

JHNIS RedHat 7.2

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"/> /home</td> </tr> <tr> <td><input type="checkbox"/> swap</td> <td><input type="checkbox"/> /var</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"/> /home	<input type="checkbox"/> swap	<input type="checkbox"/> /var				
<input type="checkbox"/> /	<input type="checkbox"/> /usr										
<input type="checkbox"/> /usr/local	<input type="checkbox"/> /home										
<input type="checkbox"/> swap	<input type="checkbox"/> /var										
<input type="checkbox"/>	<p>kill -KILL all, but the following processes:</p> <pre># ps -ef • UID PID PPID C STIME TTY TIME CMD • root 1 0 0 Feb07 ? 00:00:06 init [3] • root 2 1 0 Feb07 ? 00:00:00 [keventd] • root 3 0 0 Feb07 ? 00:28:12 [ksoftirqd_CPU0] • root 4 0 0 Feb07 ? 00:09:18 [kswapd] • root 5 0 0 Feb07 ? 00:00:00 [kreclaimd] • root 6 0 0 Feb07 ? 00:00:00 [bdflush] • root 7 0 0 Feb07 ? 00:00:00 [kupdated] • root 8 1 0 Feb07 ? 00:00:00 [mdrecoveryd] • root 450 1 0 Feb07 ? 00:00:00 syslogd -m 0 • root 455 1 0 Feb07 ? 00:00:00 klogd -2 • root 557 1 0 Feb07 ? 00:00:00 crond • root 842 1 0 Feb07 tty2 00:00:00 /sbin/mingetty tty2 • root 843 1 0 Feb07 tty3 00:00:00 /sbin/mingetty tty3 • root 844 1 0 Feb07 tty4 00:00:00 /sbin/mingetty tty4 • root 848 1 0 Feb07 tty5 00:00:00 /sbin/mingetty tty5 • root 849 1 0 Feb07 tty6 00:00:00 /sbin/mingetty tty6 • root 1495 1 0 Feb07 tty1 00:00:00 /sbin/mingetty tty1 • daemon 24999 1 0 Apr02 ? 00:00:00 /usr/sbin/atd</pre>										
<input type="checkbox"/>	<p>Strip operating system.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Disable all links in /etc/rc[012].d <input type="checkbox"/> Disable all links in /etc/rc[S3or5].d, except: <table style="margin-left: 20px; border: none;"> <tr> <td>- network</td> <td>- syslog</td> </tr> <tr> <td>- keytable</td> <td>- random</td> </tr> <tr> <td>- rawdevices</td> <td>- crond</td> </tr> <tr> <td>- anacron</td> <td>- atd</td> </tr> <tr> <td>- rc.local</td> <td></td> </tr> </table> <input type="checkbox"/> Remove all crontab files, except for root's. <input type="checkbox"/> Strip services from inetd.conf: (inetd SHOULD NOT BE STARTED AT BOOT TIME) <ul style="list-style-type: none"> <input type="checkbox"/> Strip configuration for all services, except FTP & TELNET. <input type="checkbox"/> Configure FTP & TELNET to be wrapped. <input type="checkbox"/> Comment FTP & TELNET. 	- network	- syslog	- keytable	- random	- rawdevices	- crond	- anacron	- atd	- rc.local	
- network	- syslog										
- keytable	- random										
- rawdevices	- crond										
- anacron	- atd										
- rc.local											
<input type="checkbox"/>	<p>Harden operating system:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Mount /usr read-only <input type="checkbox"/> Mount all file systems, except /usr & swap, nosuid <input type="checkbox"/> Harden /etc/passwd, /etc/group & /etc/shadow files: <ul style="list-style-type: none"> <input type="checkbox"/> Remove the following accounts: <table style="margin-left: 20px; border: none;"> <tr> <td>- uucp</td> <td>- nuucp</td> </tr> <tr> <td>- adm</td> <td>- lp</td> </tr> <tr> <td>- smtp</td> <td>- listen</td> </tr> </table> <input type="checkbox"/> Remove the following groups: <table style="margin-left: 20px; border: none;"> <tr> <td>- news</td> <td>- games</td> </tr> <tr> <td>- uucp</td> <td>- dip</td> </tr> </table> 	- uucp	- nuucp	- adm	- lp	- smtp	- listen	- news	- games	- uucp	- dip
- uucp	- nuucp										
- adm	- lp										
- smtp	- listen										
- news	- games										
- uucp	- dip										

	<ul style="list-style-type: none"> <input type="checkbox"/> - lp <input type="checkbox"/> Set the shell for the following accounts to /dev/null: (disables login) <ul style="list-style-type: none"> - daemon - bin - sys - nobody - noaccess - nobody4 <input type="checkbox"/> Create /etc/ftusers <ul style="list-style-type: none"> <input type="checkbox"/> Put the following account names in ftusers: <ul style="list-style-type: none"> - root - daemon - bin - sys - nobody - noaccess - nobody4 - UUCP - nuucp - adm - lp - listen <input type="checkbox"/> chown root:root /etc/ftusers <input type="checkbox"/> chmod 0600 /etc/ftusers <input type="checkbox"/> Remove unnecessary packages: <ul style="list-style-type: none"> - OpenSSH - All Xwindows packages if not using gui - Any programs not being used or compiled (apache,ftp) - Any desktop related packages not being used (kde, gnome) <input type="checkbox"/> Recompile kernel: <ul style="list-style-type: none"> - Remove support for all hardware not being used (USB, sound) - Be sure to add support for serial console access <input type="checkbox"/> Setup Console Access: <ul style="list-style-type: none"> - append="console=tty0 console=ttyS0,9600n8" --/etc/lilo.conf - s0:2345:respawn:/sbin/mingetty ttyS0 DT9600 --/etc/inittab 																																																																																																																																																																																				
<input type="checkbox"/>	Modify syslog to send auth.info to /var/log/authlog																																																																																																																																																																																				
<input type="checkbox"/>	shutdown -r now																																																																																																																																																																																				
<input type="checkbox"/>	Verify that only the following processes are running: <pre># ps -ef</pre> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">•</th> <th style="text-align: left;">UID</th> <th style="text-align: left;">PID</th> <th style="text-align: left;">PPID</th> <th style="text-align: left;">C</th> <th style="text-align: left;">STIME</th> <th style="text-align: left;">TTY</th> <th style="text-align: left;">TIME</th> <th style="text-align: left;">CMD</th> </tr> </thead> <tbody> <tr><td>•</td><td>root</td><td>1</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:06</td><td>init [3]</td></tr> <tr><td>•</td><td>root</td><td>2</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>[keventd]</td></tr> <tr><td>•</td><td>root</td><td>3</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:28:12</td><td>[ksoftirqd_CPU0]</td></tr> <tr><td>•</td><td>root</td><td>4</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:09:18</td><td>[kswapd]</td></tr> <tr><td>•</td><td>root</td><td>5</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>[kreclaimd]</td></tr> <tr><td>•</td><td>root</td><td>6</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>[bdflush]</td></tr> <tr><td>•</td><td>root</td><td>7</td><td>0</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>[kupdated]</td></tr> <tr><td>•</td><td>root</td><td>8</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>[mdrecoveryd]</td></tr> <tr><td>•</td><td>root</td><td>450</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>syslogd -m 0</td></tr> <tr><td>•</td><td>root</td><td>455</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>klogd -2</td></tr> <tr><td>•</td><td>root</td><td>540</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>/usr/local/sbin/sshd2</td></tr> <tr><td>•</td><td>root</td><td>557</td><td>1</td><td>0</td><td>Feb07</td><td>?</td><td>00:00:00</td><td>cron</td></tr> <tr><td>•</td><td>root</td><td>842</td><td>1</td><td>0</td><td>Feb07</td><td>tty2</td><td>00:00:00</td><td>/sbin/mingetty tty2</td></tr> <tr><td>•</td><td>root</td><td>843</td><td>1</td><td>0</td><td>Feb07</td><td>tty3</td><td>00:00:00</td><td>/sbin/mingetty tty3</td></tr> <tr><td>•</td><td>root</td><td>844</td><td>1</td><td>0</td><td>Feb07</td><td>tty4</td><td>00:00:00</td><td>/sbin/mingetty tty4</td></tr> <tr><td>•</td><td>root</td><td>848</td><td>1</td><td>0</td><td>Feb07</td><td>tty5</td><td>00:00:00</td><td>/sbin/mingetty tty5</td></tr> <tr><td>•</td><td>root</td><td>849</td><td>1</td><td>0</td><td>Feb07</td><td>tty6</td><td>00:00:00</td><td>/sbin/mingetty tty6</td></tr> <tr><td>•</td><td>root</td><td>1495</td><td>1</td><td>0</td><td>Feb07</td><td>tty1</td><td>00:00:00</td><td>/sbin/mingetty tty1</td></tr> <tr><td>•</td><td>daemon</td><td>24999</td><td>1</td><td>0</td><td>Apr02</td><td>?</td><td>00:00:00</td><td>/usr/sbin/atd</td></tr> </tbody> </table>	•	UID	PID	PPID	C	STIME	TTY	TIME	CMD	•	root	1	0	0	Feb07	?	00:00:06	init [3]	•	root	2	1	0	Feb07	?	00:00:00	[keventd]	•	root	3	0	0	Feb07	?	00:28:12	[ksoftirqd_CPU0]	•	root	4	0	0	Feb07	?	00:09:18	[kswapd]	•	root	5	0	0	Feb07	?	00:00:00	[kreclaimd]	•	root	6	0	0	Feb07	?	00:00:00	[bdflush]	•	root	7	0	0	Feb07	?	00:00:00	[kupdated]	•	root	8	1	0	Feb07	?	00:00:00	[mdrecoveryd]	•	root	450	1	0	Feb07	?	00:00:00	syslogd -m 0	•	root	455	1	0	Feb07	?	00:00:00	klogd -2	•	root	540	1	0	Feb07	?	00:00:00	/usr/local/sbin/sshd2	•	root	557	1	0	Feb07	?	00:00:00	cron	•	root	842	1	0	Feb07	tty2	00:00:00	/sbin/mingetty tty2	•	root	843	1	0	Feb07	tty3	00:00:00	/sbin/mingetty tty3	•	root	844	1	0	Feb07	tty4	00:00:00	/sbin/mingetty tty4	•	root	848	1	0	Feb07	tty5	00:00:00	/sbin/mingetty tty5	•	root	849	1	0	Feb07	tty6	00:00:00	/sbin/mingetty tty6	•	root	1495	1	0	Feb07	tty1	00:00:00	/sbin/mingetty tty1	•	daemon	24999	1	0	Apr02	?	00:00:00	/usr/sbin/atd
•	UID	PID	PPID	C	STIME	TTY	TIME	CMD																																																																																																																																																																													
•	root	1	0	0	Feb07	?	00:00:06	init [3]																																																																																																																																																																													
•	root	2	1	0	Feb07	?	00:00:00	[keventd]																																																																																																																																																																													
•	root	3	0	0	Feb07	?	00:28:12	[ksoftirqd_CPU0]																																																																																																																																																																													
•	root	4	0	0	Feb07	?	00:09:18	[kswapd]																																																																																																																																																																													
•	root	5	0	0	Feb07	?	00:00:00	[kreclaimd]																																																																																																																																																																													
•	root	6	0	0	Feb07	?	00:00:00	[bdflush]																																																																																																																																																																													
•	root	7	0	0	Feb07	?	00:00:00	[kupdated]																																																																																																																																																																													
•	root	8	1	0	Feb07	?	00:00:00	[mdrecoveryd]																																																																																																																																																																													
•	root	450	1	0	Feb07	?	00:00:00	syslogd -m 0																																																																																																																																																																													
•	root	455	1	0	Feb07	?	00:00:00	klogd -2																																																																																																																																																																													
•	root	540	1	0	Feb07	?	00:00:00	/usr/local/sbin/sshd2																																																																																																																																																																													
•	root	557	1	0	Feb07	?	00:00:00	cron																																																																																																																																																																													
•	root	842	1	0	Feb07	tty2	00:00:00	/sbin/mingetty tty2																																																																																																																																																																													
•	root	843	1	0	Feb07	tty3	00:00:00	/sbin/mingetty tty3																																																																																																																																																																													
•	root	844	1	0	Feb07	tty4	00:00:00	/sbin/mingetty tty4																																																																																																																																																																													
•	root	848	1	0	Feb07	tty5	00:00:00	/sbin/mingetty tty5																																																																																																																																																																													
•	root	849	1	0	Feb07	tty6	00:00:00	/sbin/mingetty tty6																																																																																																																																																																													
•	root	1495	1	0	Feb07	tty1	00:00:00	/sbin/mingetty tty1																																																																																																																																																																													
•	daemon	24999	1	0	Apr02	?	00:00:00	/usr/sbin/atd																																																																																																																																																																													
<input type="checkbox"/>	Connect system to the network.																																																																																																																																																																																				
<input type="checkbox"/>	Install TCPWrappers: <ul style="list-style-type: none"> <input type="checkbox"/> Install binaries in /usr/sbin <input type="checkbox"/> Install & configure template /etc/hosts.allow & /etc/hosts.deny 																																																																																																																																																																																				
<input type="checkbox"/>	Install most recent production tested version of sshd w/tcpwrappers support. <ul style="list-style-type: none"> • Be sure to remove OpenSSH packages before compiling SSH • SSH.com rpms do not have support for tcpwrappers Configure the following: <ul style="list-style-type: none"> <input type="checkbox"/> Allowed authentications password only <input type="checkbox"/> Disable root login permission <input type="checkbox"/> Configure ssh service on port 122 <input type="checkbox"/> Verify that xauth is in /usr/bin <input type="checkbox"/> Allow X11 forwarding 																																																																																																																																																																																				

	<input type="checkbox"/> Disable motd & check mail <input type="checkbox"/> Config sshd to start on system boot
<input type="checkbox"/>	Install template disclaimer files: <input type="checkbox"/> /etc/issue <input type="checkbox"/> /etc/motd
<input type="checkbox"/>	Install ntpd: <input type="checkbox"/> running as daemon <input type="checkbox"/> hourly crontab
<input type="checkbox"/>	Configure sendmail to SMARTHOST outbound through JHMAIL & send a test message.
<input type="checkbox"/>	Install & configure backups as appropriate: <input type="checkbox"/> Public <input type="checkbox"/> Private <input type="checkbox"/> Not Installed Rationale for type of back installed/not installed: <div style="border: 1px solid black; height: 20px; width: 100%; margin-top: 5px;"></div>

Hardware Manufacturer:	Model:
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Serial Number:	HostID:
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
Installed by:	Initial kernel revision:
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>
<hr style="width: 50%; margin: 10px auto;"/>	
installer's signature	date
<hr style="width: 50%; margin: 10px auto;"/>	
Approved by	