

JHNS Solaris 8 Set-up Checklist

<input type="checkbox"/>	<p>Install operating system (DO NOT ATTACH TO NETWORK) Install only Core OS + SUNWter <i>Also add the following packages, if the server will need to run X client applications:</i></p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> SUNWxwrtl</td> <td><input type="checkbox"/> SUNWxwfnt</td> <td><input type="checkbox"/> SUNWxwice</td> </tr> <tr> <td><input type="checkbox"/> SUNWtlk</td> <td><input type="checkbox"/> SUNWxilrl</td> <td><input type="checkbox"/> SUNWxildh</td> </tr> <tr> <td><input type="checkbox"/> SUNWxilow</td> <td><input type="checkbox"/> SUNWxwplt</td> <td><input type="checkbox"/> SUNWmfrun</td> </tr> </table> <p>Create separate file systems for:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> /</td> <td><input type="checkbox"/> /usr</td> <td><input type="checkbox"/> /var</td> </tr> <tr> <td><input type="checkbox"/> /usr/local</td> <td><input type="checkbox"/> /export/home</td> <td></td> </tr> <tr> <td><input type="checkbox"/> swap</td> <td><input type="checkbox"/> /opt</td> <td></td> </tr> </table> <p>Reason for non-standard file system layout:</p> <div style="border: 1px solid black; height: 40px; width: 100%;"></div>	<input type="checkbox"/> SUNWxwrtl	<input type="checkbox"/> SUNWxwfnt	<input type="checkbox"/> SUNWxwice	<input type="checkbox"/> SUNWtlk	<input type="checkbox"/> SUNWxilrl	<input type="checkbox"/> SUNWxildh	<input type="checkbox"/> SUNWxilow	<input type="checkbox"/> SUNWxwplt	<input type="checkbox"/> SUNWmfrun	<input type="checkbox"/> /	<input type="checkbox"/> /usr	<input type="checkbox"/> /var	<input type="checkbox"/> /usr/local	<input type="checkbox"/> /export/home		<input type="checkbox"/> swap	<input type="checkbox"/> /opt	
<input type="checkbox"/> SUNWxwrtl	<input type="checkbox"/> SUNWxwfnt	<input type="checkbox"/> SUNWxwice																	
<input type="checkbox"/> SUNWtlk	<input type="checkbox"/> SUNWxilrl	<input type="checkbox"/> SUNWxildh																	
<input type="checkbox"/> SUNWxilow	<input type="checkbox"/> SUNWxwplt	<input type="checkbox"/> SUNWmfrun																	
<input type="checkbox"/> /	<input type="checkbox"/> /usr	<input type="checkbox"/> /var																	
<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><input type="checkbox"/> Touch /etc/notrouter</td> <td><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>Remove Sendmail packages:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> SUNWsndmr</td> </tr> <tr> <td><input type="checkbox"/> SUNWsndmu</td> </tr> </table>	<input type="checkbox"/> SUNWsndmr	<input type="checkbox"/> SUNWsndmu																
<input type="checkbox"/> SUNWsndmr																			
<input type="checkbox"/> SUNWsndmu																			
<input type="checkbox"/>	<p>If the system will be running X applications against a remote X-server add the following packages:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> SUNWs?</td> </tr> <tr> <td><input type="checkbox"/> SUNWs?</td> </tr> </table>	<input type="checkbox"/> SUNWs?	<input type="checkbox"/> SUNWs?																
<input type="checkbox"/> SUNWs?																			
<input type="checkbox"/> SUNWs?																			
<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> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> 1.)</td> <td>Connect to the network & download latest Solaris 8 Maintenance Update</td> </tr> <tr> <td><input type="checkbox"/> 2.)</td> <td>Unplug from the network.</td> </tr> <tr> <td><input type="checkbox"/> 3.)</td> <td>Install Maintenance Update.</td> </tr> <tr> <td><input type="checkbox"/> 4.)</td> <td>reboot -- -r</td> </tr> </table>	<input type="checkbox"/> 1.)	Connect to the network & download latest Solaris 8 Maintenance Update	<input type="checkbox"/> 2.)	Unplug from the network.	<input type="checkbox"/> 3.)	Install Maintenance Update.	<input type="checkbox"/> 4.)	reboot -- -r										
<input type="checkbox"/> 1.)	Connect to the network & download latest Solaris 8 Maintenance Update																		
<input type="checkbox"/> 2.)	Unplug from the network.																		
<input type="checkbox"/> 3.)	Install Maintenance Update.																		
<input type="checkbox"/> 4.)	reboot -- -r																		
<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 & Security Fixes Patch Cluster:</p> <ul style="list-style-type: none"> <input type="checkbox"/> 1.) Connect to the network & download latest Recommended & Security Fixes Cluster. <input type="checkbox"/> 2.) Unplug from the network. <input type="checkbox"/> 3.) Install patch cluster. <input type="checkbox"/> 4.) <code>reboot -- -r</code>
<input type="checkbox"/>	<p>Strip operating system.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Disable all links in <code>/etc/rc[013].d</code> <input type="checkbox"/> Disable all links in <code>/etc/rc[S2].d</code>, except: <ul style="list-style-type: none"> - MOUNTFSYS - inet (<i>inetinit</i>) - syslog - savecore - utmpd - rootusr.sh - standardmounts.sh - buildmnttab.sh - RMTMPFILES - inetsvc - cron - sendmail - audit - keymap.sh - coreadm <input type="checkbox"/> Strip <code>/etc/init.d/inetsvc</code>: <ul style="list-style-type: none"> - Disable everything except <code>ifconfig</code> & <code>named</code> - Remove DHCP switch from <code>ifconfig</code> - Disable <code>inetd</code> <input type="checkbox"/> Disable <code>sac</code> in <code>/etc/inittab</code> <input type="checkbox"/> Remove all <code>crontab</code> files, except for <code>root</code>'s. <input type="checkbox"/> Strip services from <code>inetd.conf</code>: (<code>inetd</code> SHOULD NOT BE STARTED AT BOOT TIME) <ul style="list-style-type: none"> <input type="checkbox"/> Strip configuration for all services, except <code>FTP</code> & <code>TELNET</code>. <input type="checkbox"/> Configure <code>FTP</code> & <code>TELNET</code> to be wrapped. <input type="checkbox"/> Comment <code>FTP</code> & <code>TELNET</code>. <input type="checkbox"/> Remove NFS files: <ul style="list-style-type: none"> - <code>rm /etc/auto_*</code> - <code>rm /etc/dfs/dfstab</code>
<input type="checkbox"/>	<p>Harden operating system:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Disable <code>rhost</code> authentication in <code>/etc/pam.conf</code> <input type="checkbox"/> Add log & stack smashing defense to <code>/etc/system</code> <input type="checkbox"/> Mount <code>/usr</code> read-only <input type="checkbox"/> Mount all file systems, except <code>/</code>, <code>/usr</code> & <code>swap</code>, <code>nosuid</code> <input type="checkbox"/> Mount all file systems, except <code>/usr</code> & <code>swap</code>- logging <input type="checkbox"/> Configure the following files in <code>/etc/default</code>: <ul style="list-style-type: none"> <input type="checkbox"/> <code>login</code>- uncomment & set <code>UMASK</code>, <code>PATH</code>, <code>SUPATH</code> <input type="checkbox"/> <code>su</code>- uncomment & set <code>PATH</code> & <code>SUPATH</code> <input type="checkbox"/> <code>inetinit</code>- set <code>TCP_STRONG_ISS=2</code> <input type="checkbox"/> <code>init</code>- set <code>CMASK=022</code> <input type="checkbox"/> Harden <code>/etc/passwd</code> & <code>/etc/shadow</code> files: <ul style="list-style-type: none"> <input type="checkbox"/> Remove the following accounts: <ul style="list-style-type: none"> - <code>uucp</code> - <code>adm</code> - <code>sntp</code> - <code>nuucp</code> - <code>lp</code> - <code>listen</code> <input type="checkbox"/> Set the shell for the following accounts to <code>/dev/null</code>: (disables login) <ul style="list-style-type: none"> - <code>daemon</code> - <code>sys</code> - <code>noaccess</code> - <code>bin</code> - <code>nobody</code> - <code>nobody4</code> <input type="checkbox"/> Create <code>/etc/ftpusers</code> <ul style="list-style-type: none"> <input type="checkbox"/> Put the following account names in <code>ftpusers</code>: <ul style="list-style-type: none"> - <code>root</code> - <code>sys</code> - <code>nobody4</code> - <code>adm</code> - <code>daemon</code> - <code>nobody</code> - <code>uucp</code> - <code>lp</code> - <code>bin</code> - <code>noaccess</code> - <code>nuucp</code> - <code>listen</code> <input type="checkbox"/> <code>chown root:root /etc/ftpusers</code> <input type="checkbox"/> <code>chmod 0600 /etc/ftpusers</code>
<input type="checkbox"/>	<p>Modify <code>syslog</code> to send <code>auth.info</code> to <code>/var/log/authlog</code></p>
<input type="checkbox"/>	<p><code>reboot -- -r</code></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> <p><input type="checkbox"/> Install from package</p> <p><input type="checkbox"/> Configure /etc/hosts.allow & /etc/hosts.deny</p>
<input type="checkbox"/>	<p>Install most recent production tested version of sshd w/tcpwrappers support.</p> <p>Verify the following:</p> <p><input type="checkbox"/> Allowed authentications password only</p> <p><input type="checkbox"/> Disable root login permission</p> <p><input type="checkbox"/> Configure ssh service on port 122</p> <p><input type="checkbox"/> Verify that xauth is in /usr/bin</p> <p><input type="checkbox"/> Allow X11 forwarding</p> <p><input type="checkbox"/> Disable motd & check mail</p> <p><input type="checkbox"/> Config sshd to start on system boot</p>
<input type="checkbox"/>	<p>Install template disclaimer files:</p> <p><input type="checkbox"/> /etc/issue</p> <p><input type="checkbox"/> /etc/motd</p>
<input type="checkbox"/>	<p>Install ntpd:</p> <p><input type="checkbox"/> running as daemon <input type="checkbox"/> hourly crontab</p>
<input type="checkbox"/>	Install most recent Sendmail package & send a test message.
<input type="checkbox"/>	<p>Install most recent copy JHNS tools & Tweaks package</p> <p><input type="checkbox"/> Configure /usr/local/sbin/newsyslog.jhns</p>
<input type="checkbox"/>	<p>Install & configure backups as appropriate:</p> <p><input type="checkbox"/> Public <input type="checkbox"/> Private <input type="checkbox"/> Not Installed</p> <p>Rationale for type of back installed/not installed:</p> <div style="border: 1px solid black; height: 30px; width: 100%;"></div>

Hardware Manufacturer:	Model:
<input type="text"/>	<input type="text"/>
Serial Number:	HostID:
<input type="text"/>	<input type="text"/>
Installed by:	Initial kernel revision:
<input type="text"/>	<input type="text"/>
_____	_____
installer's signature	date

Approved by	