Global Information Assurance Certification Paper

Installing and Securing Solaris 8

By: Eric L. Sammons

Purpose

The purpose of this document is to outline the process by which Solaris 8 can be installed and secured. When installing any operating system you should know your business requirements and what applications will be running on the installed server. Though this system was installed and configured to function as a web server we will not discuss the configuration or securing of the web server. -- That is a document in its self.
In addition I have chosen not to secure the system via the EEPROM as the physical security of the system is adequate. Depending on your site's physical security for systems you may want to investigate the security features available via the EEPROM.

What You Will Need

- Solaris 8 Media Pack \ Specifically Software CD 1 of 2 and Software CD 2 of 2.
  Solaris 8 Media Pack 10/00 was used for this process.
- A server. This process applies to the SPARC platform.
  An Ultra-5 SPARC IIi was used for this process.
- A completed pre-work worksheet.
  An example of my completed worksheet is attached. Your worksheet may be in a different format, but it is highly recommended that you have one as it will make the install process go much faster.
- CD Media with the current patch cluster from sunsolve.sun.com.
- CD Media with lsof, nmap, tcp_wrappers, sudo, logrotate, and openSSH.
  (These tools are available from http://www.BigAdmin.com in binary version for each release of Solaris. Verify versions are current enough for your needs.)

Pre-work

Setting	Value
Language	English
Locale	English (C 7-Bit ASCII)
Network Connected	☒ Yes ☐ No
DHCP?	☐ Yes ☒ No
Hostname	Webserver
IP Address	100.100.100.100
Default Gateway (Not required immediately.)	100.100.100.1
DNS Name Server(1)	100.100.100.2
DNS Name Server(2)	100.100.101.2
DNS Name Server(3)	100.100.102.2
DNS Search Path	myservers.com

Filesystem Layout

Filesystem Layout *For the purpose of this document our server had two disks. Each disk was 9GB in size and were internal. The first disk was c0t0d0 and the second was c0t1d0. Disk configurations and layouts are generally a matter of preference on the part of the installer, business, or System Administrator. These allocations here are only meant to be a guide. Also note, it is current understanding that Sun Microsystems no longer offers a 9 GB disk option.*	**Disk & Slice**	**Mount Point**	**Size**
	c0t0d0s0	/	300
	c0t0d0s1	Swap	Memory + 100 MB * Differs with Administrator, system, and requirements.
	c0t0d0s2	UNUSED	UNUSED
	c0t0d0s3	/var	2500 MB
	c0t0d0s4	/opt	1500 MB
	c0t0d0s5	/usr	1000 MB
	c0t0d0s6	/usr/local	$ (remaining)
	c0t0d0s7	UNUSED	UNUSED
	c0t1d0s0	/backups	6000 MB
	c0t1d0s1	UNUSED	UNUSED
	c0t1d0s2	UNUSED	UNUSED
	c0t1d0s3	/var/crash	=swap allocation or more depending on number of desired system cores saves.
	c0t1d0s4	/home	$ (remaining)
	c0t1d0s5	UNUSED	UNUSED
	c0t1d0s6	UNUSED	UNUSED
	c0t1d0s7	UNUSED	UNUSED

System and Environment Information

The Server

Server Type: Ultra-5
Physical Memory: 256 MB RAM
Local Storage: 2x9 GB Hard Disks (Internal)
Peripherals: Serial Console (Actually a Linux Laptop running minicom with a Null Modem Cable)
Network Card(s): 10/100 Mb Ethernet
Server Function: Apache 1.3.9 Web Server

Physical Security

Data Center with Electronic Badge Access and Man Trap
Locked Cabinet
No attached Keyboard and Mouse (Headless System)
Data Center installed contingency (e.g. Halon, battery backup. . .)

Tracking / Audit

Task	Completed By	Date	Audited By	Date	Comments
Physical Security					
Initial Install (Core OS)					
Software CD 1 of 2					
SUNWntpr & SUNWntpu					
SUNWlibms					
SUNWxwrtl, SUNWxwfnt, SUNWxwice, SUNWxilrl, SUNWxildh, SUNWxilow, SUNWtltk, SUNWxwplt, SUNWctpls, SUNWmfrun, SUNWxwopt, SUNWxwcft, SUNWdtbas					
SUNWscpu					
SUNWlibC, SUNWdoc					
SUNWadmc, SUNWadmap					
Software CD 2 of 2					
SUNWman, SUNWast, SUNWgzip					
Current Patch Cluster					
Removed Startup Scripts (/etc/rc2.d)					
S30sysid.net					
S71sysid.sys					
S72autoinstall					
S71rpc					
S73nfs.client					
S74autofs					
S73cachefs.daemon					
S71ldap.client					
S80PRESERVE					
S88sendmail					
Removed Startup Scripts (/etc/rc3.d)					
S15nfs.server					
Removed Startup Scripts (/etc/rcS.d)					
(Optional) S50devfsadm					

Set UMASK for startup. /etc/rc?.d/S00umask.sh			
Set Network Parameters for Security.			
Protect the Root Filesystem.			
Modify /etc/init.d/inetsvc			
/etc/default/telnetd created.			
/etc/default/ftpd created.			
Modify /etc/mail/sendmail.cf.			
Modify the system Kernel.			
Modify syslog.conf			
Only root and sys crontabs exist.			
Mode 600 on /etc/cron.d/cron.allow and /usr/lib/cron/at.allow			
Group = sys on cron.allow and at.allow.			
Set the Default Route			
Removed auto_home and auto_master.			
Updated root's crontab.			
Updated sys' crontab.			
ASET configured.			
SAVECORE configured.			
System accounts uucp, nuucp, smtp, and listen removed.			
Shell = /dev/null for system accounts daemon, bin, sys, adm, lp, nobody, noacess, and nobody4			
Modify /etc/nsswitch.conf for DNS lookup.			
Configure Sendmail to run from cron.			
Modify /etc/vfstab.			
/etc/motd and /etc/issue created with permissions 444.			
Optional: Modify			

/etc/default/passwd.			
Configure xntpd			
Enable BSM (system Audit)			
Additional Products			
Libpcap			
Sudo			
nmap			
lsof			
Logrotate			
Tcp_wrappers			
OpenSSH			
Configure SSH Server Include keygen and startup script in /etc/rc2.d			
/usr/local/bin/* permissions = 750			
/usr/local/bin/sparcv7/* permissions = 750			
/usr/local/bin/sparcv9/* permissions = 750			
OpenSSH configured			
Tcp_wrappers configured			
Logrotate configured			

Initial Install

1.0 Getting Started

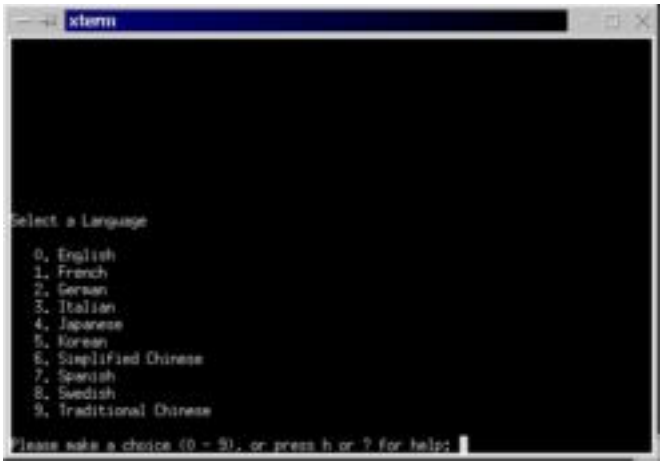
1. Ensure the system to be installed **is not connected to the network**. It is generally a good idea NOT to install a new system while connected to the network.
2. Power the system up. The system will likely attempt to boot from the network of the boot disk. If this is the case and you are in front of a Sun Keyboard use the <stop> <a> key sequence to obtain the **ok** prompt.
3. Insert Solaris 8 Software CD 1 of 2 into the CD/ROM or DVD drive.
4. At the OK Prompt type boot cdrom

   ok boot cdrom

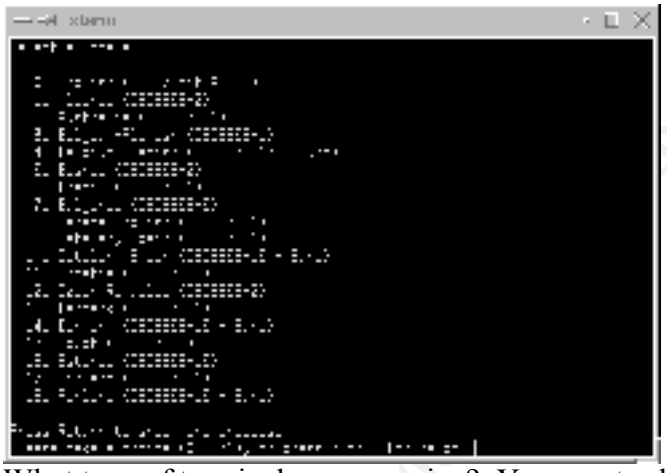
2.0 System Identification

2.1 Language and Locale

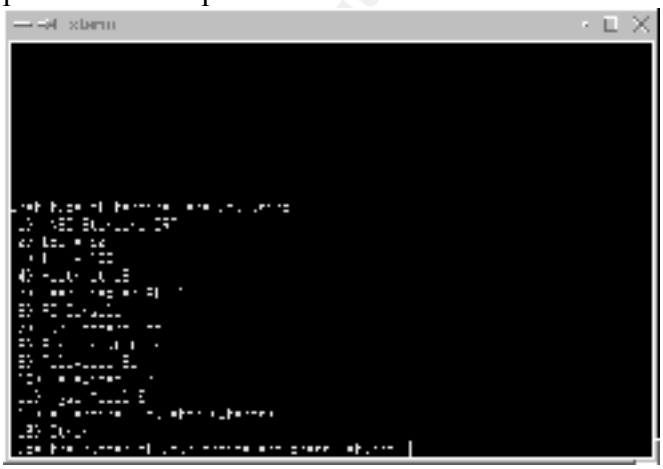
1. Select a Language.



2. Select a Locale.



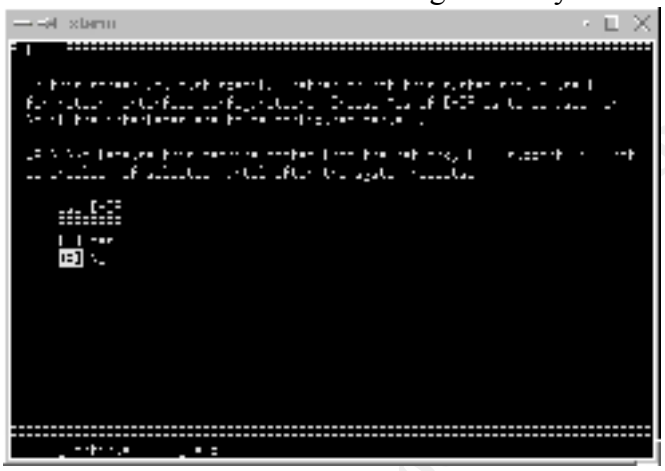
3. What type of terminal are you using? You must select the appropriate terminal when installing via a console. If you fail to select the correct terminal type the installation process will be painful one.



2.2 Network Configuration

1. Is this system connected to the network? The system should not be connected to the network at this point; however, you should still answer yes. You will receive an error message. This message is simply stating that at this time the interface can not reach the network.

2. Would like to use DHCP to configure the system network interface.



3. Server's hostname. This information should have been gathered during pre-work.

4. Enter the IP address for the server. This information should be found in your pre-work.

5. Solaris 8 supports IPv6. Would you like to enable IPv6?

6. Confirm your settings for this portion. If all the settings are correct continue. Otherwise you may select to go back; however, should you select to go back you will be asked to enter all the network information again.

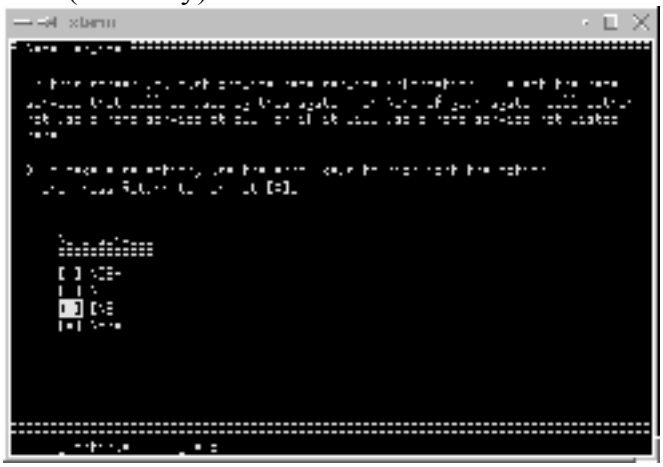
2.3 Security Policy

1. Would you like to configure Kerberos?

2. This completes the security policy section. You will now be asked to confirm the information and continue.

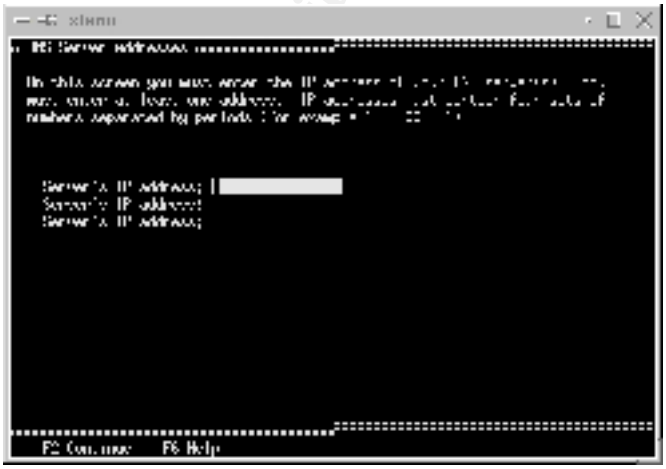
2.4 Configure the Name Service

1. Select the Name service you will be using. If you would like to configure DNS at a later time (manually) or not use a name service select None.

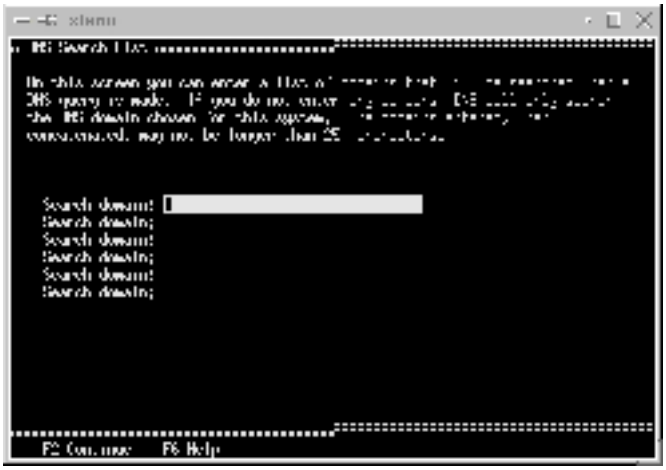


2. Enter the domain name for your system.

3. Enter the DNS Name Server addresses. This should be in the form of an IP address.



4. Enter the domains to search in the space available.



5. You have now completed the Name Service portion. You will be asked to confirm your configuration and then continue.

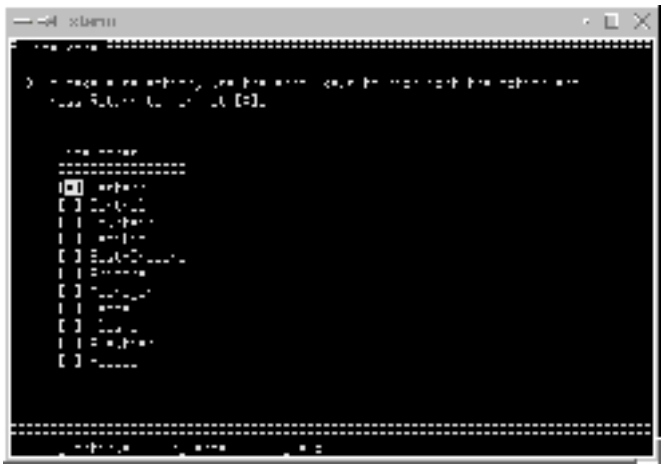
2.5 Time Zone

You are now at the final portion of the System Identification portion of the install.

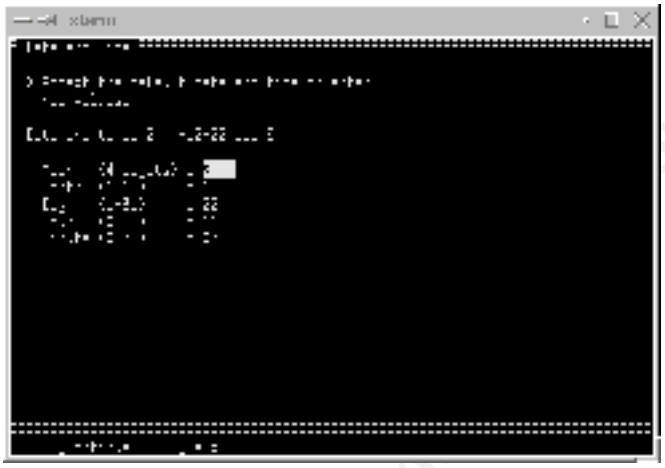
1. Is this system part of a subnet.
2. If you answered yes to the previous question you will now be asked to enter the netmask for this system.

3. Select your Time Zone Region.

4. Select the Time Zone.



5. Set the date and time.



6. At this point you have configured all the data and time settings. You will now be asked to confirm these settings and continue.

   Note: Once you select continue, you will receive a network error. This is expected because the system is not connected to the network.

3.0 Installation Options

With the system identification section complete the process moves onto the installation options portion. In this section we will define the install type, geographic regions to support, software bundle to install, and disks to use and filesystem layout for those disks.

3.1 Install Type and Geographic Region Support

1. What type of install will this be?

Use the function key <f4> or <esc> +<4> to select Initial install.

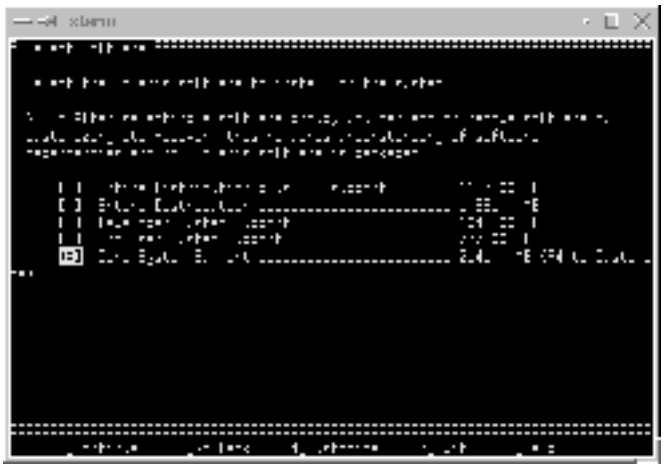
2. The next screen will simply be notes related to the interactive install type. Continue to the next step.
3. Select the Geographic Regions you wish to support.

Use the space bar to place X next to each region you wish to install support for.

4. Solaris 8 supports both 32 bit and 64 bit install types. You will now select whether you wish to install Solaris 8 in 64 bit mode or not.

3.2 Select Software

1. Select which software set you wish to install. You should keep in mind that more is easier, but less is more secure. Because we are installing this server to be secure we will select the smallest install set – Solaris **Core System Support.**



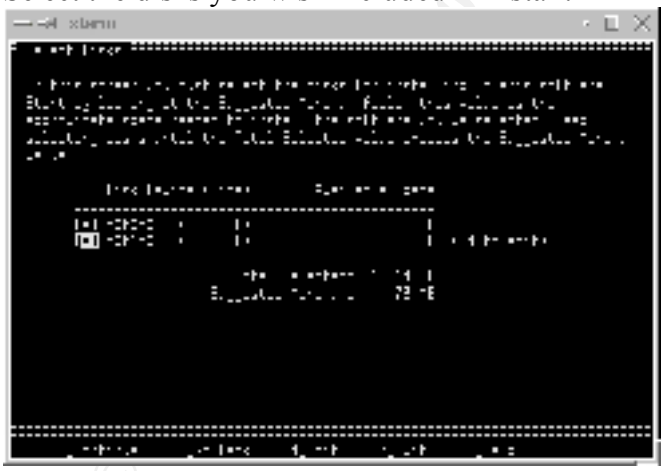
Note: Some applications may not work with this install and additional packages need to be added. Additional packages will be added later in this install. However, at no point will the packages required to run Oracle be installed.

3.3 Disk Configuration

1. Select the disks to be included in this install. In this process we had two disks, c0t0d0 and c0t1d0. Common disk configurations are as follows:

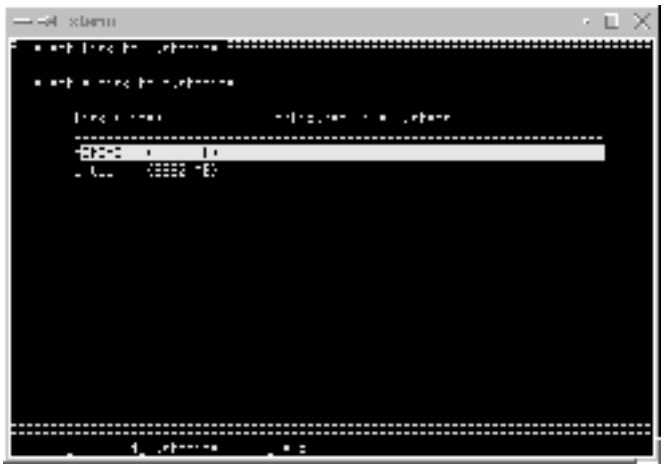
Disk	Disk Label
Disk0	c0t0d0 (Sun4u) c0t3d0 (Sun4m)
Disk1	c0t1d0 c0t8d0 (Sun E250)

2. Select the disks you wish included in install.



Use the space bar to place an X next to the disks you wish to use. <F2> or <esc> +<2> will take you to the next window.

3. Once you have selected the disks you will need to choose to preserve existing data or not to. You will also be asked to select a manual disk lay out process or an auto_layout process.

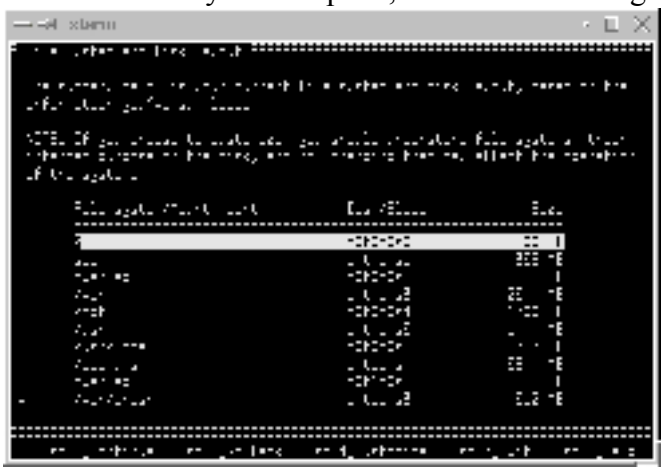


You will likely select Manual Layout. You will then to highlight (select) a disk followed by <f4> or <esc> +<4> to customize that disk. Disk layouts will vary. The layout used in this process is found in the pre-work section.

Below is a screenshot for the "Customize Disk" window for disk0 and disk1.

Note: In this configuration backups will be done using ufsdump to the /backups directory. To restore a primary boot disk you must have /, /opt, /var, /usr filesystems backups. Your backups / restore process for the primary boot disk may differ.

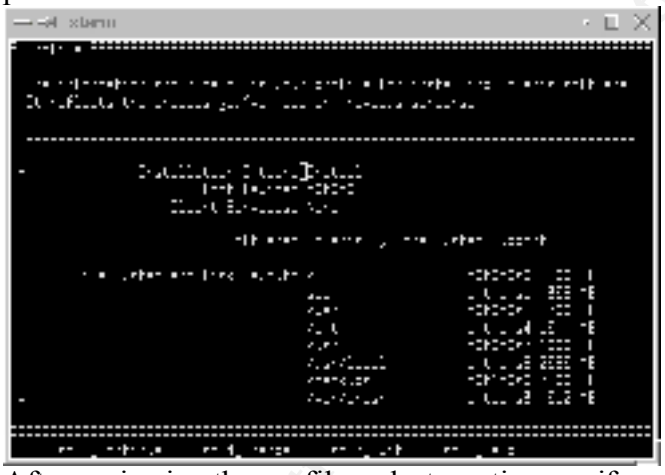
4. With the disk layout complete, confirm the settings and continue.



5. Would you like to mount a remote filesystem? <NO>

3.4 Final Review and Installation Begins

1. We are now closing the configuration section. Now you must confirm your install profile.



After reviewing the profile, select continue or if you have found any problems select to change.

2. Would you like the system to auto reboot? <YES>
3. Installation Begins!

Post - Install

Once the install process has completed you will login to the console as root with no password. Once logged in you will be prompted to set root's password.

Introduction

In this section we will cover the installation of select software and the customization of the environment. We will also cover patching the system; however, prior to that we must install other Sun software from the media.

4.0 Additional Sun Software

Will install the following additional products from the available Sun media.

Product	Packages
Network Time Protocol	SUNWntpr SUNWntpu

Sun Workshop Bundled libm	SUNWlibms
X Client Software	SUNWxwrtl SUNWxwfnt SUNWxwice SUNWxirl SUNWxildhl SUNWxilow SUNWtltk SUNWxwplt SUNWctpls SUNWmfrun SUNWxwopt SUNWxwcft SUNWdtbas
Berkley Style Binaries	SUNWscpu
Document Tools	SUNWdoc
System Admin Applications	SUNWadmc SUNWadmap
System Accounting Tools	SUNWaccr SUNWaccu
Man Pages	SUNWman
ASET	SUNWast
GZip	SUNWgzip

4.1 Install Sun Products Software CD 1 of 2

1. Insert Sun Software CD 1 of 2.
2. Make a directory to act as the mount point. A good choice is /cdrom.
   mkdir /cdrom
3. mount -r -f hsfs /dev/dsk/c0t2d0s0 /cdrom
   Note: Your device may not be c0t2d0.
4. cd /cdrom/Solaris_8/Product
   Note during this process you will be prompted with warnings and continue. You will need to enter <y> to continue.
5. Install the Network Time Protocol.
   pkgadd -d . SUNWntpr SUWNntpu
6. Install the Workshop libm.
   pkgadd -d . SUNWlibms
7. Install the Xclient software, this will include such applications as dtterm and xterm.
   pkgadd -d . SUNWxwrtl SUNWxwfnt SUNWxwice SUNWxirl SUNWxildhl SUNWxilow SUNWtltk SUNWxwplt SUNWctpls SUNWmfrun

   pkgadd -d . SUNWxwopt SUNWxwcft SUNWdtbas
   Note: Due to line length limitations we divided this step into two separate commands.
8. Install the Berkley Binaries.
   pkgadd -d . SUNWscpu
9. Install the Document Tools.
   pkgadd -d . SUNWlibc SUNWdoc
10. Install the Admin tool set.
    pkgadd -d . SUNWadmc SUNWadmap
11. Eject the Software CD 1 of 2.
    cd /
    umount /cdrom
    The CD should now be ready to be removed.

4.2 Install Sun Products Software CD 2 of 2

1. Insert Sun Software CD 2 of 2.

2. mount -r -F hsfs /dev/dsk/c0t2d0s0 /cdrom
3. cd /cdrom/Solaris_8/Product
   Note: Again you will be prompted with warnings. You should enter <y> to continue the install.

4. Install man pages and ASET.
   pkgadd -d . SUNWman SUNWast SUNWgzip
5. Remove the Software CD 2 of 2
   cd /
   umount /cdrom
   The CD should now be ready to be removed.

4.3 Install Current Patch Cluster

This process will vary depending on how you obtained or but what means you have the patch cluster available to you. For the purpose of this process our patch cluster was obtained via a download and then "burned" to CD by a CD/R device. For this reason the process will follow as an install from CD. Because the system should not be on the network at this point this would be the easiest approach.

1. Take the system to single user mode.
   /etc/telinit S
2. Insert the CD into the CD/ROM device. (This should be the CD with the current recommended and security patch cluster.)
3. mount -r -F hsfs /dev/dsk/c0td2d0s0 /cdrom
4. cd /cdrom/8_recommended
5. ./install_cluster –q
   This process will take a couple of minutes, depending on number of installed products requiring a fix and the number and size of fixes in the current cluster.

4.4 Modify Startup Scripts

When a Solaris system starts up, many processes will start that both are un-necessary for most Internet servers and could introduce security issues. For this reason, in this process we will eliminate the processes, which are not required for a Web Server.

The following processes can be eliminated. How they are eliminated is really a matter of personal preference. This process demonstrates the process of hiding the scripts. This will allow the scripts to be easily re-instated should they be required at a later time.

/etc/rc2.d

S30sysid.net S71sysid.sys S72autoinstall S71rpc S73nfs.client S74autofs S73cachefs.daemon S71ldap.client S80PRESERVE S88sendmail

The nscd startup script, though questionable, will likely need to be left. This is because Netscape uses the Name Service Cache Daemon.

/etc/rc3.d

S15nfs.server

/etc/rcS.d

S50devfsadm

Note: Only remove this script if you are not planning to use hot-plug devices. In this

process we removed it because the server does not support hot-plug devices.

The Process

For each of the scripts listed above execute the following steps.

1. cd /etc/rc?.d
2. mv S##script .OLDS##script
   i.e. mv S30sysid.net .OLDS30sysid.net
3. Repeat step two for each script in the related rc directory. When finished with that directory move to the next rc, start at step 1.

4.5 Set umask for System Daemons

1. echo 'umask 022' > /etc/init.d/umask.sh
2. chmod 544 /etc/init.d/umask.sh
3. ln -s ../init.d/umask.sh /etc/rcS.d/S00umask.sh
   ln -s ../init.d/umask.sh /etc/rc1.d/S00umask.sh
   ln -s ../init.d/umask.sh /etc/rc2.d/S00umask.sh
   ln -s ../init.d/umask.sh /etc/rc3.d/S00umask.sh
   ln -s ../init.d/umask.sh /etc/rc0.d/S00umask.sh

4.6 Setup Network Parameters for Security

1. cd /etc/init.d
2. vi inetsvc
3. Modify the file so that the file appears as below:

```
#!/bin/sh
#
#ident  "@(#)inetsvc 1.16 97/04/17 SMI"
#
# This system is not a NIS participant or a DNS server.
#

/usr/sbin/ifconfig -auD netmask + broadcast +

#
#/usr/sbin/inetd -s
```

4. mv /etc/inetd.conf /etc/.OLDinetd.conf
5. Edit the /etc/init.d/inetinit file. The following lines should be added to the end of this file. These settings change the way the system will interact on the network. Some key things these settings will do are; stop IP forwarding, set the ARP cache cleanup interval, and increase the maximum number of requested connections.

```
#
# Set network configuration for security.
#
ndd -set /dev/tcp tcp_conn_req_max_q0 8096
ndd -set /dev/tcp tcp_conn_req_max_q 1024
ndd -set /dev/tcp tcp_ip_abort_cinterval 60000
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip_ire_arp_interval 60000
ndd -set /dev/arp arp_cleanup_interval 60000
ndd -set /dev/ip ip_forward_src_routed 0
ndd -set /dev/ip ip_forward_directed_broadcasts 0
ndd -set /dev/ip ip_forwarding 0
ndd -set /dev/ip ip_strict_dst_multihoming 1
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
ndd -set /dev/ip ip_respond_to_timestamp_broadcast 0
ndd -set /dev/ip ip_respond_to_address_mask_broadcast 0
ndd -set /dev/ip ip_ignore_redirect 1
ndd -set /dev/ip ip_send_redirects 0
ndd -set /dev/ip ip_respond_to_timestamp 0
ndd -set /dev/tcp tcp_smallest_nonpriv_port 3050
```

4.7 Modify Remote System Information

1. vi /etc/default/telnetd and add the following line.
   BANNER="Unlisted OS"
2. vi /etc/default/ftpd and add the following line.
   BANNER="Unlisted OS"
3. Modify /etc/mail/sendmail.cf so that following lines appear as below:

```
# SMTP initial login message (old $e macro)
O SmtpGreetingMessage=Mail Server Ready
```

4.8 Protect the Root Filesystem

1. cd /
2. mkdir /root
3. chmod 750 /root
4. chown root:root /root
5. passmgmt –m –h /root root
6. There should be no .$$$ files, i.e. environment files. However, if there are you should move these environment files to the new root home directory.

4.9 Modifying the Kernel

In this section we will cover two items. The first, making the system stack non-executable and the second, preventing the creation of core files.

1. vi /etc/system
   add the following lines:

```
set noexec_user_stack = 1
set noexec_user_stack_log = 1
```

2. If this is to be a production system you may want to disallow the creation of core files.
   vi /etc/system
   add the following line:

```
set sys:coredumpsize = 0
```

4.10 Modify Syslog

1. vi /etc/syslog.conf

2. Modify the file to your desired configuration. The example below reflects a suitable example for a system that will not use syslog to forward messages to other servers. Instead all files are local and we have opted to single out the local2.notice entries as this is the facility and log level which sudo uses.

```
#ident  "@(#)syslog.conf        1.5     98/12/14 SMI"   /* SunOS 5.0
*/
#
#
*.notice;mail.none;local2.none;kern.notice      /var/adm/messages
local2.notice                   /var/adm/local2.log
auth.*          /var/log/auth.log
mail.info       /var/log/sys.log
```

3. touch /var/adm/local2.log
4. touch /var/log/auth.log
5. touch /var/log/sys.log
6. chown root:sys /var/adm/local2.log /var/log/auth.log /var/log/sys.log /var/adm/messages
7. chmod 600 /var/adm/local2.log /var/log/auth.log /var/log/syslog /var/adm/messages

4.11 Modify Crontab & AT Configuration

1. Remove unused crontabs. In this configuration you should only have a crontab for root and sys.
   cd /var/spool/cron/crontabs
   Verify only root and sys crontabs exist. Remove others that may exist.
2. Modify the /etc/cron.d/cron.allow file to include the root and sys user.
   vi /etc/cron.d/cron.allow

```
root
sys
```

3. chgrp sys /etc/cron.d/cron.allow
4. chmod 600 /etc/cron.d/cron.allow
5. mv /usr/lib/cron/at.deny /usr/lib/cron/.OLDat.deny
6. touch /usr/lib/cron/at.allow
7. chgrp sys /usr/lib/cron/at.allow
8. chmod 600 /usr/lib/cron/at.allow

4.12 Set the Default Router

1. vi /etc/defaultrouter
   Add a single line, the IP address of the default router.

```
100.100.100.254
```

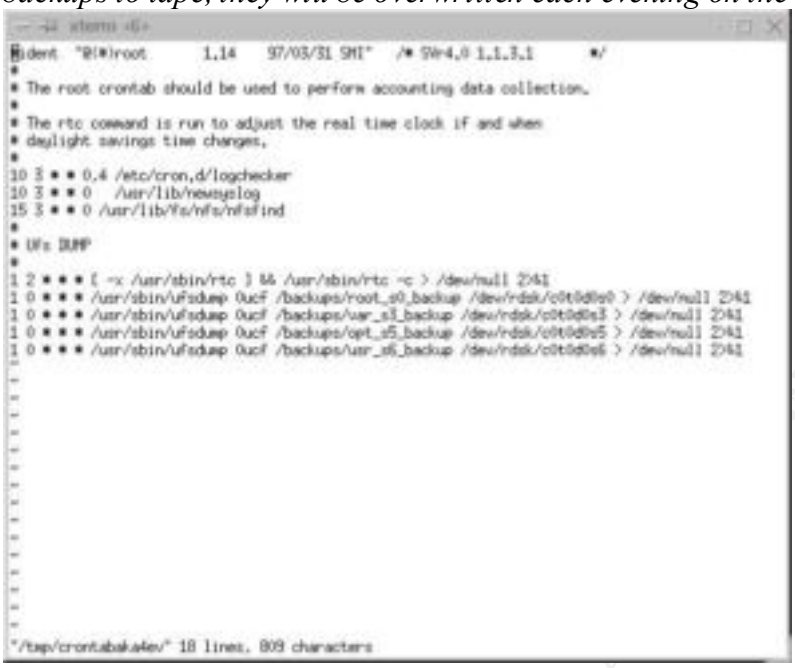
4.13 Move auto_home and auto_master

1. cd /etc
2. mv auto_home .OLDauto_home
3. mv auto_master .OLDauto_master

4.14 Edit root's crontab

1. EDITOR=vi export EDITOR
2. crontab –e
3. Add the following lines as they appear in the image below to complete nightly backups of

critical filesystems. *Note: A separate network backup solution should archive these backups to tape, they will be overwritten each evening on the local disk.*



4.15 Configure ASET

1. /usr/aset/aset -l high -p
   Note: This configures aset to run on regular basis out of CRON with level set equal to high.
2. Remove the /etc/rc2.d/S69inet.asetoriginal file.
   # mv /etc/rc2.d/S69inet.asetoriginal /etc/rc2.d/.OLDS69inet.asetoriginal

4.16 Edit Crontab for Sys

1. crontab -e sys
   Add the following lines for performance. (SAR configuration)

```
0 * * * 0-6 /usr/lib/sa/sa1 300 12
58 23 * * 1-5 /usr/lib/sa/sa2 -i 300 -A
```

4.17 Configure the savecore function of Solaris

At this point we will now configure the system to save "system core" files generated in the event of a system crash.

1. dumpadm –c all –d /dev/dsk/c0t0d0s1 –m 1m –s /var/crash/`hostname`
2. mkdir /var/crash/`hostname`
3. Use dumpadm with no parameters to verify settings.

4.18 Modify / Remove Default System Accounts

1. Execute the following to remove user ids that are not needed.

```
for user in uucp nuucp smtp listen
do
passmgmt –d $user
done
```

2. Execute the following to set system users to have no shell.

```
for user in daemon bin sys adm lp nobody noacess nobody4
do
passmgmt –m –s /dev/null $user
done
```

4.19 Edit /etc/nsswitch.conf (This step can be skipped if DNS is not Used.)

1. Edit the nsswitch.conf file. Most configurations are likely to use DNS as configured at install.
   vi /etc/nsswitch.conf
2. Modify the hosts line so that it appears as below:

```
hosts        files [NOTFOUND=continue] dns [NOTFOUND=return]
```

3. Save changes and exit the file.

4.20 Configure Sendmail to Run From CRON

1. Edit root's crontab
   crontab -e
2. Add the following lines to the end of the file.

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

4.21 Configure /etc/vfstab

1. Edit /etc/vfstab
   vi /etc/vfstab
2. Configure the vfstab file to look similar to the one below.

```
#device         device          mount           FS      fsck    mount   mount
#to mount       to fsck         point           type    pass    at boot options
#
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr          ufs     1       yes     -
fd      -       /dev/fd fd      -       no      -
/proc   -       /proc   proc    -       no      -
/dev/dsk/c0t0d0s1       -       -       swap    -       no      -
/dev/dsk/c0t0d0s0       /dev/rdsk/c0t0d0s0      /       ufs     1       no      -
/dev/dsk/c0t0d0s5       /dev/rdsk/c0t0d0s5      /usr    ufs     1       no
ro,nosuid
/dev/dsk/c0t0d0s3       /dev/rdsk/c0t0d0s3      /var    ufs     1       no
nosuid,logging
/dev/dsk/c0t1d0s0       /dev/rdsk/c0t1d0s0      /backups        ufs     2       yes
nosuid,logging
/dev/dsk/c0t1d0s4       /dev/rdsk/c0t1d0s4      /home   ufs     2       yes
nosuid,logging
/dev/dsk/c0t0d0s4       /dev/rdsk/c0t0d0s4      /opt    ufs     2       yes
nosuid,ro
/dev/dsk/c0t0d0s6       /dev/rdsk/c0t0d0s6      /usr/local      ufs     2       yes
ro
/dev/dsk/c0t1d0s3       /dev/rdsk/c0t1d0s3      /var/crash      ufs     2       yes
nosuid,logging
swap    -       /tmp    tmpfs   -       yes     -
```

– Set /usr, /var, /opt, /home, and /var/crash to have nosuid.
Do not place nosuid on /usr/local or /
– Set /usr, /opt, and /usr/local to be read-only
– Set /var, /backups, /home, /var/crash to have logging

4.22 Create /etc/motd and /etc/issue

1. Edit /etc/motd
   vi /etc/motd
2. Insert lines similar to those below. You may need to bring the legal department in on this area to determine the correct wording.

```
**************************************************************************
* This is a private network for authorized uses by authorized users only.*
* Unauthorized access attempts are subject to legal prosecution.         *
* Individuals using this system are subject to having their activities   *
* monitored and anyone using this system expressly consents to such      *
* monitoring.                                                            *
**************************************************************************
```

Note: Be sure that a carriage returned is entered at the end of the last line.

3. Save and exit this file.
4. Edit /etc/issue
   vi /etc/issue
5. Insert lines similar to those below. Again the actual wording should be worked out with your legal department.

```
**************************************************************************
* THIS IS A PRIVATE NETWORK FOR AUTHORIZED USES BY AUTHORIZED USERS ONLY.*
* UNAUTHORIZED ACCESS ATTEMPTS ARE SUBJECT TO LEGAL PROSECUTION.         *
**************************************************************************
```

Note: Be sure that a carriage return is entered at the end of the last line.

6. Save and exit this file.
7. chmod 444 /etc/issue /etc/motd

4.22 Modify /etc/default/passwd

Consider This

Before changing /etc/default/passwd keep in mind that the first time a user, including root, changes their password they will inherit these new default settings. What this means is in a large environment you may be spending a great deal of time changing root passwords as they expire.

Instead of implementing the /etc/default/passwd a you may use the passwd command with -x (MAXWEEKS), -m (MINWEEKS) and -w (WARNWEEKS) flags.

Modifying /etc/default/passwd

1. vi /etc/default/passwd
2. Update the file so that it looks similar to the one below.

```
#ident  "@(#)passwd.dfl 1.3     92/07/14 SMI"
MAXWEEKS=4
MINWEEKS=1
WARNWEEKS=1
PASSLENGTH=6
```

This simply states that user passwords will expire every 28 days (4 weeks). A user must allow their password to age 1 week prior to changing it again. Users will be warned one week in advance that their password is about to expire. The final setting is the minimum length of user passwords. Because Solaris only looks at the first 8 characters, we set this to 6. This allows users to manipulate their passwords somewhat and takes away the assumption that all user passwords will be 8 characters. The less information an intruder has the better.

4.23 Configure xntpd

1. Change directory to /etc/inet
   # cd /etc/inet
2. Edit the ntp.conf file.
   # vi ntp.conf

3. Edit the file to look the one found below. Simply change the time servers to meet your needs. *If you need further information on the Network Time Protocol you can view the*

```
driftfile /etc/inet/ntp.drift

server 127.127.1.1
fudge 127.127.1.1 stratum 8

server 100.100.100.100
server 100.100.100.101
server 100.100.100.102

restrict default nomodify
```

man pages or go to www.ntp.org. This file is suited for those systems that will use the network to synchronize time.
Save and exit the file when you are finished updating it.
4. Create the ntp.drift file.
touch /etc/inet/ntp.drift

4.24 Enable BSM (System Audit)

1. As root execute the bsmconv command to enable the Basic Security Module.
cd /etc/security
./bsmconv
2. You will be prompted to answer questions to proceed.
3. Once enabled you will need to configure what actually will be audited. You should use caution here as too much auditing will cause the system disks to fill up rapidly.
Modify the /etc/security/audit_control file as required. An example of a good starting point is found below:

```
flags:lo,ad,-all,^-fc
naflags:lo,nt
minfree:20
dir:/etc/security/audit/webserver/files
```

5.0 Additional Security Software and Tools

We will no proceed with the installation of additional software. This software is available from the www.sunfreeware.com site. The software here is packaged based on platform and Solaris release and is compiled and ready to install. You may also obtain the source code from the site for each of the products.

5.1 Before You Start

Download the following software from the www.sunfreeware.com web site and have them copied to CD/R media. This is the easiest manner by which to get these products installed.
libpcap-200.11.28-sol8-sparc-local
logrotate-3.3-sol8-sparc-local
lsof-4.49-sol8-sparc-64-local (For 64bit installed servers only)
nmap-2.54BETA7-sol8-sparc-local
openssh-2.2.0p1-sol8-sparc-local
tcp-wrapprs-7.6-sol8-sparc-local
sudo-1.6.3p5-sol8-sparc-local
With the CD media created in advance proceed. You may proceed to the first product install

process if your current patch cluster and the additional software from above are on the same media.

1. If /cdrom is mounted un-mount and remove the media, likely your current patch cluster CD.
   # cd /
   # umount /cdrom
   eject CD and remove.
2. Mount the CD with the additional software.
   Insert CD into drive.
   # mount -r -F hsfs /dev/dsk/c#t#d#s0 /cdrom

All of the products installed at this point will be installed into the /usr/local directory tree.

5.2 Install "libpcap"

1. Go to the /cdrom directory.
   # cd /cdrom
2. Install the libpcap-200.11.28-sol8-sparc-local
   # pkgadd –d libpcap-200.11.28-sol8-sparc-local
3. Select "y" when prompted, to **all** questions, to proceed.

5.3 Install "sudo"

1. Change directory to /cdrom
   # cd /cdrom
2. Install the sudo-1.6.3p5-sol8-sparc-local package.
   # pkgadd -d sudo-1.6.3p5-sol8-sparc-local
   Note: You may receive Attribute warnings, ignore these warnings and continue.
3. Select "y" when prompted, to **all** questions, to proceed.
4. Set your MANPATH to include /usr/local/man.
   # MANPATH=$MANPATH;/usr/local/man export MANPATH
5. Use the man pages for sudo and visudo to configure sudo policies. This is critical as with nosuid the su command will not work. To execute su, sudo and corresponding policies will have to be used.

5.4 Install "nmap"

1. If you are not already in the /cdrom directory go there now.
   # cd /cdrom
2. Install the nmap-2.54BETA7-sol8-sparc-local
   # pkgadd –d nmap-2.54BETA7-sol8-sparc-local
3. Select "y" when prompted, to **all** questions, to proceed.

5.5 Install "lsof" (Solaris 8 installed in 64Bit Mode)

1. You should still be in the /cdrom directory. If not go there now.
   # cd /cdrom
2. Install the lsof-4.49-sol8-sparc-64-local
   # pkgadd -d lsof-4.49-sol8-sparc-64-local
3. Answer "y" when prompted to continue with the install.

5.6 Install "logrotate"

1. You should still be in the /cdrom directory. If not go there now.
   # cd /cdrom
2. Install the logrotate-3.3-sol8-sparc-local
   # pkgadd -d logrotate-3.3-sol8-sparc-local

3. Answer “y” when prompted to continue with the install.
4. The man pages for logrotate and logrotate.conf provide great information for how to configure the logrotate facility.
5. Once configured, modify the crontab for root.
   Remove the newsyslog line all together.
6. Add a line for logrotate to execute at given time.
   An example might be:
   0 * * * * /usr/local/bin/logrotate /usr/local/etc/logrotate.cf 2>&1
7. Save and exit the file.
8. This should complete your root crontab updates entirely and the final crontab should look something like the one below.

5.7 Install “tcp_wrappers”

1. Go to the /cdrom directory.
   # cd /cdrom
2. Install the tcp-wrapprs-7.6-sol8-sparc-local
   # pkgadd -d tcp-wrapprs-7.6-sol8-sparc-local
3. Select “y” when prompted, to **all** questions, to proceed.
4. At this point you must now configure Tcp_Wrappers.
   # vi /usr/local/etc/hosts.allow
   Add a line similar to the below:
   ALL: <network>
5. Save and exit the file.
6. Modify the /usr/local/etc/hosts.deny file.
   # vi /usr/local/etc/hosts.deny
   Add the following line:
   ALL: ALL: /usr/bin/mailx –s “%s: connection attempt from %a” \
   root@somedomain.com
7. Change ownership and permissions on the configuration files:
   # chown root:root /usr/local/etc/hosts.allow /usr/local/etc/hosts.deny

chmod 600 /usr/local/etc/hosts.allow /usr/local/etc/hosts.deny

5.8 Install "OpenSSH"

1. Go to the /cdrom directory.
   # cd /cdrom
2. Install the openssh-2.2.0p1-sol8-sparc-local
   # pkgadd -d openssh-2.2.0p1-sol8-sparc-local
3. Select "y" when prompted, to **all** questions, to proceed.
4. Generate the server key file:
   # /usr/local/bin/ssh-keygen –b 1024 –N '' –f /usr/local/etc/ssh_host_key
5. Configure the SSH server.
   Create a configure file in /usr/local/etc, name it sshd_config.
   # vi /usr/local/etc/sshd_config

```
Port 22
ListenAddress 0.0.0.0
PidFile /usr/local/etc/sshd.pid
SyslogFacility AUTH
FascistLogging yes

HostKey /usr/local/etc/ssh_host_key
KeyRegenerationInterval 900
RandomSeed /usr/local/etc/ssh_random_seed
ServerKeyBits 1024

CheckMail no
KeepAlive no
PrintMotd no
QuietMode no
SilentDeny no

PermitRootLogin no
IgnoreRhosts yes
RhostsAuthentication no
RhostsRSAAuthentication no
PasswordAuthentication yes
PermitEmptyPasswords no
RSAAuthentication yes
StrictModes yes
UseLogin no
LoginGraceTime 180
```

6. Change ownership and permissions on the SSD server configuration file.
   # chown root:root /usr/local/etc/sshd_config
   # chmod 600 /usr/local/etc/sshd_config
7. Create the start-up script for sshd.

```
#!/bin/sh

case "$1" in
'start')
    if [ -x /usr/local/sbin/sshd –a –f /usr/local/etc/sshd_config ]; then
          /usr/local/sbin/sshd
     fi
     ;;
'stop')
     /usr/bin/kill `cat /usr/local/etc/sshd.pid`
          ;;
*)
         echo "Usage: $0 {start | stop}"
         ;;
esac
exit 0
```

vi /etc/init.d/sshd
An example sshd startup file is below.
Save and exit the file.

8. Change permissions on the file.
   # chmod 740 /etc/init.d/sshd
9. Create link to sshd startup in the /etc/rc2.d directory.
   # cd /etc/rc2.d
   # ln –s ../init.d/sshd S75sshd
10. Verify the script works.
    # /etc/rc2.d/S75sshd start

5.9 Modify Permissions

1. Remove all rights from "other" on all new files in /usr/local/bin, include sub-directories.
   # chmod –R o-rwx /usr/local/bin/*

6.0 Install Complete

6.1 Final System Reboot

/etc/telinit 6

Last Updated: September 22nd, 2017

Upcoming Training

SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**