root Password

Enter the root password. Immediately write this down on the same form (see Appendix B) you will use to record the EEPROM password later in this installation. Make sure you don't leave that step for another day, thereby leaving the password form out in the open.

12. Insert the Solaris Software 2 of 2 CD.

- a. Click "Continue."

13. Installation Summary

This screen provides you with the opportunity to view the details of the OS installation.

Click "Next" to continue.

14. Reboot

Remove the CD; click "Reboot Now" to continue.

15. Log in

Log in as root; take a few minutes to get your desktop arranged and organized the way you like it.

16. Create Your Account

Immediately create an account for yourself. Once completed, log off as root, log in as yourself, and su to root.

17. Once the system is back up, stop the volume management daemon (this will make it easier to do the following steps with the CD), & mount the CD manually.

- a. ensure the directory /cdrom exists, and is mode 777; if not, create and chmod it before running the next commands:

```
mkdir /cdrom && chmod 777 cdrom
```

- b. stop the Volume Manager & mount the CD

```
/etc/rc2.d/S92volmgt stop
```

```
mount -o ro -F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

```
cd /cdrom/Solaris_8/Product
```

18. Install the following packages that were left out of the initial installation (note that these packages are all on CD 2 of 2, which should still be in the drive):

```
/usr/sbin/pkgadd -d . SUNWarc SUNWbtool SUNWsprot \  
SUNWhea SUNWtnfc SUNWtnfd SUNWlibm
```

## Post-installation Network Configuration Changes

1. Create the file `/etc/defaultrouter`. The format is simply the IP address (or hostname) of one or more default routers for the network, separated by white space. Note that if you use hostnames (not recommended), you need to add and maintain static hostname entries in the `/etc/hosts` file for those routers.
2. Create the file `/etc/resolv.conf`. The format is a list of keyword-value pairs, one to a line, as follows:

```
nameserver 192.168.1.1
nameserver 10.10.2.2
```

There is (currently) a maximum of three nameserver entries for this file.

3. Change the name service switch file.
  - a. After an initial installation, the current `/etc/nsswitch.conf` should be identical to `/etc/nsswitch.files`. Run the following command to verify this:

```
diff /etc/nsswitch.conf /etc/nsswitch.files
```

If the two are identical, you will get no errors or other messages; continue with the next step. If the latter file does not exist, or if the two are not identical, you will get an output from the `diff` command enumerating the differences and their locations within the files; go to step 3.c (the output itself is irrelevant here).

- b. If the two files (`/etc/nsswitch.conf` and `/etc/nsswitch.files`) are identical, simply run the following copy command to set the name service to use DNS (secondarily to files):

```
cp /etc/nsswitch.dns /etc/nsswitch.conf
```

- c. If the two files (`/etc/nsswitch.conf` and `/etc/nsswitch.files`) are different, simply edit the existing `nsswitch.conf` file, and change the line that begins with the word “hosts” to read

```
hosts files dns
```

4. Set the domain for the machine:

```
domainname {domain name provided by Office of _____}
domainname > /etc/defaultdomain
```

5. Reboot the machine.

## Install Patches

1. Using a machine that is connected to the Internet (since you are doing this install while disconnected from any network, right?), obtain the latest release of the Recommended Patch Cluster for Solaris 8 from <http://sunsolve.sun.com>. The file will be in ZIP format, as opposed to the older .Z format (UNIX compressed).
2. Unpack the ZIP file (assuming you downloaded it to `/tmp`):

```
cd /tmp
unzip 8_Recommended
```

3. Apply the patch cluster:

```
cd 8_Recommended
./install_cluster -nosave
```

Note 1: the `-nosave` option disallows backout – this isn't an issue at this point (you are freshly installing the OS, there's nothing to break yet), but you should generally not use this strategy once the system is operational, without making an informed decision).

Note 2: you will in all likelihood get a number of errors; error code 8 indicates that the patch applies to a package that is not installed on the system, and error code 2 indicates that the patch was already installed from the OS CD.

4. Remove the patch cluster:  

```
rm -r /tmp/8_Recommended*
```
5. Reboot.

### **Strip down the Operating System**

The default Solaris installation enables a number of services that are simply not needed, and are therefore potential security problems. The best way to protect yourself from security problems dealing with a service that you don't need is simply to not run the service. The following section eliminates as many of the normally unneeded services and their respective start-up scripts as possible. As with anything, however, please use your experience and common sense – don't disable a service that you are going to use (whether recommended or not).

The easiest way to accomplish the basic task of removing these services is to run the script that you've been provided (and is reproduced at the end of this document). Again, this script is not a panacea – some things will be turned off or removed that you may want for your installation. Likewise some things may be left enabled that, through your experience, you feel you simply don't need and would rather do without.

While the script is documented to explain what it is doing as it goes along, I recommend that you read through the script carefully to understand what it is doing before running it. That way, if you disagree with any of the services or files that it is set to remove, you can comment that section out of the script. Alternatively, you can do each of the steps listed within the script manually.

### **Fine Tuning the OS Security**

Some things yet need to be done that cannot be automated in a script, or are perhaps better left to be done manually. These steps are detailed below.

1. Remove (or comment out (using #)) the following line from `/etc/inittab`:  

```
sc:234:respawn:/usr/lib/saf/sac -t 300
```

2. Edit the `/etc/passwd` file, and make `/dev/null` the shell for all non-root users left after running the post-install script provided (assuming you've created no other accounts yet, and not including the account you created for yourself). Do not leave the shell field blank – add `/dev/null` as the shell for added security.
3. Edit the `/etc/vfstab` file, and change the mount options on the filesystems other than root (`/`). The rule of thumb is that normal UFS filesystems (n/i root) are mounted either read-only or no-suid. As the `/usr` filesystem has all of the suid files, it should be mounted read-only. The remainder of the files systems should be mounted nosuid. Below is an example `/etc/vfstab` file:

#device #to mount	device to fsck	mount point	FS type	fsck pass	mount at boot	mount options
#						
#/dev/dsk/c1d0s2	/dev/rdisk/c1d0s2	/usr	ufs	1	yes	-
fd	-	/dev/fd	fd	-	no	-
/proc	-	/proc	proc	-	no	-
/dev/dsk/c0t0d0s3	-	-	swap	-	no	-
/dev/dsk/c0t0d0s0	/dev/rdisk/c0t0d0s0	/	ufs	1	no	-
/dev/dsk/c0t0d0s6	/dev/rdisk/c0t0d0s6	/usr	ufs	1	no	ro
/dev/dsk/c0t0d0s1	/dev/rdisk/c0t0d0s1	/var	ufs	1	no	nosuid
/dev/dsk/c0t0d0s7	/dev/rdisk/c0t0d0s7	/home	ufs	2	yes	nosuid
/dev/dsk/c0t0d0s5	/dev/rdisk/c0t0d0s5	/opt	ufs	2	yes	nosuid
/dev/dsk/c0t0d0s4	/dev/rdisk/c0t0d0s4	/usr/local	ufs	2	yes	nosuid
swap	-	/tmp	tmpfs	-	yes	nosuid

4. Create root's home directory:
  - a. create the directory `/root`.
  - b. Change permissions to 400.
  - c. Edit the `/etc/password` file and change root's home directory entry.
5. Edit the `/etc/syslog` file to add the LOG\_AUTH functionality. Add the following line:
 

```
auth.info          /var/log/authlog
```
6. It's recommended that you create a script to rotate these log files on a regular basis. Reference `/usr/lib/newsyslog` as an example.
7. You do not need to run the sendmail daemon, as seems to be the thinking of those who create the installation programs. Eliminating sendmail from the startup scripts has already been accomplished (via the `post_install.sh` script you were provided). However, for the system to be able to maintain some semblance of email sanity, even if it's only `cron` sending mail to root on a nightly basis, you need to run sendmail on a periodic basis; since we aren't running the daemon, we need a `cron` entry, as follows:

```
0 * * * * /usr/lib/sendmail -q
```

It is highly recommended that you also replace the `/etc/mail/sendmail.cf` file with the one provided in Appendix C.

Note: ***Please*** keep your version of sendmail current. For this reason, it may be beneficial for you to use the Open Source version, as opposed to the Solaris version, which can be slightly behind. The Open Source version is available from <http://www.sendmail.org>.

8. Create (or modify) the file `/etc/motd` to display the current Department of \_\_\_\_\_ (Office of \_\_\_\_\_) statutory warning. You can get the wording for this from the Office of \_\_\_\_\_.
9. Turn on EEPROM-level security, and set the EEPROM password:
  - a. `eeeprom security-mode=command`
  - b. this will ask you for a password: enter the eeprom security-password (do NOT use the same password as is used for the root account)
  - c. Immediately write down the EEPROM password. Use the same form (Appendix B) used to record the root password.
  - d. Seal the envelope, and hand-carry the sealed envelope to the Office of \_\_\_\_\_ for storage in the DP Manager's safe.
10. Edit the file `/etc/default/login`, and uncomment the line that reads:  
`#umask=022`
11. Edit the file `/etc/default/inetinit`, and change the entry there to read as follows:  
`TCP_STRONG_ISS=2`
12. Edit the file `/etc/default/passwd` to turn on password aging, making the following changes:  
`MAXWEEKS=6`  
`MINWEEKS=2`  
Leave the `PASSLENGTH` setting as it is.
13. It is highly recommended that you obtain, install, and configure the TCP Wrappers software and the SSH software. These both will be addressed with detailed installation & configuration instructions separately.

## **Backup**

Do a complete level-0 backup on the entire system. You can put it all on one tape or use a separate tape for each filesystem, depending on your preference. Replicate the tape(s), and maintain one (set) on site (locked up), and a second at your off-site storage facility.

## Bibliography

The SANS Institute Solaris Security, Step by Step (version 1.0)  
Hal Pomeranz, editor

The SANS Institute Global Incident Analysis Center Linux/Solaris Practicum (from the Securing UNIX Systems Course)

Sun Microsystems Web Sites (<http://www.sun.com>):

BigAdmin (<http://www.sun.com/bigadmin>)

SunDocs (<http://docs.sun.com>)

Sun Online Support Center (<http://www.sun.com/service/online>)

Solaris 8 On-Line Manual Pages

© SANS Institute 2000 - 2005, Author retains full rights.

## Appendix A: Post Installation Script (post\_install.sh)

```
#!/bin/sh

#####
# Set a few variables
#####

ECHO='/usr/ucb/echo -n'
LOGFILE="/var/adm/log/post_install.log"
NFS_PRESERVE=
RM='/usr/bin/rm -f'
CP='/usr/bin/cp'
MV='/usr/bin/mv'
REMOVED='/etc/.REMOVED'
BLANK='echo ""'

#####
# Housekeeping: get/verify OS version; check for existing logfile; verify that
# root is running the script; create save directory
#####

OSV=`uname -r`
if [ $OSV != "5.8" ]; then
    echo "This script is intended for Solaris 8 (SunOS 5.8).\"
    echo "You are at the wrong OS Version; bailing.\"
    exit 1
fi

if [ -f $LOGFILE ] ; then
    echo \"$LOGFILE already exists; this could indicate that the script\"
    echo \"has already been run, or that it did not complete cleanly on a previous run.\"
    echo \"Please check and clean this up, and restart the script if warranted.\"
    exit 1
fi

if [ -x /usr/bin/id ]
then
    eval ` /usr/bin/id | /usr/bin/sed 's/[^a-z0-9=].*//`
    if [ \"${uid:=0}\" -ne 0 ]
    then
```



## Appendix A: Post Installation Script (post\_install.sh)

```
                echo "$0: Only root can run $0"
                exit 1
            fi
else
    echo "$0: can't check user id."
    exit 1
fi

if [ -d $REMOVED ] ; then
    echo "$REMOVED directory already exists; cannot continue."
    echo "Please resolve this conflict and re-run this script."
    exit 1
else
    /usr/bin/mkdir /etc/.REMOVED
fi

#####
# Preserve a list of filenames from the /etc/rc[013].d directories, just in case
#####

$ECHO "preserving a list of filenames from /etc/rc[013].d directories..." | tee -a $LOGFILE
ls -la /etc/rc[013].d > /etc/rc013_files_list
echo "done." | tee -a $LOGFILE
echo "(this can be found in /etc/rc013_files_list)" | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Check to make sure the sysadmin doesn't want to run an NFS server
#####

echo "Will you be running the NFS service on this box (NOT recommended)? [n]"
read NFS_PRESERVE
case $NFS_PRESERVE in
    y|Y) echo "You said yes; the NFS Server startup script will be preserved." | tee -a $LOGFILE
        $CP /etc/rc3.d/S15nfs.server /etc
        NFS_PRESERVE="YES"
        ;;
    *) echo "the NFS Server startup script will be removed." | tee -a $LOGFILE
        ;;
esac
```

## Appendix A: Post Installation Script (post\_install.sh)

```
$BLANK; $BLANK

#####
# Remove the startup scripts from /etc/rc[013].d
#####

$ECHO "removing startup scripts from /etc/rc[013].d ..." | tee -a $LOGFILE
$RM /etc/rc[013].d/*
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Put the NFS Server startup script back, if preserved
#####

if [ $NFS_PRESERVE = "YES" ]; then
    $ECHO "restoring the NFS Server startup script..." | tee -a $LOGFILE
    $MV /etc/S15nfs.server /etc/rc3.d
    echo "done." | tee -a $LOGFILE
$BLANK; $BLANK
fi

#####
# Turn off autoconfiguration startup scripts
#####

$ECHO "turning off autoconfiguration capability ..." | tee -a $LOGFILE
for file in S30sysid.net S71sysid.sys S72autoinstall; do
    $MV /etc/rc2.d/$file /etc/rc2.d/.NO$file
done
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Turn off NFS related links
#####

if [ $NFS_PRESERVE != "YES" ]; then
    $ECHO "turning off NFS related links ..." | tee -a $LOGFILE
```

## Appendix A: Post Installation Script (post\_install.sh)

```
    for file in K*nfs.server S73nfs.client S74autofs *cachefs*; do
        $MV /etc/rc2.d/$file /etc/rc2.d/.NO$file
    done
    echo "done." | tee -a $LOGFILE
$BLANK; $BLANK
fi

#####
# ...RPC links
#####

$ECHO "turning off RPC related links ..." | tee -a $LOGFILE
for file in S76nsd; do
    $MV /etc/rc2.d/$file /etc/rc2.d/.NO$file
done
echo "done." | tee -a $LOGFILE

#### note that S71rpc was originally included in abv list; removed (and left enabled
#### during startup) so that the Desktop Login will continue to work (there is a problem
#### with the DT Message Server (apparently needing RPC) without this.

$BLANK; $BLANK

#####
# ...volume management
#####

$ECHO "turning off volume management ..." | tee -a $LOGFILE
$MV /etc/rc2.d/S92volmgt /etc/rc2.d/.NOS92volmgt
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# ...and Sendmail & expreserve
#####

$ECHO "turning off sendmail and expreserve ..." | tee -a $LOGFILE
```

## Appendix A: Post Installation Script (post\_install.sh)

```
$MV /etc/rc2.d/S88sendmail /etc/rc2.d/.NOS88sendmail
$MV /etc/rc2.d/S80PRESERVE /etc/rc2.d/.NOS80PRESERVE
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Check the default system UMASK; fix if necessary
#####

echo "checking system default umask ..." | tee -a $LOGFILE
/usr/bin/grep "CMASK=022" /etc/default/init
if [ $? -ne 0 ]; then
    echo "Your default system umask value is *NOT* 022; change it (HIGHLY recommended)? [y]"
    read CHGMSK
    case $CHGMSK in
        n|N)
            echo "default system umask value not set/changed." | tee -a $LOGFILE
$BLANK; $BLANK
            ;;
        *)
            echo 'umask 022' > /etc/init.d/umask.sh
            chmod 744 /etc/init.d/umask.sh
            for dir in /etc/rc?.d; do
                ln -s ../init.d/umask.sh $dir/S00umask.sh
            done
            echo "default system umask changed to 022." | tee -a $LOGFILE
            $BLANK; $BLANK
            ;;
    esac
else
    echo "default umask is fine (022)." | tee -a $LOGFILE
$BLANK; $BLANK
fi

#####
# Set tunable INET parameters to add network protections
#####

$ECHO "setting tunable parameters for TCP/IP interface ..." | tee -a $LOGFILE
```

## Appendix A: Post Installation Script (post\_install.sh)

```
cat <<EOF> /etc/rc2.d/S69inet-b
/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 8096
/usr/sbin/ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
/usr/sbin/ndd -set /dev/ip ip_ignore_redirect 1
/usr/sbin/ndd -set /dev/ip ip_send_redirects 0
/usr/sbin/ndd -set /dev/ip ip_ire_arp_interval 60000
/usr/sbin/ndd -set /dev/arp arp_cleanup_interval 60000
/usr/sbin/ndd -set /dev/ip ip_forward_src_routed 0
/usr/sbin/ndd -set /dev/ip ip_forward_directed_broadcasts 0
/usr/sbin/ndd -set /dev/ip ip_forwarding 0
/usr/sbin/ndd -set /dev/ip ip_scrip_dst_multihoming 1
EOF

/usr/bin/chmod 744 /etc/rc2.d/S69inet-b
/usr/bin/chgrp sys /etc/rc2.d/S69inet-b
echo "done." | tee -a $LOGFILE
echo "(see /etc/rc2.d/S69inet-b for details)." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Remove /etc/init.d/inetsvc (and /etc/rc2.d/S72inetsvc), and replace
# with scaled down version
#####

echo "Replacing /etc/init.d/inetsvc script -- note that once this step" | tee -a $LOGFILE
echo "is completed, you will no longer be able to telnet/ftp to this machine" | tee -a $LOGFILE
echo "unless/until you install and configure SSH." | tee -a $LOGFILE
$BLANK

$ECHO "Moving old file ..." | tee -a $LOGFILE
$MV /etc/init.d/inetsvc /etc/init.d/OLDinetsvc
$MV /etc/rc2.d/S72inetsvc /etc/rc2.d/.NOS72inetsvc

$ECHO "creating new file ..." | tee -a $LOGFILE
cat <<EOF> /etc/init.d/inetsvc
#!/bin/sh
```

## Appendix A: Post Installation Script (post\_install.sh)

```
/usr/sbin/ifconfig -au netmask + broadcast +

if [ -f /usr/sbin/in.named -a -f /etc/named.boot ]; then
    /usr/sbin/in.named
    echo "starting internet domain name server."
fi

#mcastif=`uname -n`
#echo "Setting default interface for multicast: \c"
#/usr/sbin/route add -interface \
#    -netmask "240.0.0.0" "224.0.0.0" "$mcastif"

# Run inetd in "standalone" mode (-s flag)
#/usr/sbin/inetd -s
EOF

ln /etc/init.d/inetsvc /etc/rc2.d/S72inetsvc

echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Some final cleanup steps: removing NFS services, cleaning
# up the password file, crontabs, etc.
#####

$ECHO "cleaning up empty/unused crontab files (adm, lp, & sys) ..." | tee -a $LOGFILE
cd /var/spool/cron/crontabs
$RM adm lp sys
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

echo "cleaning out the /etc/passwd file ..." | tee -a $LOGFILE
for user in uucp nuucp adm kp smtp listen; do
    /usr/bin/passmgmt -d $user
    echo "$user removed from /etc/passwd" >> $LOGFILE
done
```

## Appendix A: Post Installation Script (post\_install.sh)

```
echo "...done." | tee -a $LOGFILE
$BLANK; $BLANK

$ECHO "removing the inetd.conf file..." | tee -a $LOGFILE
$MV /etc/inet/inetd.conf $REMOVED
$RM /etc/inetd.conf
echo "done." | tee -a $LOGFILE
$BLANK
echo "/etc/inet/inetd.conf was moved to $REMOVE, and /etc/inetd.conf was deleted;" >> $LOGFILE
echo "if this file is needed later, restore to /etc/inet, and link /etc/inetd.conf to that." >> $LOGFILE
$BLANK; $BLANK

if [ NFS_PRESERVE != "YES" ] ; then
    $ECHO "cleaning out NFS files in /etc..." | tee -a $LOGFILE
    $MV /etc/auto_* $REMOVED
    $MV /etc/dfs/dfstab $REMOVED
    echo "... done." | tee -a $LOGFILE
    $BLANK
    echo "/etc/auto_* and /etc/dfs/dfstab were moved to $REMOVE" >> $LOGFILE
    $BLANK; $BLANK
fi

#####
# Enable/fix logging (syslog events to be sent to AUTH_LOG; failed logins)
#####

$ECHO "Creating /var/log/authlog ..." | tee -a $LOGFILE
/usr/bin/touch /var/log/authlog && /usr/bin/chown root /var/log/authlog && /usr/bin/chmod 600 /var/log/authlog
echo "done." | tee -a $LOGFILE
echo "(This will allow the syslog utility to log events to the LOG_AUTH facility)." | tee -a $LOGFILE
$BLANK; $BLANK

$ECHO "Creating /var/adm/loginlog ..." | tee -a $LOGFILE
/usr/bin/touch /var/adm/loginlog && /usr/bin/chown root /var/adm/loginlog
/usr/bin/chgrp sys /var/adm/loginlog && /usr/bin/chmod 600 /var/adm/loginlog
echo "done." | tee -a $LOGFILE
echo "(This will capture failed logins.)" | tee -a $LOGFILE
$BLANK; $BLANK
```

## Appendix A: Post Installation Script (post\_install.sh)

```
#####
# Miscellaneous
#####

$ECHO "Creating /etc/ftpusers file ..." | tee -a $LOGFILE
/usr/bin/touch /etc/ftpusers
for user in root daemon bin sys nobody noaccess nobody4 uucp nuucp adm lp smtp listen; do
    echo $user >>/etc/ftpusers
done
/usr/bin/chown root /etc/ftpusers && /usr/bin/chgrp root /etc/ftpusers && /usr/bin/chmod 600 /etc/ftpusers
echo "done." | tee -a $LOGFILE
echo "(see /etc/ftpusers file for a list of those accounts now denied FTP access)." | tee -a $LOGFILE
$BLANK; $BLANK

$ECHO "Removing .rhosts support from /etc/pam.conf ..." | tee -a $LOGFILE
/usr/bin/grep -v rhosts_auth /etc/pam.conf > /etc/pam.new
$MV /etc/pam.new /etc/pam.conf
/usr/bin/chown root /etc/pam.conf && /usr/bin/chgrp sys /etc/pam.conf && /usr/bin/chmod 644 /etc/pam.conf
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

echo "Do you want to disable Stop-A abort sequence (recommended if physical security is weak/lacking)? [y]"
read STOPA
case $STOPA in
    n|N)
        echo "Stop-A abort sequence will be preserved"
        ;;
    *)
        $ECHO "disabling Stop-A abort sequence ..." | tee -a $LOGFILE
        /usr/bin/sed 's/^#KEYBOARD_ABORT=disable/KEYBOARD_ABORT=disable/g' \
            /etc/default/kbd > /etc/default/kbd.new
        $MV /etc/default/kbd.new /etc/default/kbd
        /usr/bin/chown root /etc/default/kbd && /usr/bin/chgrp sys /etc/default/kbd
        /usr/bin/chmod 444 /etc/default/kbd
        echo "done." | tee -a $LOGFILE
        ;;
esac
```



## Appendix A: Post Installation Script (post\_install.sh)

```
$BLANK; $BLANK

$ECHO "editing /etc/system to try to prevent some log buffer overrun attacks ..." | tee -a $LOGFILE
$CP /etc/system /etc/system.bak
if [ -r /etc/system.bak ]; then
cat <<EOF>> /etc/system
* Attempt to prevent and log stack-smashing attacks
set noexec_user_stack = 1
set noexec_user_stack_log = 1
EOF
fi
echo "done." | tee -a $LOGFILE
$BLANK; $BLANK

#####
# Final Cleanup
#####

/usr/bin/chown root $REMOVED && /usr/bin/chgrp root $REMOVED && /usr/bin/chmod 400 $REMOVED

cat <<EOF | tee -a $LOGFILE
Finished with automated post-install hardening.
Please continue manually with your checklist.

Notes:
1. Files removed from /etc/rc[013].d can be re-linked to their originals in /etc/init.d,
   if necessary. These files were not permanently deleted.
2. Files removed from the /etc directory are preserved in /etc/.REMOVED (mode 400).
3. Files removed from /etc/rc2.d were hidden within the same directory (renamed
   to .NO{filename}).
4. Details of this install process can be found in $LOGFILE.

Reboot now.
EOF
```

Appendix A: Post Installation Script (post\_install.sh)

```
exit 0
```

© SANS Institute 2000 - 2005, Author retains full rights

© SANS Institute 2000 - 2005, Author retains full rights.

US Department of \_\_\_\_\_, Office of \_\_\_\_\_

**Server Identification & Password Form**

Machine hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_

Location (Physical): \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

EEPROM Password: \_\_\_\_\_

Superuser (root) password: \_\_\_\_\_

\_\_\_\_\_

System Administrator Name: \_\_\_\_\_

System Administrator Signature: \_\_\_\_\_

Date: \_\_\_\_\_

© SANS Institute 2000 - 2005, Author retains full rights.

## Appendix C: Minimal /etc/mail/sendmail.cf File

```
# Minimal client sendmail.cf

### Defined macros
# The name of the mail hub - PUT APPROPRIATE HOSTNAME FOR YOUR SITE HERE!!!!
    DRmailhost

# Define version
V8

# From whom errors should appear to be
DnMailer-Daemon

# Formatting of the UNIX from line
DlFrom $g $d

# Separators
Do.:%@!^=/[[]

# From of the sender's address
Dq<$g>

# Spool directory
OQ/usr/spool/mqueue

### Mailer Delivery Agents
# Mailer to forward mail to the hub machine
Mhub,      P=[IPC], S=0, R=0, F=mDFMuCX, A=IPC $h
# Sendmail requires these, but are not used
Mlocal, P=/dev/null, F=rlsDFMmnuP, S=0, R=0, A=/dev/null
Mprog,  P=/dev/null, F=lsDFMeuP, S=0, R=0, A=/dev/null

### Rule sets - WHITE SPACE BETWEEN COLUMNS MUST BE TABS!!!!

S0
R@$+      $#hub $: Missing user name
R$+      $#hub $@#R $:$1          forward to hub

S3
R$*<>$*   $n                      handle <> error address
R$<$*>$*  $2                      basic RFC822 parsing
```

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



<b>SANS 2018</b>	<b>Orlando, FL</b>	<b>Apr 03, 2018 - Apr 10, 2018</b>	<b>Live Event</b>
<b>SANS OnDemand</b>	<b>Online</b>	<b>Anytime</b>	<b>Self Paced</b>
<b>SANS SelfStudy</b>	<b>Books &amp; MP3s Only</b>	<b>Anytime</b>	<b>Self Paced</b>