

# **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 permited without express written permission.

## Building a Secure Solaris 9 JumpStart Server

Bayly Eley September 14, 2004

GCUX Practical v2.0 Option1 - Securing UNIX Step by Step

## Abstract

Over the past ten years there has been a rapid proliferation of servers in our data centers, as well as, a need for increased security. Solaris JumpStart can help with both of these challenges. Solaris JumpStart is an installation server included with the SPARC Solaris operating environment. Gone are the days of shuffling CDROMs for hours while performing an installation. Nor does each installation have to be painstakingly hardened. JumpStart enables administrators to install SPARC Solaris in an automated, unattended, and consistent manner.

This paper will present how to build a secure Solaris 9 JumpStart server to be used to install secure Solaris 9 servers. The necessary hardware and software will be discussed, and the installation, configuration, hardening, and maintenance will be detailed. In addition, the hardening process will be tested using common UNIX applications and common vulnerability assessment tools, such as Nessus.

### **System Description**

It is always a good practice to perform installations in a non-networked or securely networked environment. The JumpStart server will be located on an isolated private network, separate from the production network. In addition to the JumpStart server, only JumpStart clients will be placed on this network. Once a client's installation is complete, it can be easily moved to the production network.

The hardware for the JumpStart server will consist of a single Sun Ultra 5 with one 360 MHz UltraSPAR-IIi processor, 128 MB of memory, one 10/100 Ethernet interface, a CDROM drive, and one 8.3 GB IDE hard drive. For the purposes of this project, an additional Sun Ultra 5 will be used as a JumpStart client to test the installation process. The client utilizes a 270 MHz UltraSPARC-IIi processor, 256 MB of memory, one 10/100 Ethernet interface, a CDROM drive, and one 4.0 GB IDE hard drive.

Solaris has a rich history as a UNIX operating system. It is one of the most widely distributed commercial UNIX operating systems in use today. As such, it is the primary operating system in our environment. JumpStart can be configured to install Solaris 2.6, 7, 8, or 9. However, Solaris 9 is the most recent release from Sun Microsystems and is used exclusively in our environment. Therefore, this document will detail the configuration of JumpStart for Solaris 9, and not any previous versions.

The needs and roles of servers vary from site to site. Each of our servers run different applications, so we have found it to be more efficient to use JumpStart for the basic operating system installation, but still install any server specific applications manually. Therefore, this document aims to describe how to create a basic and secure installation that can be built upon.

In addition to the essential operating system daemons, the JumpStart server will need RPC (for bootp), and NFS and TFTP to perform network installations. NFS will be restricted to read-only access on the isolated network. TCP Wrappers will be used to restrict the use of TFTP and other network services to the private network. SSH will be installed and will be the only remote access available to the server and clients. In addition, no remote root log in will be permitted; users must SU to root after being authenticated as a normal user. Only authorized administrators should have access to the JumpStart server.

Regular backups are not necessary for the JumpStart server. The information contained on the server is static. An initial backup after configuration is complete and incremental backups when any configuration changes are made will be sufficient. For this, we will use TAR and burn the archives to CDROM.

The JumpStart server should be located in a secure location. Physical access should be limited to authorized administrators. A computer room with some type of access control should be used. Effective security policies should be in place to enforce such access restrictions.

#### **Risk Analysis**

A JumpStart server is a key and vulnerable system. From it, all new installations will be created. The potential for an attacker to poison all installations is real. Therefore, the following risks must be considered:

- Hardware Failure
- Physical Damage
- Software Malfunction
- Internal Attacks
- External Attacks

Hardware failure and physical damage for our JumpStart server is a real and acceptable risk. The JumpStart server is not an operationally critical system; basic vendor support is sufficient for replacement of any failed hardware components, such as: disks, power supplies, etc. Initial and incremental backups will be burned to CDROM and stored in a secure location in case of a catastrophic hardware failure or damage. However, the JumpStart clients will most likely become more operationally critical systems. So, disk mirroring will be implemented, and redundant hardware components should be used when available.

Software malfunction risk is low for the JumpStart server, since JumpStart is part of the Solaris operating system and no third-party applications will be used. To help guard against any operating system issues, Solaris patch clusters will be installed at monthly intervals. Likewise, software malfunction risk is low for the JumpStart clients, as the installation of any third-party applications after installation is complete is beyond the scope of this document. However, all clients will receive the latest Solaris patch cluster as part of the installation process.

Internal attacks do represent some risk, but can be mitigated by restricting the JumpStart services to an isolated network with TCP Wrappers. SSH will insure secure remote access. Adequate security policies and physical isolation will help deter or stop most internal risks.

External attacks are possible, however unlikely. A firewall provides perimeter security and SSH, TCP Wrappers, and network isolation provide additional layers of security. No services will be available to the outside, and a well-defined security policy will help make it extremely difficult for an external attacker to penetrate the JumpStart server.

#### Installation (Operating System)

- 1. Begin by powering on the system. For the Ultra 5 platform, the power button is located on the top right of the front face. At this point, you should be able to insert the Solaris 9 Software CDROM 1/2. Press the eject button on the CDROM, insert the CDROM, and close the drive sled. Once the OpenBoot memory banner is displayed, you may send a "break" using the Stop-A keys (the precise method may differ depending your specific type of terminal connection).
- 2. At the OK prompt type boot cdrom.
- 3. The first screen will ask for choice of language. Type "0" for English.

•						🐔 Terminal	$\Box = \Box \times$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
							<b>^</b>
Selec 0. 1. 2. 3. 4. 5. 6. 7. 7. 8. 9. 9. Pleas	t a Lan Englis French German Italia Japane Korean Simpli Spanis Swedis Tradit e make	iguage h i se fied h h ional a cho	Chinese Chinese ice (0 -	9), 1	or pres	ss h or ? for help: O	

4. The next screen will ask for locale. Type "0" for English.



5. The next screen will ask what type of terminal you are using. In most cases, VT100 is appropriate, but your exact environment may differ. Select "3" for VT100.

•						🐔 Terminal	$\Box = \Box \times$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
What 1) # 2) I 3) I 4) H 5) I 6) P 7) S 8) S 9) I 10) 11) 12) 13) 14)	type of NSI Si EC VTS EC VTS eathk: ear Si C Cons Sun Cor un Wo Pelevic Televic Televic X Terr CDE Te Other	- bf term tandard 52 100 it 19 iegler sole mmand 7 ckstati deo 910 ideo 92 Model 5 minal E erminal	Ainal are d CRT ADM31 Cool .on 25 50 Emulator L Emulator	you (xter: c (dt	using? ms) term)		<b>•</b>
Tybe	che ni	ninet c	n your cr	TOTCE	anu pi	Less Neculn: 3	<b>_</b>

6. Select F2 Continue after reading a description of the installation program.

•						🐔 Terminal	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
The	Solar	ris Ins	tallation	Pro	gram		<b></b>
The whe the mad	Solar re you end o e befo	ris ins 1'll be of each Dre con	tallation prompted section, tinuing.	pro to you	gram is provide 'll be	divided into a series of short sections information for the installation. At able to change the selections you've	
Abo	ut nav - 7 - 1 1 1	vigatio The mou If your respond vill ch	n se cannot keyboard , press E ange to s	be doe SC; how	used s not h the leg the ESC	ave function keys, or they do not end at the bottom of the screen keys to use for navigation.	
F	2_Cont	tinue	F6_Help				J

7. Select F2 Continue after reading a description about the identification process.



8. Select "Yes" for a networked system, and **F2\_Continue**.

•						🐔 Terminal	$\Box = \Box \times$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
Net	twork (	Connect	ivity				<b>_</b>
Spe or Sol sup Spe is Hel	ecify ? vendon Laris ( pported ecify P not su Lp.	Yes if r netwo CD. See d cards No if t upporte	the syste rk/commur your har he system d on the	em is Nicat: Odwar) Nis N Sola:	conne ion Et e docu connec ris CD	cted to the network by one of the Solaris hernet cards that are supported on the mentation for the current list of ted to a network/communication card that , and follow the instructions listed under	
	Netwo	orked					
	<b>[2]</b> 1	Йез No					
H	2_Cont	tinue	F6_Helr	)			J

9. Select "No" for DHCP and F2\_Continue.

•						🐔 Terminal	
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
DHCP	•						1
On t for No i	chis so networ f the	reen y k int inter	you must erface co faces are	spec: onfig e to l	ify who uration be con:	ether or not this system should use DHCP n. Choose Yes if DHCP is to be used, or figured manually.	
NOTE rebo	: DHCE ots.	supp	ort will	not ]	be enal	bled, if selected, until after the system	
	Use DH	łCP					
	[ ] Ye [ <b>X]</b> No	es D					
F2	_Conti	inue	F6_Help	)			
							•

10.Enter a "*Host name*" for the JumpStart server in the space provided and **F2\_Continue**.

👻 🧭 Terminal	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Host Name	<b>_</b>
On this screen you must enter your host name, which identifies this system on the network. The name must be unique within your domain; creating a duplicate host name will cause problems on the network after you install Solaris.	
A host name must be at least two characters; it can contain letters, digits, and minus signs (-).	
Host name: <b>j<u>urpstart</u></b>	
F2_Continue F6_Help	•

11.Enter the "*IP address*" for the JumpStart server and **F2\_Continue**.

👻 🧭 Terminal	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
IP Address	<b>_</b>
On this screen you must enter the Internet Protocol (IP) address for this system. It must be unique and follow your site's address conventions, or system/network failure could result.	a
IP addresses contain four sets of numbers separated by periods (for example 129.200.9.1).	e
IP address: <b>192.168.0.10</b>	
F2_Continue F6_Help	
	•

12. Most network configurations are part of a subnet. Select "Yes" and **F2\_Continue**.

•						🐔 Terminal	$\square$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
Sut	nets						<b></b>
On you net	this s speci work a	screen ify inc after y	you must orrectly, ou reboot	spec: the	ify wh system	ether this system is part of a subnet. If m will have problems communicating on the	
> 1 > 1	'o make )ress F	e a sel Return	ection, u to mark i	ise ti .t [X	he arro ].	ow keys to highlight the option and	
	Syste	em part	; of a sub	net			
	7 <b>[2]</b> []	7es No					
F	'2_Cont	inue	F6_Helr	)			Ţ

13.Enter the "*Netmask*" and **F2\_Continue**.

👻 🧭 Terminal	$\Box = \Box \times$
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Netmask	<b>_</b>
On this screen you must specify the netmask of your subnet. A default netmask is shown; do not accept the default unless you are sure it is correct for your subnet. A netmask must contain four sets of numbers separated by periods (for example 255.255.255.0).	
Netmask: <b>255.255.0</b>	
F2 Continue F6 Help	
	-

14. Most environments do not yet support IPv6. Select "No" and **F2\_Continue**.

•						💈 Terminal	$\Box = \Box \times$				
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp						
IPv	6						<b>_</b>				
On Int no IPv	On this screen you should specify whether or not IPv6, the next generation Internet Protocol, will be enabled on this machine. Enabling IPv6 will have no effect if this machine is not on a network that provides IPv6 service. IPv4 service will not be affected if IPv6 is enabled.										
> T P	'o make ress R	: a sel Ceturn	ection, u to mark i	ise ti .t [X	ne arr ].	ow keys to highlight the option and					
	Enabl	e IPv6.									
	[] y [X] N	'es lo									
F	2_Cont	inue	F6_Help	)			•				

15. Select to specify a "Default Route" (if needed) and **F2\_Continue**.

👻 🧭 Terminal	$\square \square \times$
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Set the Default Route	<b>_</b>
To specify the default route, you can let the software try to detect one upon reboot, you can specify the IP address of the router, or you can choose None. Choose None if you do not have a router on your subnet.	
> To make a selection, use the arrow keys to select your choice and press Return to mark it [X].	
Default Route	
<pre>[ ] Detect one upon reboot [X] Specify one [ ] None</pre>	
F2_Continue F6_Help	
	-

16.Enter the "*Default Router IP Address*" and **F2\_Continue**.

•						💈 Terminal	$\Box = \Box \times$
<u>F</u> ile	e <u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
De	efault 1	Route I	P Address	3			<b>_</b>
En /e (e	nter th etc/def: example	e IP ad aultrou 129.14	dress of ter file 6.89.225)	the and '	defau will b	lt route. This entry will be placed in the e the default route after you reboot	
	Router	IP Add	lress: <b>192</b>	2. 168	.0.1		
	F2_Con	tinue	F6_Helr	)			•

17.Confirm the identification information and **F2\_Continue**.



18.Select "No" for "Configure Kerberos Security" and **F2\_Continue**.



19. Yes, we are sure we do not want to use Kerberos Security. Select F2\_Continue.



20.Select "None" for the Name Service and F2 Continue.



21.Yes, we are sure we do not want to use a Name Service. **F2** Continue.



22.Select "Americas" for the Time Zone and **F2\_Continue**.

👻 🧭 Terminal	$\Box = \Box \times$
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Time Zone	<b>_</b>
On this screen you must specify your default time zone. You can specify a time zone in three ways: select one of the continents or oceans from the list, select other - offset from GMT, or other - specify time zone file.	
> To make a selection, use the arrow keys to highlight the option and press Return to mark it [X].	
Continents and Oceans	
<ul> <li>Africa</li> <li>Americas</li> <li>Antarctica</li> <li>Arctic Ocean</li> <li>Asia</li> <li>Atlantic Ocean</li> <li>Australia</li> <li>Europe</li> </ul>	
v [] Indian Ocean F2_Continue F6_Help	T

23.Select "United States" for the Country and F2\_Continue.

👻 🦉 Terminal	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Country or Region	<b>_</b>
> To make a selection, use the arrow keys to highlight the option and press Return to mark it [X].	
Countries and Regions	
<ul> <li>Inited States</li> <li>Anguilla</li> <li>Antigua &amp; Barbuda</li> <li>Argentina</li> <li>Aruba</li> <li>Bahamas</li> <li>Barbados</li> <li>Belize</li> <li>Bolivia</li> <li>Brazil</li> <li>Canada</li> <li>Cayman Islands</li> <li>V</li> </ul>	
F2_Continue F6_Help	Ţ

24.Select the "Central" (or other) Time Zone and F2 Continue.



25.Set the year and date, and F2\_Continue.

-					💈 Terminal 🛛 👔 🗖 📉
<u>F</u> ile <u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o _	<u>H</u> elp	
Date and	d Time				·
> Accept new va	t the de alues.	fault dat	ce and	time	or enter
Date and	d time:	2004-07-2	22 13:3	30	
Year Month Day Hour Minute	(4 dig (1-12) (1-31) (0-23) (0-59)	(its) : 20 : 07 : 22 : 13 : 30	1 <b>04</b> 7 2 3 0		
F2_Cor	ntinue	F6_Help	)		-

26.Confirm the Time Zone and Date/Time information, and **F2\_Continue**.

•							🐔 Tei	rminal					$^{1\times}$
E	ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp							
	Con	firm I	nforma	tion									
	> 0 t	onfirm o char	i the f ige any	ollowing informat	info ion,	rmation press	. If 74.	it is	correct	;, pres	s F2;		
		Tin	ie zone	: Central (US/Cer	. Tim tral	e )							
	D	ate an	nd time	: 2004-07	-22	13:30:0	D						
	F	2_Cont	inue	F4_Char	ıge	F6_He	lp						-

27.Most Sun systems come from the factory with the operating system pre-installed. We want to perform an "Initial" install to overwrite any previous installation. Select **F4\_Initial**.

👻 🧭 Terminal	$\Box = \Box \times$
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp	
Solaris Interactive Installation	<b>_</b>
This system is upgradable, so there are two ways to install the Solaris software.	
The Upgrade option updates the Solaris software to the new release, saving as many modifications to the previous version of Solaris software as possible. Back up the system before using the Upgrade option.	
The Initial option overwrites the system disks with the new version of Solaris software. This option allows you to preserve any existing file systems. Back up any modifications made to the previous version of Solaris software before starting the Initial option.	
After you select an option and complete the tasks that follow, a summary of your actions will be displayed. If you want to install the system with a Flash archive, select Initial.	
F2_Upgrade F4_Initial F5_Exit F6_Help	T

28.Select F2 Standard installation.

🐔 Terminal ÷  $\square \square \times$ <u>F</u>ile <u>E</u>dit <u>V</u>iew <u>T</u>erminal <u>G</u>o <u>H</u>elp ٠ Solaris Interactive Installation You'll be using the initial option for installing Solaris software on the system. The initial option overwrites the system disks when the new Solaris software is installed. On the following screens, you can accept the defaults or you can customize how Solaris software will be installed by: Selecting the type of Solaris software to install
Selecting disks to hold software you've selected
Specifying how file systems are laid out on the disks After completing these tasks, a summary of your selections (called a profile) will be displayed. There are two ways to install your Solaris software: - "Standard" installs your system from a standard Solaris Distribution. - "Flash" installs your system from one or more Flash Archives. F3\_Go Back F2\_Standard F4\_Flash F5\_Exit F6\_Help -

29.Select any additional Geographic Regions for which support should be installed. Usually, none are necessary. Select F2\_Continue.

•						💈 Terminal 🛛 👔 🗌 🔪	<
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp		
Se] Se] >   >   >   >   >   >   >   >   >   >	Lect Ge Lect th [ ] Au: [ ] Mid [ ] East [ ] We: [ ] Noi [ ] Sou [ ] Cer [ ] Cer [ ] Noi [ ] As:	eograph ne geog stralas rthern ddle Eas stern E stern E stern Ame uthan athan Atral A tral C rthern ia	ic Regior raphic re Africa st urope rica Europe rica merica urope Europe Europe	is egions	for wh	which support should be installed.	1
1	<b>ve le</b> F2_Cor	ft, rig ntinue	<b>ht, up, d</b> F3_Go	<b>lown u</b> s Back	sing th F5_F	t <b>he arrow keys</b> Exit F6_Help	•

30.Select 64-bit Support and F2\_Continue.



31.Select "Core System Support 64-bit" and F4\_Customize.

•				🐔 Terminal			[	
<u>F</u> ile <u>E</u>	dit <u>V</u> iew	<u>T</u> erminal	<u>G</u> o <u>H</u> elp					
Selec	t Software							<b>_</b>
Selec	t the Sola	ris softw	are to in:	stall on the	system.			
NOTE: custo depen displ	After sel mizing it. dencies an aying 64-b	ecting a However, d how Sol it contai	software ( this requ aris soft n 64-bit :	group, you ca lires underst ware is packa support.	n add or rem anding of so ged. The so	nove software oftware ftware groups	by	
[ [ [ [	] Entire ] Entire ] Develo ] End Us X Core S	Distribu Distribu per Syste er System ystem Sup	tion plus tion 64-b: m Support Support ( port 64-b:	0EM support it 64-bit 54-bit it	64-bit 251 246 196 146 72	3.00 MB 5.00 MB 1.00 MB 2.00 MB 1.00 MB		
F2	_Continue	F3_Go	Back F4	4_Customize	F5_Exit	F6_Help		-

32.The Customize Software Screen allows you to add and remove individual software components of the "Core System Support" software group. The installer displays an ASCII menu with four columns (see screen capture).

•	🐔 Terminal		$\Box = \Box \times$
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o <u>H</u> elp		
Cu	stomize Software: Core System Support		<b>_</b>
> > > > >	<pre>[] 64-bit iconv conversion for Eastern European locales 64-bit iconv conversion for ISO Latin character sets A Windows SMB/CIFS fileserver for UNIX. ABI. Admin/Install Java Extension Libraries. Apache Common Logging. Apache Web Server. Apptrace utility and support shared objects. Apptrace utility and support shared objects. Apptrace utility and support shared objects (64-bit). Archive Libraries. Archive Libraries. Archive Libraries (64-bit). X Audio Drivers (64-bit). X Audio Drivers and applications X Audio Applications. X Audio Header Files. X Audio Sound Files. AuditService Implementation.</pre>	0.00 MB 0.00 MB 0.42 MB 0.42 MB 0.28 MB 0.28 MB 0.28 MB	
1	ove left, right, up, down using the arrow keys		
	F2_OK F6_Help		T

The first column works like an inverted tree. A ">" represents an unexpanded cluster of packages, a "V" represents an expanded cluster of packages, and no symbol represents a single package. You can expand and collapse a cluster by using the arrow keys to place the cursor over the ">" or "V" respectively and pressing <Enter>.

The second column shows which clusters or packages are selected. No symbol means that no cluster or package is selected. An "X" shows that a cluster or package is selected. A "!" indicates that the cluster or package is required, and may not be removed. Finally, a "/" indicates a partially selected cluster. Clusters and packages may be selected or unselected by placing the cursor over the brackets and pressing <Enter>.

The third column is the cluster or package name. Highlighting the name and pressing <Enter> will display a detailed description.

The fourth column displays the size of the cluster or package. A size of 0.00 MB indicates the cluster or package is not selected.

Because we have selected the "Core System Support" software group, which does not include the Java Virtual Machine, the WebStart Installer cannot automatically install the Solaris Software 2/2 CDROM. So, we need not concern ourselves with selecting any clusters or packages that are part of the second disk. We will install those packages manually after the initial install is complete.

Now we can start to customize our installation by making the following changes:

Cluster/Package	Additions
SUNWzlib	- Zip Compression Library (required by SSH)
SUNWnptr	- NTP Daemon (root)
SUNWntpu	- NTP (var)
SUNWmdr	- Solaris Volume Manager (root)
SUNWmdu	- Solaris Volume Manager (usr)
SUNWmdx	- Solaris Volume Manager Drivers
SUNWlibC	- SunWorkShop compilers libC required by system tools
SUNWadmfw	- System and Network Administrative Framework
SUNWadmc	- System Administration Core Libraries
SUNWtcpd	- TCPD access control (TCP Wrappers)
1	
Cluster/Package	Deletions
SUNWatfsr	- AutoFS (root)
SUNWatfsu	- AutoFS (usr)
SUNWftpr	- FTP Server Configuration Files
SUNWftpu	- FTP Server and Utilities
SI INW/Irehr	Varbaras Sunnart (reat)

- SUNWkrbr- Kerberos Support (root)SUNWkrbu- Kerberos Support (usr)
- SUNWIIdap LDAP development libraries
- SUNWCsndm Sendmail Support
- SUNWnisr NIS Client (root)
- SUNWnisu NIS Client (usr)
- SUNWdtcor Solaris Desktop /usr/dt File System
- SUNWinamd Internet Domain Name Server
- SUNWrcmdr Remote Network Server Commands (root)
- SUNWrcmdu Remote Network Server Commands (usr)
- SUNWtnetr Telnet Server (root)
- SUNWtnetu Telnet Server (usr)
- SUNWtnamr Trivial Name Server (root)
- SUNWtnamd \_\_\_\_\_\_ Trivial Name Server (usr)

As many packages have been removed as possible. The above lists should be fairly selfexplanatory. Some security tools have been added, such as Zlib for SSH, TCPD for access control of network services, and NTP for network time synchronization. Deletions include vulnerable network services such as FTP, Telnet, AutoFS, NIS, and LDAP. Note that some hardware platforms may require additional clusters or patches.

Select F2\_OK to exit the customization screen and return to the "Select Software" screen.

33.At the "Select Software" screen, choose **F2\_Continue**.

👻 🧭 🧟 Terminal											
<u>File Edit View Terminal Go H</u> elp											
Select Software	<b>_</b>										
Select the Solaris software to install on the system.											
NOTE: After selecting a software group, you can add or remove software by customizing it. However, this requires understanding of software dependencies and how Solaris software is packaged. The software groups displaying 64-bit contain 64-bit support.											
<pre>aisplaying 64-bit contain 64-bit support. [ ] Entire Distribution plus OEM support 64-bit 2513.00 MB [ ] Entire Distribution 64-bit</pre>											
F2_Continue F3_Go Back F4_Customize F5_Exit F6_Help	Ţ										

34.Select the disks that will be for the installation. More than one disk may be selected. In our case, only one disk is present. Select F2\_Continue.

•				🐔 Ter	minal		
<u>F</u> ile <u>E</u> d	lit <u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp			
Select	Disks						1
On thi Start approx select value.	s screen by lookir imate spa ing disks	you must ug at the uce neede s until t	selec Sugge d to i he Tot	t the disks sted Minimum nstall the s al Selected	for install field; thi oftware you value excee	ing Solaris software. s value is the Yve selected. Keep ds the Suggested Minimum	
	Disk	Device (	Size)	Avail	able Space		
	🔀 cOtOd	10 (822	2 MB)	boot disk	8222 MB	(F4 to edit)	
		}	Tot Sugges	al Selected: ted Minimum:	8222 MB 182 MB		
F2_	Continue	F3_Go	Back	F4_Edit	F5_Exit	F6_Help	T

35.No existing data (partitions) should be preserved. Select F2 Continue.



36.We have come to one of the greatest debates in UNIX Administration, disk partitioning. Most administrators prefer greater control over file system layout and will want to select **F4\_Manual** Layout.

•						🐔 Termina	al			
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> ermir	nal <u>(</u>	<u>a</u> o <u>H</u> elp	)				
Aut	tomatio	ally L	ayout	File	Systems	1?				<b>_</b>
Do Mar sk:	you wa nually ills.	nt to laying	use ai ; out f	ato-la file :	ayout to systems	automatica requires ad	lly layou vanced sy	t file syst stem admini	ems? stration	
	F2_Aut	co Layo	out	F3_G	) Back	F4_Manual	Layout	F5_Exit	F6_Help	Ţ

37.Select the appropriate disk (if there is more than one) and F4 Customize.



38.By using the arrow keys, you can navigate through the ASCII menu to layout the file system. We prefer to keep all of the core partitions under / and only break out /var separately. However, it is certainly worth noting that many administrators may not want to do this.

A good balance between security and convenience must be obtained. And since our servers are for internal use only, convenience outweighed security. Conversely, it is often recommended that /usr and /opt be separate partitions so that they may be mounted read-only, especially when providing external facing services. Bottom line, site-specific needs and personal preference go a long way here, so make sure you consider your partitioning scheme very carefully.

No matter what you decide, try to pick a standard scheme that can be used for most configurations. This will make setting up JumpStart much easier.

-						🐔 Terminal				$\Box = \Box \times$
<u>F</u> ile <u>E</u>	dit <u>V</u>	<u>/</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp					
Custon Boot 1	mize I Device	)isk: e: cO	cOtOdO tOdOsO							<b>_</b>
Entry	:					Recommended:	MB	Minimum:	MB	
Slice 0 1 2 3 4 5 6 7	Mour Swap ove: /va)	nt Po clap c	int			Size (MB) 6222 1000 8222 0 1000 0 0 0 0 0				
Es	c-2_0#	K	A F4_Option	Capac: llocat Fi	ity: ted: ree: F5_C;	8222 MB 8222 MB O MB ancel F6_Help				-

Use Esc-2 OK to exit.

39. The "File System and Disk Layout" screen provides a summary of the current disk and file system layouts. Select **F2\_Continue**.

•	🐔 Terminal							
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>T</u> erminal <u>G</u> o	<u>H</u> elp							
File System and Disk Layout			<b>_</b>					
The summary below is your cur information you've supplied.	The summary below is your current file system and disk layout, based on the information you've supplied.							
NOTE: If you choose to custom intended purpose on the disk, of the system.	NOTE: If you choose to customize, you should understand file systems, their intended purpose on the disk, and how changing them may affect the operation of the system.							
File system/Mount point	Disk/Slice	Size						
/	cOtOdOsO	6222 MB						
swap overlap	cOtOdOs1 cOtOdOs2	1000 MB 8222 MB						
/var	cOtOdOs4	1000 MB						
F2 Continue F3 Go Back	F4 Customize F5 Exit	F6 Help						
	uotomilo 10_b/10		-					
7								

40.We do not want to mount any remote (NFS) file systems. Select **F2\_Continue**.

•					🐔 Terminal	$\Box \_ \Box \times$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	Help	
Mor	unt Rer	note Fi	le Syster	ns?		<b>_</b>
Do	you wa	ant to	mount so	ftwar	e from a remote file server? This may be	
ne	cessary	7 if yo	u had to	remov	7e software because of disk space problems.	
	F2_Cor	ntinue	F3_Go	Back	F4_Remote Mounts F5_Exit F6_Help	
						-

41.The "Profile" screen summarizes your installation profile. Verify for correctness, and **F2\_Continue**.



42.Select "Auto Reboot" after the installation, and F2\_Continue.



43. The installation will begin and its progress will be displayed. The system will reboot once the installation of the Solaris 9 Software 1/2 CDROM is complete.

•						🐔 Terminal			$\Box = \Box \times$
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>T</u> erminal	<u>G</u> o	<u>H</u> elp				
									<b>_</b>
	Solari	is Init	ial Insta	11					
		MByte MByte	s Install Remaini	.ed: ng:	0.00 150.57				
			Installi	ng: I	Core Sol	aris, (Usr)			
				-					
	5				1	1	1		
	(	)	20		40	60	80	100	
									-

- 44.Because the WebStart Installer cannot run, the root password will not be set. Once the JumpStart server has rebooted, log in as root and set the root password using the **passwd** command.
- 45.Now we can proceed with the package installation from the Solaris 9 Software 2/2 CDROM. Start by ejecting the Solaris 9 Software 1/2 CDROM from the CDROM drive:

# eject cdrom

Load the Solaris 9 Software 2/2 CDROM into the CDROM drive and mount the it using the following command (Note: In most cases the CDROM drive will be /dev/dsk/c0t6d0s0. However IDE systems may be different):

# mount -F hsfs -o ro /dev/dsk/c0t2d0s0 /mnt

Change to the package directory:

```
# cd /mnt/Solaris_9/Product
```

Install the following additional packages, using the command:

# pkgadd -d . package1 [package2 package3 ...]

Additional PackagesSUNWaccr - System Accounting (root)SUNWaccu- System Accounting (usr)SUNWbash- GNU Bash Shell (required for Gzip)SUNWgcmn- Common GNU Packages (required for GNU software)

SUNWgtar	- GNU Tar Utility
SUNWgzip	- Gzip Compress Utility
SUNWsshcu	- SSH Common Utilities
SUNWsshr	- SSH Client and Utilities (root)
SUNWsshu	- SSH Client and Utilities (usr)
SUNWsshdr	- SSH Server (root)
SUNWsshdu	- SSH Server (usr)
SUNWzip	- Zip Compression Utility
SUNWzlibx	- Zlib Compression Library (64-bit)

After all of the above packages have been added, the Solaris Software 2/2 CDROM can be unmounted:

```
# cd /
# umount /mnt
```

At this point the CDROM may be safely removed, and the system should be rebooted: # init 6

- 46.Next, the latest Solaris 9 patch cluster should be downloaded from <u>http://sunsolve.sun.com</u> to a secure intermediate location and burned to a CDROM. The CDROM can then be mounted on the JumpStart server to install the patches:
  - # cp /mnt/9\_Recommended.zip /tmp
  - # cd /tmp
  - # unzip 9\_Recommended.zip
  - # cd 9\_Recommended
  - # ./install\_cluster

Since this is a minimal installation, you will see many errors during the patch process. Most of the errors should be "return code 8", which indicates that the target packages are not installed, and can safely be ignored. "return code 2" indicates the patch has already been applied and can be ignored as well. After the patch cluster has been successfully installed, the CDROM can be unmounted and removed, then server should be rebooted.

47.First, /etc/inetd.conf needs to be modified to remove any unnecessary services. Make a copy of the original inetd.conf:

# cp /etc/inetd.conf /etc/inetd.conf.orig

Remove all services except TFTP:

# echo "Only Services for JumpStart" > /etc/inetd.conf # echo "tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot" >> /etc/inetd.conf

48.By default, TCP Wrappers are not enabled. Will enable them with these commands:

- # echo "ENABLE\_CONNECTION\_LOGGING=YES" \
- > >> /etc/default/inetd
- # echo "ENABLE\_TCPWRAPPERS=YES" >> /etc/default/inetd

Now, we configure TCP Wrappers to accept TFP and SSH connections on the private network by

creating the /etc/hosts.allow file with the following commands:

# echo "in.tftpd: 192.168.0.0" > /etc/hosts.allow
# echo "in.sshd: 192.168.0.0" >> /etc/hosts.allow

Next, we create the /etc/hosts.deny file to block all other services from any host except the localhost:

# echo "ALL: ALL EXCEPT localhost : DENY" > /etc/hosts.deny

49.Logging of all failed authentication attempts should be enabled by the commands:

# echo "SYSLOG\_FAILED\_LOGINS=0" >> /etc/default/login

- # echo "auth.notice /var/log/authlog" >> \
- > /etc/syslog.conf
- # touch /var/log/authlog
- # chmod 600 /var/log/authlog

Logging of all SU attempts should be enabled by the commands:

- # touch /var/log/sulog
- # chmod 600 /var/log/sulog

50.A default banner message should be configured using the command:

```
# echo "Authorized Uses Only." > /etc/issue
```

Next, make sure SSH displays the banner message with the following command: # echo "Banner /etc/issue" >> /etc/ssh/sshd config

51.NTP should be configured by creating the following /etc/inet/ntp.conf file and creating the drift file.

```
# cat > /etc/inet/ntp.conf <<EOF
restrict default nomodify
restrict 192.168.0.5
restrict 192.168.0.6
restrict 127.0.0.1
server 192.168.0.5
server 192.168.0.6
driftfile /var/ntp/ntp.drift
EOF
# touch /var/ntp/ntp.drift</pre>
```

52. We need to disable any unnecessary services that are started at boot time in the /etc/rc2.d directory. (Note: RPC is required for bootp, a necessary component of the JumpStart server. However, RPC will be disabled on all clients.)

- # cd /etc/rc2.d
- # rm S711dap.client S73cachefs.daemon S76nscd \
- > S89PRESERVE S93cacheos.finish

53. Finally, we create an administrator user account that can used to connect via SSH and if necessary, SU to root:

```
# useradd -g 10 -d /export/home/admin -m -c "Admin User" \
> -s /usr/bin/bash admin
```

Be sure and set a password for the admin user:

# passwd admin
New Password:
Re-enter new Password:
passwd: password successfully changed for admin

54.Last, reboot the server so that all the above changes will take effect.

# init 6

### Installation (JumpStart Server)

JumpStart consists of three core components, installation, identification, and configuration. The installation component contains all of the installation media. The identification component holds individual host client information, such as: IP address, host name, etc. The configuration component mandates how JumpStart behaves. All of these most components are shared over NFS so that JumpStart clients can access this information during installation. We will organize each of the components into a separate directory.

Installation Component: **# mkdir /export/install** Identification Component:

# mkdir /export/sysidcfg

Configuration Component: # mkdir /export/jumpstart

To share these components, we add the following line to the /etc/dfs/dfstab. The "-o ro=@*IP address*" option restricts NFS to be read-only to a specific IP address or range of addresses. (Note: The anon=0 is required for JumpStart to operate properly).

```
# cat > /etc/dfs/dfstab <<EOF
share -F nfs -o ro=@192.168.0.0,anon=0 /export/install
share -F nfs -o ro=@192.168.0.0,anon=0 /export/jumpstart
share -F nfs -o ro=@192.168.0.0,anon=0 /export/sysidcfg
EOF</pre>
```

The following command will start sharing the directories:

# shareall

In case we decide to add additional Solaris versions in the future, we will create a sparc9 directory to hold the installation files in /export/install, and a sparc9 directory to hold the configuration files in /export/jumpstart.

```
# mkdir /export/jumpstart/sparc9 /export/install/sparc9
```

The next step is to install the installation media on the JumpStart server in the /export/install/sparc9 directory. Insert and mount the Solaris 9 Software1/2 CDROM, as we have previously.

```
# cd /mnt/Solaris_9/Tools
```

```
# ./setup_install_server /export/install/sparc9
```

Next, copy the JumpStart configuration check tool and sample JumpStart rules files to the configuration directory. The check tool verifies any rules that are created to define a JumpStart session, and the rules file contains the JumpStart session definitions.

- # cd ../Misc/jumpstart\_sample
- # cp check /export/jumpstart
- # cp rules /export/jumpstart

Now, unmount and eject the Solaris 9 Software 1/2 CDROM, and insert and mount the Solaris 9

#### Software 2/2 CDROM.

# # cd /mnt/Solaris\_9/Tools # ./add\_to\_install\_server /export/install/sparc9

Once the operation is complete, unmount and eject the Solaris 9 Software 2/2 CDROM.

Now, we need to set up some basic configuration files for JumpStart. These configuration files are specified in the /export/jumpstart/rules file (see Appendix A for more information the rules file). There are three types of configuration files that can used in the rules file: begin scripts, profiles, and finish scripts.

Begin Scripts	– An optional Bourne shell script that is executed before installation begins.
	This can be useful for copying configuration files to the client before
	installation, but in reality, it is seldom used. Our implementation of
	JumpStart does not require the use of begin scripts.

- Profiles A text file that is used as a template by JumpStart, which defines how to install the Solaris operating system.
- Finish Script An optional Bourne script that is executed after installation is complete. This is useful for installing patches, third-party software, and updating configuration files.

Because different Sun hardware may have different sized hard drives we will create three different profiles (Appendix B), one profile for drives < 18 GB (small.profile), one profile for drives > 18 GB (default.profile), and one for drives > 36 GB (large.profile). Each profile specifies the:

- install\_type upgrade, flash, or initial
  geo geographic location
- locale language set
- cluster software cluster
- partitioning defines whether or not to use auto-sizing
- filesys defines each partition's location and size
- package adds or removes additional packages (we use the same additional packages we specified for the JumpStart server, except for any components that are unique requirements for JumpStart).

Now that we have defined the basic installation, we need to add a finish script to perform the hardening and configuration. But first, we need to add some directories to the /export/jumpstart/sparc9 directory to help keep everything organized. We will create a "files" directory to hold JumpStart client configuration files, a "software" directory to hold third-party applications, and a "patches" directory to place an uncompressed copy of the latest Solaris 9 patch cluster.

- # mkdir /export/jumpstart/files \
- > /export/jumpstart/software \

#### > /export/jumpstart/patches

The finish script (see Appendix C for detailed information) requires some trial and error to get perfect. The most import item to remember is that when the finish script is executed after the installation, the root of the newly installed drive is mounted on /a not /. So, all modifications, package

installations, and patch installation must be modified to use /a as the base directory. We created two different finish scripts. One performs disk mirroring (default-end.sh), and the other does not (nomirror-end.sh). Share have been and the second of the second

### Installation (JumpStart Client)

Each JumpStart client requires a "sysidcfg" file. This tells JumpStart about the basic identification information needed to install a client. JumpStart looks for a file named "sysidcfg" in a location that you provide when setting up the JumpStart client. We have found the best way to handle this is to make a new directory for each JumpStart client in the /export/sysidcfg directory. The new directory is named after the *hostname* of the client, and contains a single sysidcfg file for that specific client. sysidcfg files contain the following information (an example can be found in Appendix D):

- system local language set
- name\_service type of naming service to use
- network\_interface network parameters
- security\_policy security policy type
- root\_password the root password in hash form
- timezone default timezone
- timehost where to set the from
  - terminal terminal type

The next steps may be performed in variety of ways. We have found the setup of jumpstart clients to be a manual and tedious procedure. So, we created a script called "/export/jumpstart/setup-client" (Appendix E) to automate the process. It is possible to do the set up manually, using the /export/install/sparc9/Solaris\_9/Tools/add\_install\_client script (see the MAN page for detailed instructions on its usage). To help you understand the process, here is the procedure that the setup-client script performs:

1. setup-client accepts a number of arguments to determine what type of installation should be performed. The syntax is as follows:

setup-client [-n] [-s | -l] <hostname> <IP\_Addr> <MAC\_Addr> -n = nomirror: Turns off automatic root disk mirroring (optional) -s | -l = small | large: Disk size/layout hostname = Desired hostname of the new client IP\_Addr = Desired IP address of the new client (must be 192.168.0.x) MAC\_Addr = MAC address for the primary interface of the new client

- 2. First, setup-client checks to see if any of the disk parameters have been entered, if not then defaults of "mirroring enabled" and "default disk size" are taken.
- 3. Then setup-client determines if this JumpStart client has any previous configuration entries that might conflict with its operation. If so, setup-client issues an error requesting that the problem be fixed. Otherwise, execution continues.
- 4. setup-client adds an entry to /etc/hosts for the JumpStart client.
- 5. setup-client adds an entry to /etc/ethers for the JumpStart client.
- 6. Now, setup-client creates a sysidcfg file for the JumpStart client in /export/sysidcfg/*hostname*/sysidcfg.
- 7. Next, setup-client adds a rule to the /export/jumpstart/rules file based on the disk layout parameters specified.
- 8. setup-client uses /export/jumpstart/check to verify and commit the rule file.

- 9. Then, setup-client performs the /export/install/sparc9/Solaris\_9/Tools/add\_install\_client command to set up the /tftpboot network boot image and the /etc/bootparams file.
- 10. Finally, setup-client logs the successful completion and date to /export/jumpstart/client.log

Now, we can use the setup-client tool to add our JumpStart client to the server.

- # cd /export/jumpstart
- # ./setup-client -n -s server1 192.168.0.20 0:3:ba:27:b5:6f

Finally, The JumpStart client is ready for installation. To proceed with the installation, we attach the client to the private JumpStart network. Then we power on the client. After the initial banner message, we issue a break using **stop-a** and at the OK prompt we issue the following command:

#### ok boot net - install

The installation will now proceed unattended through completion. Installation times vary from about thirty minutes to several hours, depending on the speed of the client.

© SANS Institute 2004,

### Testing

Before the JumpStart server can be used safely, we need to conduct some tests to verify its security.

1. SSH as the "admin" user to the JumpStart server from a host on the private network (the only network allowed by TCP Wrappers to SSH to our server). We should be able to successfully connect.

```
# ssh admin@192.168.0.10
admin's password:
Authentication Successful.
...
```

2. SSH as the "admin" user to the JumpStart server from a host not on the private network. TCP Wrappers should not allow you to connect.

```
# ssh admin@192.168.0.10
warning: Authentication failed.
Disconnected (local); connection lost (Connection
closed by remote host.).
```

3. SSH as "root" to the JumpStart server from a host on the private network. Root log in is disallowed; you should not be able to connect.

```
# ssh root@192.168.0.10
admin's password:
admin's password:
admin's password:
Disconnected; no more authentication methods available
(No further authentication methods available.).
```

4. Make several botched log in attempts, then examine the /var/log/authlog to ensure that failed log ins are being logged. For example:

```
Aug 3 08:20:55 192.168.0.10 sshd[5801]: [ID 702911 auth.warning] Wrong password given for user 'admin'.
```

5. SU from the "admin" user to "root". Then, SU from the "admin" user to "root", and intentionally botch the password. Check the /var/log/sulog to ensure that both successful and unsuccessful SU attempts are logged. Successful:

```
SU 08/03 08:24 + pts/5 admin-root
Unsuccessful:
SU 08/03 08:25 - pts/5 admin-root
```

6. Examine the output of the mount command to ensure that all files systems are logging. Look for the "logging" attribute for each mounted filesystem partition. For example: / on /dev/dsk/c0t0d0s0 read/write/setuid/intr/ largefiles/logging/xattr... 7. Perform a **ps** -ef and examine all running processes. Be sure that nothing is out of place or unaccounted for. Look for the following processes, and investigate discrepancies:

```
sched
/etc/init -
pageout
fsflush
/usr/lib/saf/sac -t 300
/usr/sbin/auditd
/usr/sbin/cron
/usr/lib/sysevent/syseventd
/usr/lib/picl/picld
/usr/sbin/rpcbind
/usr/sbin/inetd -s
/usr/lib/inet/xntpd
/usr/lib/nfs/lockd
/usr/lib/nfs/statd
/usr/sbin/syslogd -t
/usr/sbin/nscd
/usr/lib/utmpd
/usr/sbin/in.rarpd -a
/usr/lib/saf/ttymon
/usr/lib/nfs/nfsd
/usr/sbin/rpc.bootparamd
/usr/lib/nfs/mountd
/usr/local/sbin/sshd2
```

8. Use NMAP to scan the JumpStart server for open ports. Any ports other than those listed below need to be investigated and secured.

# nmap 192.168.0.10

Starting nmap 3.50
Interesting ports on jumpstart (192.168.0.10):
The 1657 ports scanned but not shown below are in
state: closed)
PORT STATE SERVICE
22/tcp open ssh
111/tcp open rpcbind
2049/tcp open nfs
4045/tcp open lockd
32771/tcp open sometimes-rpc5
32778/tcp open sometimes-rpc19

9. Use Nessus to perform more detailed vulnerability scans. After scanning our JumpStart server, there were no unexpected abnormalities. RPC and NFS are of the greatest risk. But, our exposure is limited by the firewall and private network.

Host	<b>Port/Service</b>	Issue
192.168.0.10	ssh (22/tcp)	Security Notes
192.168.0.10	rpc (111/tcp)	Security Warning
192.168.0.10	nfs (2049/tcp)	Security Warning
192.168.0.10	general icmp	Security Warning
192.168.0.10	general tcp	Security Notes
192.168.0.10	general tcp	Security Warning

10.Test that NFS is restricted to the private network. First, use a host on the private network to mount a NFS share. This should be successful for read-only mounts. Then try to mount a NFS share from a host not on the private network. You should not be able to mount a share. Private:

```
# mount 192.168.0.10:/export/install /mnt
#
```

Non-Private:

```
# mount 192.168.0.10:/export/install /mnt
nfs mount: 192.168.0.10:/export/install: Permission
denied
```

11.Last, verify that NTP is working correctly by executing the following command (the output should be similar that which is displayed below):

```
# ntptrace
localhost: stratum 16, offset 0.000073, synch distance
1.00066
192.168.0.5: stratum 3, offset 0.000026, synch
distance 1.00086
192.168.0.6: stratum 3, offset 0.000079, synch
distance 1.00122
```

### **Ongoing Maintenance**

1. Backups

As mentioned earlier, backups will not be performed on a regularly scheduled basis. However, backups will be performed whenever changes are made to the JumpStart server, such as, after applying patches or making configuration changes. We will make an initial backup of each mounted UFS filesystem using TAR, and burn the the tar files to a CDROM. Thereafter, the same procedure for backups will be followed after any patching or configuration changes.

# tar cvf root.`date`.tar /
# tar cvf var.`date`.tar /var

2. Log Rotation

Log rotation is an important part of administration. Log files must be rotated to conserve disk space; ever growing log files can consume a partition. Rotating log files also makes it easier to search through the log files when you are looking for something specific. Log rotation in Solaris 9 is much improved over previous versions. It is now accomplished by a tool called LOGADM. LOGADM should already be set up to run from cron nightly as part of the default Solaris installation. By default, the configuration file, /etc/logadm.conf, contains entries for syslog, messages, cron, lpsched, and process accounting. You will probably want to make additions to these defaults. For example, to rotate /var/log/authlog:

#### # echo ``/var/log/authlog -C 8 -P '`date`' -a 'kill -HUP `cat /var/run/syslog.pid`'"

3. Log Monitoring

Log monitoring can be accomplished in a multitude of ways, from manual observations to complex scripts and utilities. Programs such as LogCheck <u>http://sourceforge.net/projects/sentrytools/</u> can monitor log files and email an administrator when anything suspicious is noted. Also, many administrators prefer to send all syslog entries to a remote syslog server, so they can monitor everything centrally. While others, prefer to keep all the logging local. There are pros and cons to all of these options.

For simplicity, we will keep all the logging local to the JumpStart server. Weekly, we will manually review the syslog, messages, and authlog files for any anomalies.

4. Patching

Patching is one of the single most important proactive things that you can do to help prevent problems and attacks. There are several methods available for patching Solaris servers. First, Patch Manager, from Sun, can examine your system, find out what patches are available / needed, and automatically apply the patches. Second, PatchDiag, from Sun, can also identify which patches are available / needed, but will not automatically install them. Third, Sun provides patch clusters of the most commonly needed patches and all critical security patches for download from http://sunsolve.sun.com.

Again, for simplicity, we will download the newest patch cluster on the first of each month and install it manually. Installation instructions can be found in the README file of the patch cluster.

#### 5. Password Maintenance

Passwords are one of the weakest links in the security chain. A good password scheme is dependent on choosing adequately strong passwords, keeping passwords secrete, as well as changing passwords often.

Choosing strong passwords is not difficult, but often over-looked. Secure passwords can be generated by a random password generator, such as <u>http://www.multicians.org/thvv/gpw.html</u>. Or, a simple recipe, such as:

- A. Take a phrase such as: I have a yellow dog named sam.
- B. Take the first letter of each word: Ihaydns
- C. Change some of the letters to numbers and mix capitalization: !hAydn5

We will use a password generator to create our strong passwords.

Passwords must be kept secrete to remain effective. That means that only trusted administrators should have access to the root password. Do not send passwords in email, unless encrypted. Do not write passwords down... no sticky notes taped to the underside of your keyboard!

Passwords must be changed regularly. No matter how hard you try, passwords will "leak" out. We will change our passwords monthly. Making password maintenance part of your patching routine is a good way to remember.

6. Permissions

Many systems files have permissions that are not strict enough, possibly allowing an attacker to modify critical system files, or insert malicious code. Tools, such as Fix-Modes <a href="http://mrtg.stanford.edu/SECURITY/Scripts/fix-modes/">http://mrtg.stanford.edu/SECURITY/Scripts/fix-modes/</a>, should be used regularly to insure that file permissions are kept secure. Be sure to run Fix-Modes after any patches applied, as the patches may reset file permissions.

Additional tools, such as TripWire <u>http://www.tripwire.com/products/tripwire\_asr/</u>, can be used with cron to constantly monitor for any file changes and send an email if changes occur. Initially, TripWire creates a baseline MD5 checksum of each file. Each time TripWire is run, it recomputes the checksum of each and compares it with the baseline checksum. If they do not match, an alert is sent via email.

#### 7. General Monitoring

General monitoring is useful for keeps tabs on things like disk utilization, CPU utilization, swap file usage, memory utilization, etc. We use a proprietary software package from Concord <u>http://www.concord.com</u> to monitor our systems over the network via SNMP. It's installation is beyond the scope of this document. However, there are free solutions as well. SRS Net Connect <u>http://srsnetconnect.sun.com</u> from Sun provides basic system monitoring and email alerts at no charge. If you have Sun support, it will also analyze your systems on a monthly basis for security and configuration vulnerabilities.

### **Appendix A - rules**

# # @(#)rules 1.12 94/07/27 SMI # # The rules file is a text file used to create the rules.ok file for # a custom JumpStart installation. The rules file is a lookup table # consisting of one or more rules that define matches between system # attributes and profiles. # # This example rules file contains: o syntax of a rule used in the rules file # # o rule keyword and rule value descriptions # o rule examples # # See the installation manual for a complete description of the rules file. # # # **# RULE SYNTAX:** # # [!]rule keyword rule value [&& [!]rule keyword rule value]... begin profile finish # "[]" indicates an optional expression or field # # "..." indicates the preceding expression may be repeated "&&" used to "logically AND" rule keyword and rule value pairs together # # "!" indicates negation of the following rule keyword # # rule keyword a predefined keyword that describes a general system attribute. It is used with the rule value to match a # # system with the same attribute to a profile. # # rule value a value that provides the specific system attribute # for the corresponding rule keyword. A rule value can # be text or a range of values (NN-MM). # To match a range of values, a system's value must be # greater than or equal to NN and less than or equal to MM. # # begin a file name of an optional Bourne shell script # that will be executed before the installation begins. # If no begin script exists, you must enter a minus sign (-) # in this field. # # profile a file name of a text file used as a template by the # custom JumpStart installation software that defines how # to install Solaris on a system. #

```
# finish
           a file name of an optional Bourne shell script
#
          that will be executed after the installation completes.
#
          If no finish script exists, you must enter a minus sign (-)
#
          in this field.
#
# Notes:
# 1. You can add comments after the pound sign (#) anywhere on a line.
# 2. Rules are matched in descending order: first rule through the last rule.
# 3. Rules can be continued to a new line by using the backslash (\) before
  the carriage return.
#
# 4. Don't use the "*" character or other shell wildcards, because the rules
#
  file is interpreted by a Bourne shell script.
#
#
#
# RULE KEYWORD AND RULE VALUE DESCRIPTIONS
#
#
# rule keyword rule value Type
                                rule value Description
# -----
           minus sign (-) always matches
# any
# arch
           text system's architecture type
# domainname text
                            system's domain name
# disksize
                           system's disk size
            text range
#
                       disk device name (text)
#
                       disk size (MBytes range)
                          system's host name
# hostname
             text
# installed
                          system's installed version of Solaris
            text text
                       disk device name (text)
#
#
                       OS release (text)
                        system's kernel architecture
# karch
            text
# memsize
                           system's memory size (MBytes range)
           range
# model
            'text'
                         system's model number
                         system's IP address
# network
            text
# totaldisk
                          system's total disk size (MBytes range)
            range
#
#
*****
#
# RULE EXAMPLES
#
# The following rule matches only one system:
#
#hostname sample host -
                          host class
                                      set root pw
#
# The following rule matches any system that is on the 924.222.43.0 network
# and has the sun4c kernel architecture:
```

# Note: The backslash (\) is used to continue the rule to a new line. # #network 924.222.43.0 && \ # karch sun4c - net924 sun4c # # The following rule matches any sparc system with a c0t3d0 disk that is # between 400 to 600 MBytes and has Solaris 2.1 installed on it: # #arch sparc &&  $\$ # disksize c0t3d0 400-600 && \ # installed c0t3d0s0 solaris 2.1 - upgrade -# # The following rule matches any system: # #any - - any machine -# \*\*\*\*\*\* # **# BEGIN ACTUAL RULES** hostname server1 - ./sparc9/small.profile ./sparc9/nomirror-end.sh hostname server2 - ./sparc9/large.profile ./sparc9/default-end.sh

hostname server3 - ./sparc9/default.profile ./sparc9/default-end.sh

## Appendix B – small.profile

install_type	initial_install		
geo	N_America		
locale	С		
cluster	SUNWCcore		
partitioning	explicit		
filesys	rootdisk.s0 free	/	logging
filesys	rootdisk.s1 1025	swap	<u></u>
filesys	rootdisk.s4 1025	/var	logging
filesys	rootdisk.s5 12	unnam	led
package	SUNWzlib	add	
package	SUNWzlibx	add	
package	SUNWntpr	add	
package	SUNWntpu	add	
package	SUNWmdr	add	
package	SUNWmdu	add	
package	SUNWlibC	add	
package	SUNWadm	fw add	
package	SUNWadme	e add	
package	SUNWtcpd	add	
package	SUNWaccr	add	
package	SUNWaccu	add	
package	SUNWbash	add	
package	SUNWgcm	n add	
package	SUNWgtar	add	
package	SUNWgzip	add	
package	SUNWzip	add	
package	SUNWsshd	radd	
package	SUNWsshd	u add	
package	SUNWsshr	add	
package	SUNWsshu	add	
package	SUNWatfsr	delete	
package	SUNWatfsu	delete	
package	SUNWftpr	delete	
package	SUNWkrbr	delete	
package	SUNWkrbu	delete	
package	SUNWIIdap	delete	
package	SUNWCsnd	lm delete	
package	SUNWnisr	delete	
package	SUNWnisu	delete	
package	SUNWdtcor	delete	
package	SUNWinam	d delete	
package	SUNWreme	lr delete	
package	SUNWreme	lu delete	
package	SUNWtnetr	delete	
package	SUNWtnetu	delete	
package	SUNWtnam	r delete	

package package package	SUNWtnamd SUNWtftp SUNWtftpr	delete delete delete	

## Appendix B (cont.) – default.profile

install_type	initial_install			
geo	N_America			
locale	C			
cluster	SUNWCcore			
partitioning	explicit			
filesys	rootdisk.s0 free	;	/	logging
filesys	rootdisk.s1 410	0	swap	
filesys	rootdisk.s4 410	0	/var	logging
filesys	rootdisk.s5 12		unnam	ed
package	SUNWzlib		add	
package	SUNWzlibz	X	add	
package	SUNWntpr	•	add	
package	SUNWntpu	ı	add	
package	SUNWmdr	•	add	
package	SUNWmdu	l	add	
package	SUNWlibC	1	add	
package	SUNWadm	nfw	add	
package	SUNWadm	IC	add	
package	SUNWtcpd	l	add	
package	SUNWaccr	•	add	
package	SUNWaccu	1	add	
package	SUNWbash	1	add	
package	SUNWgcm	n	add	
package	SUNWgtar		add	
package	SUNWgzip	)	add	
package	SUNWzip		add	
package	SUNWsshd	lr 🛛	add	
package	SUNWsshd	łu	add	
package	SUNWsshr		add	
package	SUNWsshu	ı	add	
package	SUNWatfs	r	delete	
package	SUNWatfsı	u	delete	
package	SUNWftpr		delete	
package	SUNWkrbr	•	delete	
package	SUNWkrbu	1	delete	
package	SUNWIIda	р	delete	
package	SUNWCsn	dm	delete	
package	SUNWnisr		delete	
package	SUNWnisu	l	delete	
package	SUNWdtco	or	delete	
package	SUNWinan	nd	delete	
package	SUNWrcme	dr	delete	
package	SUNWrcme	du	delete	
package	SUNWtnet	r	delete	
package	SUNWtnet	u	delete	
package	SUNWtnan	nr	delete	

package package package	SUNWtnamd SUNWtftp SUNWtftpr	delete delete delete	

## Appendix B (cont.) - large.profile

install_type	initial_install			
geo	N_America			
locale	C			
cluster	SUNWCcore			
partitioning	explicit			
filesys	rootdisk.s0 fre	ee	/	logging
filesys	rootdisk.s1 82	200	swap	<u></u>
filesys	rootdisk.s4 82	200	/var	logging
filesys	rootdisk.s5 12	2	unnam	ed
package	SUNWzli	ib	add	
package	SUNWzli	ibx	add	
package	SUNWntj	pr	add	
package	SUNWnt	pu	add	
package	SUNWm	dr	add	
package	SUNWmo	du	add	
package	SUNWlib	bС	add	
package	SUNWad	lmfw	add	
package	SUNWad	lmc	add	
package	SUNWter	pd	add	
package	SUNWac	cr	add	
package	SUNWac	cu	add	
package	SUNWba	sh	add	
package	SUNWgc	mn	add	
package	SUNWgta	ar	add	
package	SUNWgz	zip	add	
package	SUNWzij	p	add	
package	SUNWss	hdr 🕐	add	
package	SUNWssl	hdu	add	
package	SUNWssl	hr	add	
package	SUNWssl	hu	add	
package	SUNWath	fsr	delete	
package	SUNWath	fsu	delete	
package	SUNWftr	or	delete	
package	SUNWkr	br	delete	
package	SUNWkr	bu	delete	
package	SUNWIId	lap	delete	
package	<b>SUNWC</b>	sndm	delete	
package	SUNWnis	sr	delete	
package	SUNWnis	su	delete	
package	SUNWdto	cor	delete	
package	SUNWina	amd	delete	
package	SUNWrci	mdr	delete	
package	SUNWrci	mdu	delete	
package	SUNWtne	etr	delete	
package	SUNWthe	etu	delete	
package	SUNWtna	amr	delete	

package package package	SUNWtnamd SUNWtftp SUNWtftpr	delete delete delete	

#### Appendix C – default-end.sh

#!/sbin/sh

# Declare Variables
#
BASE=/a
MNT=/a/mnt
ADMIN\_FILE=/a/tmp/admin
mount -f nfs 192.168.0.10:/export/jumpstart/sparc9 \${MNT}

# Copy, change, or create all those files for which settings need to be customized
#
echo "\*\*\* Copying / Modifying configuration files \*\*\*"

# Backup and remove all entries from /etc/inetd.conf cp \${BASE}/etc/inetd.conf cp /dev/null \${BASE}/etc/inetd.conf.orig \${BASE}/etc/inetd.conf

# Install TCP Wrappers
echo "ENABLE\_CONNECTION\_LOGGING=YES" >> \${BASE}/etc/default/inetd
echo "ENABLE\_TCPWRAPPERS=YES" >> \${BASE}/etc/default/inetd
echo "in.tftpd: 192.168.0.0" >> \${BASE}/etc/hosts.allow
echo "in.sshd: 192.168.0.0" >> \${BASE}/etc/hosts.allow
echo "ALL: ALL EXCEPT localhost : DENY" > \${BASE}/etc/hosts.deny

# Log failed authentications and SU attempts echo "SYSLOG\_FAILED\_LOGINS=0" >> \${BASE}/etc/default/login echo "auth.notice /var/log/authlog" >> /etc/syslog.conf touch \${BASE} /var/log/authlog chmod 600 \${BASE} /var/log/authlog touch \${BASE}/var/log/sulog chmod 600 \${BASE}/var/log/sulog

# Set default banner message
echo "Authorized Uses Only." > \${BASE}/etc/issue

# Set default banner for SSH
echo "Banner /etc/issue" >> \${BASE}/etc/ssh/sshd\_config

# Set up NTP Client cat > \$ {BASE}/etc/inet/ntp.conf <<EOF restrict default nomodify restrict 192.168.0.5 restrict 192.168.0.6 restrict 127.0.0.1 server 192.168.0.5 server 192.168.0.6 driftfile /var/ntp/ntp.drift EOF touch \${BASE}/var/ntp/ntp.drift

# Disable Unnecessary service in /etc/rc2.d
rm \${BASE}/etc/rc2.d/S711dap.client \${BASE}/etc/rc2.d/S71rpc \
\${BASE}/etc/rc2.d/S73cachefs.daemon \${BASE}/etc/rc2.d/S76nscd \
\${BASE}/etc/rc2.d/S89PRESERVE \${BASE}/etc/rc2.d/S93cacheos.finish

#Install the mirror script from the "files" directory (see Appendix F for the mirror script) cp \${SI\_CONFIG\_DIR}/sparc9/files/mirror \${BASE}/etc/rc2.d/S99mirror chmod +x \${BASE}/etc/rc2.d/S99mirror

```
## EXAMPLE - Add Third party packages / software from the "software" directory
## Enable by removing first column of comments
##
#echo "*** Adding third party packages and software ***'
#
#mkdir ${BASE}/usr/local
#cat >${ADMIN FILE} <<EOF</pre>
#mail=root
#instance=overwrite
#partial=nocheck
#runlevel=nocheck
#idepend=nocheck
#rdepend=nocheck
#space=ask
#setuid=nocheck
#conflict=nocheck
#action=nocheck
#basedir=default
#EOF
#
#echo " ...installing packages."
#/usr/sbin/pkgadd -a ${ADMIN_FILE} -n -d ${MNT}/software/coreutils-4.5.4-sol9-sparc-local \
#-R ${BASE} <<EOF
#all
#EOF
```

# Install recommended patch cluster
# Get the patches from the "patch" directory
echo "\*\*\* Installing recommended patch cluster \*\*\*"

cp /etc/mnttab  $\{BASE\}/etc/mnntab cd {MNT}/patches/9_Recommended; /usr/sbin/patchadd -R <math display="inline">\{BASE\}$  -M . ./patch\_order -u;  $\ cd \{BASE\}$ 

sleep 30

umount \${MNT} # # # End script

Contraction of the second of t

#### Appendix C (cont.) – nomirror-end.sh

#!/sbin/sh

# Declare Variables
#
BASE=/a
MNT=/a/mnt
ADMIN\_FILE=/a/tmp/admin
mount -f nfs 192.168.0.10:/export/jumpstart/sparc9 \${MNT}

# Copy, change, or create all those files for which settings need to be customized
#
echo "\*\*\* Copying / Modifying configuration files \*\*\*"

# Backup and remove all entries from /etc/inetd.conf cp \${BASE}/etc/inetd.conf cp /dev/null \${BASE}/etc/inetd.conf.orig \${BASE}/etc/inetd.conf

# Install TCP Wrappers
echo "ENABLE\_CONNECTION\_LOGGING=YES" >> \${BASE}/etc/default/inetd
echo "ENABLE\_TCPWRAPPERS=YES" >> \${BASE}/etc/default/inetd
echo "in.tftpd: 192.168.0.0" >> \${BASE}/etc/hosts.allow
echo "in.sshd: 192.168.0.0" >> \${BASE}/etc/hosts.allow
echo "ALL: ALL EXCEPT localhost : DENY" > \${BASE}/etc/hosts.deny

# Log failed authentications and SU attempts echo "SYSLOG\_FAILED\_LOGINS=0" >> \${BASE}/etc/default/login echo "auth.notice /var/log/authlog" >> /etc/syslog.conf touch \${BASE} /var/log/authlog chmod 600 \${BASE} /var/log/authlog touch \${BASE}/var/log/sulog chmod 600 \${BASE}/var/log/sulog

# Set default banner message
echo "Authorized Uses Only." > \${BASE}/etc/issue

# Set default banner for SSH
echo "Banner /etc/issue" >> \${BASE}/etc/ssh/sshd\_config

# Set up NTP Client cat > \$ {BASE}/etc/inet/ntp.conf <<EOF restrict default nomodify restrict 192.168.0.5 restrict 192.168.0.6 restrict 127.0.0.1 server 192.168.0.5 server 192.168.0.6 driftfile /var/ntp/ntp.drift EOF touch \${BASE}/var/ntp/ntp.drift

# Disable Unnecessary service in /etc/rc2.d
rm \${BASE}/etc/rc2.d/S711dap.client \${BASE}/etc/rc2.d/S71rpc\
\${BASE}/etc/rc2.d/S73cachefs.daemon \${BASE}/etc/rc2.d/S76nscd \
\${BASE}/etc/rc2.d/S89PRESERVE \${BASE}/etc/rc2.d/S93cacheos.finish

# DO NOT need to copy a mirroring script. This is the nomirror script.# See the "default-end-sh" (Appendix C) script and the# "mirror" script (Appendix F) for more information.

```
## EXAMPLE - Add Third party packages / software from the "software" directory
## Enable by removing first column of comments
##
#echo "*** Adding third party packages and software ***
#
#mkdir ${BASE}/usr/local
#cat >${ADMIN FILE} <<EOF</pre>
#mail=root
#instance=overwrite
#partial=nocheck
#runlevel=nocheck
#idepend=nocheck
#rdepend=nocheck
#space=ask
#setuid=nocheck
#conflict=nocheck
#action=nocheck
#basedir=default
#EOF
#
#echo " ...installing packages."
#/usr/sbin/pkgadd -a ${ADMIN_FILE} -n -d ${MNT}/software/coreutils-4.5.4-sol9-sparc-local \
#-R ${BASE} <<EOF
#all
#EOF
```

# Install recommended patch cluster
# Get the patches from the "patch" directory
echo "\*\*\* Installing recommended patch cluster \*\*\*"

sleep 30

umount \${MNT} # # # End script

Contraction of the second of t

#### Appendix D (cont.) - sysidcfg

system\_locale=C name service=NONE network interface=primary {hostname=server1 ip\_address=192.168.0.20 And the second of the second o netmask=255.255.255.0 protocol ipv6=no security\_policy=NONE root password=H5o.sHX3wB6 timezone=US/Central timeserver=localhost terminal=vt100

### Appendix E – setup-client

#!/sbin/sh

```
Usage() {
       echo"
       echo 'This is a small utility to setup new Solaris 9 Jumpstart clients. This works'
       echo 'for 99% of clients. Known limitations include: mirroring only works on'
       echo 'clients with scsi/fiber disks on c0 or c1, and x86 clients are not supported.'
       echo"
       echo 'Usage: setup-client [-n] [-s | -l] <8 | 9> <hostname> <IP Addr> <MAC Addr>'
                     = nomirror: Turns off automatic root disk mirroring (optional)'
       echo'-n
       echo' -s \mid -l = small \mid large: Disk size/layout
                                                                (optional)'
       echo ' 8 | 9 = Solaris Version'
       echo ' hostname = Desired hostname of the new client'
       echo' IP Addr = Desired IP address of the new client (must be 192.168.0.x)'
       echo' MAC Addr = MAC address for the primary interface of the new client'
       echo "
       echo 'Example: setup-client
                                      9 foo 10.10.10.10 0:3:ba:2e:99:1d'
       echo 'Example: setup-client -n -s 8 foo 10.10.10.10 0:3:ba:2e:99:1d'
       echo "
       exit 1
}
NOMIRROR="default"
DISK="default"
while getopts 'lns' c
do
       case $c in
              1) DISK="large" ;;
              n) NOMIRROR="nomirror" ;;
              s) DISK="small" ;;
              *) Usage ;;
       esac
done
shift `expr $OPTIND - 1`
if [ ${NOMIRROR} != "default" ]
then
       echo "Root disk mirroring has been set to ${NOMIRROR}"
fi
if [ ${DISK} != "default" ]
then
       echo "Disk size/layout has been set to ${DISK}"
fi
```

```
if [ $# != 4 ]
then
Usage
exit 1
fi
```

```
# echo "exiting test... DISK=${DISK}, NOMIRROR=${NOMIRROR}"
# exit 0
```

```
VERSION=9
HOST NAME=$2
IP ADDR=$3
MAC ADDR=$4
JMP SERVER=jumpstart
INST CLIENT BASE=
PROFILE=
END SCRIPT=
fgrep -s "$HOST NAME" /etc/hosts
if [ $? != 1 ]
then
       echo "!!! $HOST NAME is already present in /etc/hosts. Please correct and re-run
setup-client !!!"
       exit 1
fi
fgrep -s "$HOST NAME" /etc/ethers
if [ $? != 1 ]
then
       echo "!!! $HOST NAME is already present in /etc/ethers. Please correct and re-run
setup-client !!!"
       exit 1
fi
fgrep -s "$HOST NAME" /export/jumpstart/rules
if [ $? != 1 ]
then
       echo "!!! $HOST NAME is already present in /export/jumpstart/rules. Please correct
and re-run setup-client !!!"
      exit 1
```

```
fi
```

else

mkdir /export/sysidcfg/\$HOST NAME

fi

echo "\$IP ADDR \$HOST NAME #Added by setup-client for Jumpstart" >> /etc/hosts echo "\$MAC ADDR \$HOST NAME #Added by setup-client for Jumpstart" >> /etc/ethers echo "system locale=C name service=NONE network interface=primary {hostname=\$HOST NAME ip address=\$IP ADDR netmask=255.255.255.0 protocol ipv6=no default route=192.168.0.1} security policy=NONE root password=H5o.sHX3wB6 timezone=US/Central timeserver=localhost terminal=vt100" > /export/sysidcfg/\$HOST NAME/sysidcfg

echo "hostname \$HOST\_NAME - ./sparc\$ {VERSION}/\$ {DISK}.profile ./sparc\$ {VERSION} \$ {NOMIRROR}-end.sh" >> /export/jumpstart/rules cd /export/jumpstart; ./check

/export/install/sparc\${VERSION}/Solaris\_\${VERSION}/Tools/add\_install\_client -c \$JMP\_SERVER:/export/jumpstart -p \$JMP\_SERVER:/export/sysidcfg/\$HOST\_NAME -s \$JMP\_SERVER:/export/install/sparc\${VERSION} \$HOST\_NAME sun4u

echo "Added \$HOST\_NAME to Jumpstart on `date`" >> /export/jumpstart/client.log #end script

## Appendix F – mirror

#!/sbin/sh

```
#This mirror script will work for 99% of the configurations, but you may
#have trouble with weird things like ATA drives.
#
#Set up variable for disks
DISK1=notfound
DISK2=notfound
#First, see what type of disk we're mirroring
fgrep -s "c0t0d0s0" /etc/vfstab
if [ $? != 1 ]
then
       echo "Found root disk. Trying to mirror disks on controller-0."
       #Now we need to be sure there is a second drive to mirror
       DISK1=c0t0d0s
       fgrep -s "c0t1d0s0" /var/sadm/system/data/vfstab.unselected
       if [ $? != 1 ]
       then
               DISK2=c0t1d0s
       else
               echo "There is no second drive on controller-0 to mirror."
       fi
else
       echo "Cannot find any disks on controller-0... Trying controller-1..."
fi
fgrep -s "c1t0d0s0" /etc/vfstab
if [ $? != 1 ]
then
     echo "Found root disk. Trying to mirror disks on controller-1."
     #Now we need to be sure there is a second drive to mirror
     DISK1=c1t0d0
       fgrep -s "c1td0s0" /var/sadm/system/data/vfstab.unselected
       if [ $? != 1 ]
       then
               DISK2=c1t1d0
       else
          echo "There is no second drive on controller-1 to mirror."
       fi
else
       echo "Cannot find any disks on controller-0 or controller-1. Please mirror disks manually."
fi
```

```
if [ "$DISK1" != "notfound" ] && [ "$DISK2" != "notfound" ]
```

then

# fd

/usr/sbin/prtvtoc /dev/rdsk/\${DISK1}s2 | /usr/sbin/fmthard -s - /dev/rdsk/\${DISK2}s2 /usr/sbin/metadb -a -f -c 2 c\${DISK1}s5 \${DISK2}s5 /usr/sbin/metainit -f d1 1 1 \${DISK1}s0 /usr/sbin/metainit -f d11 1 1 \${DISK1}s1 /usr/sbin/metainit -f d21 1 1 \${DISK1}s4 /usr/sbin/metainit -f d2 1 1 \${DISK2}s0 /usr/sbin/metainit -f d12 1 1 \${DISK2}s1 /usr/sbin/metainit -f d22 1 1 \${DISK2}s4 /usr/sbin/metainit d0 -m d1 /usr/sbin/metainit d10 -m d11 /usr/sbin/metainit d20 -m d21 /usr/sbin/metaroot d0 cp /etc/vfstab /etc/vfstab.orig cat > /etc/vfstab <<EOF FS #device device fsck mount mount mount #to mount to fsck at boot options point pass type /dev/fd fd no /proc -/proc proc no \_ /dev/md/dsk/d10 \_ swap no 1 /dev/md/dsk/d0 /dev/md/rdsk/d0 / logging ufs no /dev/md/dsk/d20 /dev/md/rdsk/d20 /var ufs 1 no logging /tmp tmpfs swap yes \_ EOF cat > /etc/rc3.d/S99mirror2 <<EOF #!/sbin/sh /usr/sbin/metattach d0 d2 /usr/sbin/metattach d10 d12 /usr/sbin/metattach d20 d22 /usr/sbin/dumpadm -d /dev/md/dsk/d10 /bin/rm /etc/rc3.d/S99mirror2 # End script EOF chmod +x /etc/rc3.d/S99mirror2

fi

/bin/rm /etc/rc2.d/S99mirror

sleep 30

/usr/sbin/reboot

# End script

Share the second of the second