

## JHNS Solaris 7 Set-up Checklist

<input type="checkbox"/>	<p>Install operating system (DO NOT ATTACH TO NETWORK)</p> <p>Create separate file systems for:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;"><input type="checkbox"/> /</td> <td style="width: 50%;"><input type="checkbox"/> /usr</td> </tr> <tr> <td><input type="checkbox"/> /usr/local</td> <td><input type="checkbox"/> /export/home</td> </tr> <tr> <td><input type="checkbox"/> swap</td> <td><input type="checkbox"/> /opt</td> </tr> </table> <p>Reason for non-standard file system layout:</p> <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	<input type="checkbox"/> /	<input type="checkbox"/> /usr	<input type="checkbox"/> /usr/local	<input type="checkbox"/> /export/home	<input type="checkbox"/> swap	<input type="checkbox"/> /opt
<input type="checkbox"/> /	<input type="checkbox"/> /usr						
<input type="checkbox"/> /usr/local	<input type="checkbox"/> /export/home						
<input type="checkbox"/> swap	<input type="checkbox"/> /opt						
<input type="checkbox"/>	<p>Configure networking:</p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%;"><input type="checkbox"/> Touch /etc/notrouter</td> <td style="width: 50%;"><input type="checkbox"/> Create /etc/defaultrouter</td> </tr> <tr> <td><input type="checkbox"/> Create /etc/resolv.conf</td> <td><input type="checkbox"/> Edit /etc/netmasks</td> </tr> <tr> <td><input type="checkbox"/> Edit /etc/nsswitch.conf</td> <td></td> </tr> </table>	<input type="checkbox"/> Touch /etc/notrouter	<input type="checkbox"/> Create /etc/defaultrouter	<input type="checkbox"/> Create /etc/resolv.conf	<input type="checkbox"/> Edit /etc/netmasks	<input type="checkbox"/> Edit /etc/nsswitch.conf	
<input type="checkbox"/> Touch /etc/notrouter	<input type="checkbox"/> Create /etc/defaultrouter						
<input type="checkbox"/> Create /etc/resolv.conf	<input type="checkbox"/> Edit /etc/netmasks						
<input type="checkbox"/> Edit /etc/nsswitch.conf							
<input type="checkbox"/>	<p>reboot</p>						
<input type="checkbox"/>	<p>kill -KILL all, but the following processes:</p> <pre># ps -ef   UID    PID  PPID  C   STIME TTY      TIME CMD   root     0     0  0   Oct 19 ?        0:00 sched   root     1     0  0   Oct 19 ?        0:31 /etc/init -r   root     2     0  0   Oct 19 ?        0:00 pageout   root     3     0  0   Oct 19 ?        0:54 fsflush   root    199     1  0   Oct 19 console 0:00 /usr/lib/saf/ttymon -g -h -p nsl console login: -T sun -d /dev/console -l cons   root    129     1  0   Oct 19 ?        0:02 /usr/sbin/syslogd   root    128     1  0   Oct 19 ?        0:00 /usr/sbin/cron   root    128     1  0   Oct 19 ?        0:00 /usr/lib/utmpd   root   4365  4354  0  07:09:25 pts/0   0:00 sh #</pre>						
<input type="checkbox"/>	<p>Install Maintenance Update:</p> <ol style="list-style-type: none"> <li><input type="checkbox"/> 1.) Connect to the network &amp; download latest Solaris 7 Maintenance Update</li> <li><input type="checkbox"/> 2.) Unplug from the network.</li> <li><input type="checkbox"/> 3.) Install Maintenance Update.</li> <li><input type="checkbox"/> 4.) reboot -- -r</li> </ol>						
<input type="checkbox"/>	<p>kill -KILL all, but the following processes:</p> <pre># ps -ef   UID    PID  PPID  C   STIME TTY      TIME CMD   root     0     0  0   Oct 19 ?        0:00 sched   root     1     0  0   Oct 19 ?        0:31 /etc/init -r   root     2     0  0   Oct 19 ?        0:00 pageout   root     3     0  0   Oct 19 ?        0:54 fsflush   root    199     1  0   Oct 19 console 0:00 /usr/lib/saf/ttymon -g -h -p nsl console login: -T sun -d /dev/console -l cons   root    129     1  0   Oct 19 ?        0:02 /usr/sbin/syslogd   root    128     1  0   Oct 19 ?        0:00 /usr/sbin/cron   root    128     1  0   Oct 19 ?        0:00 /usr/lib/utmpd   root   4365  4354  0  07:09:25 pts/0   0:00 sh #</pre>						
<input type="checkbox"/>	<p>Install Recommended &amp; Security Fixes Patch Cluster:</p> <ol style="list-style-type: none"> <li><input type="checkbox"/> 1.) Connect to the network &amp; download latest Recommended &amp; Security Fixes Cluster.</li> <li><input type="checkbox"/> 2.) Unplug from the network.</li> <li><input type="checkbox"/> 3.) Install patch cluster.</li> <li><input type="checkbox"/> 4.) reboot -- -r</li> </ol>						

<input type="checkbox"/>	<p>Strip operating system.</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Disable all links in /etc/rc[013].d</li> <li><input type="checkbox"/> Disable all links in /etc/rc[S2].d, except: <ul style="list-style-type: none"> <li>- MOUNTFSYS</li> <li>- inet (<i>inetinit</i>)</li> <li>- syslog</li> <li>- savecore</li> <li>- utmpd</li> <li>- rootusr.sh</li> <li>- standardmounts.sh</li> <li>- buildmnttab.sh</li> <li>- RMTMPFILES</li> <li>- inetsvc</li> <li>- cron</li> <li>- sendmail</li> <li>- audit</li> <li>- keymap.sh</li> <li>- coreadm</li> </ul> </li> <li><input type="checkbox"/> Strip /etc/init.d/inetsvc: <ul style="list-style-type: none"> <li>- Disable everything except ifconfig &amp; named</li> <li>- Remove DHCP switch from ifconfig</li> <li>- Disable inetd</li> </ul> </li> <li><input type="checkbox"/> Disable sac in /etc/inittab</li> <li><input type="checkbox"/> Remove all crontab files, except for root's.</li> <li><input type="checkbox"/> Strip services from inetd.conf: (inetd SHOULD NOT BE STARTED AT BOOT TIME) <ul style="list-style-type: none"> <li><input type="checkbox"/> Strip configuration for all services, except FTP &amp; TELNET.</li> <li><input type="checkbox"/> Configure FTP &amp; TELNET to be wrapped.</li> <li><input type="checkbox"/> Comment FTP &amp; TELNET.</li> </ul> </li> <li><input type="checkbox"/> Remove NFS files: <ul style="list-style-type: none"> <li>- rm /etc/auto_*</li> <li>- rm /etc/dfs/dfstab</li> </ul> </li> </ul>
<input type="checkbox"/>	<p>Harden operating system:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Set daemon umask: <ul style="list-style-type: none"> <li>- Create /etc/init.d/umask.sh</li> <li>- ln -s /etc/init.d/umask.sh /etc/rc?.d/S00umask.sh</li> </ul> </li> <li><input type="checkbox"/> Disable rhost authentication in /etc/pam.conf</li> <li><input type="checkbox"/> Add log &amp; stack smashing defense to /etc/system</li> <li><input type="checkbox"/> Add IP kernel tuning parameters to end of /etc/init.d/inetinit</li> <li><input type="checkbox"/> Mount /usr read-only</li> <li><input type="checkbox"/> Mount all file systems, except /usr &amp; swap, nosuid</li> <li><input type="checkbox"/> Configure the following files in /etc/default: <ul style="list-style-type: none"> <li><input type="checkbox"/> login- uncomment &amp; set UMASK, PATH, SUPATH</li> <li><input type="checkbox"/> su- uncomment &amp; set PATH &amp; SUPATH</li> <li><input type="checkbox"/> inetinit- set TCP_STRONG_ISS=2</li> </ul> </li> <li><input type="checkbox"/> Harden /etc/passwd &amp; /etc/shadow files: <ul style="list-style-type: none"> <li><input type="checkbox"/> Remove the following accounts: <ul style="list-style-type: none"> <li>- uucp</li> <li>- adm</li> <li>- smtp</li> <li>- nuucp</li> <li>- lp</li> <li>- listen</li> </ul> </li> <li><input type="checkbox"/> Set the shell for the following accounts to /dev/null: (disables login) <ul style="list-style-type: none"> <li>- daemon</li> <li>- sys</li> <li>- noaccess</li> <li>- bin</li> <li>- nobody</li> <li>- nobody4</li> </ul> </li> </ul> </li> <li><input type="checkbox"/> Create /etc/ftpusers <ul style="list-style-type: none"> <li><input type="checkbox"/> Put the following account names in ftpusers: <ul style="list-style-type: none"> <li>- root</li> <li>- sys</li> <li>- nobody4</li> <li>- adm</li> <li>- daemon</li> <li>- nobody</li> <li>- uucp</li> <li>- lp</li> <li>- bin</li> <li>- noaccess</li> <li>- nuucp</li> <li>- listen</li> </ul> </li> <li><input type="checkbox"/> chown root:root /etc/ftpusers</li> <li><input type="checkbox"/> chmod 0600 /etc/ftpusers</li> </ul> </li> </ul>
<input type="checkbox"/>	<p>Modify syslog to send auth.info to /var/log/authlog</p>
<input type="checkbox"/>	<p>reboot -- -r</p>

<input type="checkbox"/>	<p>Verify that only the following processes are running:</p> <pre># ps -ef   UID    PID  PPID  C   STIME TTY      TIME CMD   root     0     0  0   Oct 19 ?        0:00 sched   root     1     0  0   Oct 19 ?        0:31 /etc/init -r   root     2     0  0   Oct 19 ?        0:00 pageout   root     3     0  0   Oct 19 ?        0:54 fsflush   root    199     1  0   Oct 19 console 0:00 /usr/lib/saf/ttymon -g -h -p nsl console login: -T sun -d /dev/console -l cons   root    129     1  0   Oct 19 ?        0:02 /usr/sbin/syslogd   root    128     1  0   Oct 19 ?        0:00 /usr/sbin/cron   root    128     1  0   Oct 19 ?        0:00 /usr/lib/utmpd   root   4365  4354  0 07:09:25 pts/0   0:00 sh</pre> <p>#</p>
<input type="checkbox"/>	Connect system to the network.
<input type="checkbox"/>	<p>Install TCPWrappers:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Install binaries in /usr/sbin</li> <li><input type="checkbox"/> Install &amp; configure template /etc/hosts.allow &amp; /etc/hosts.deny</li> </ul>
<input type="checkbox"/>	<p>Install most recent production tested version of sshd w/tcpwrappers support.</p> <p>Configure the following:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Allowed authentications password only</li> <li><input type="checkbox"/> Disable root login permission</li> <li><input type="checkbox"/> Configure ssh service on port 122</li> <li><input type="checkbox"/> Verify that xauth is in /usr/bin</li> <li><input type="checkbox"/> Allow X11 forwarding</li> <li><input type="checkbox"/> Disable motd &amp; check mail</li> <li><input type="checkbox"/> Config sshd to start on system boot</li> </ul>
<input type="checkbox"/>	<p>Install template disclaimer files:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> /etc/issue</li> <li><input type="checkbox"/> /etc/motd</li> </ul>
<input type="checkbox"/>	<p>Install ntpd:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> running as daemon</li> <li><input type="checkbox"/> hourly crontab</li> </ul>
<input type="checkbox"/>	Configure sendmail to SMARTHOST outbound through JHMAIL & send a test message.
<input type="checkbox"/>	Install most recent copy of nightly check scripts
<input type="checkbox"/>	Install & configure /usr/local/sbin/newsyslog.jhmi
<input type="checkbox"/>	<p>Install &amp; configure backups as appropriate:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Public</li> <li><input type="checkbox"/> Private</li> <li><input type="checkbox"/> Not Installed</li> </ul> <p>Rationale for type of back installed/not installed:</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>

<p>Hardware Manufacturer:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	<p>Model:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<p>Serial Number:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	<p>HostID:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
<p>Installed by:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	<p>Initial kernel revision:</p> <div style="border: 1px solid black; height: 20px; width: 100%;"></div>
installer's signature	date
Approved by	