

JumpStart for Solaris Systems, Part Two

Ido Dubrawsky 2001-04-16

JumpStart for Solaris Systems, Part Two

by [Ido Dubrawsky](#)

last updated April 16, 2001

This is the second of two articles examining JumpStart, a tool that enables Solaris system administrators to install and configure systems remotely. In the [first article](#) we introduced Sun's JumpStart system as well as the JumpStart Architecture and Security Scripts (JASS) toolkit from Sun. We also showed how the JumpStart system allows a system administrator to automate the installation of Solaris systems, while the JASS toolkit takes JumpStart one step further by building on top of JumpStart, thus allowing the automated installation of hardened systems.

This article will focus on the use of the JASS toolkit in the installation of a bastion mail host. The configuration for this host is similar to the DNS host in Hal Pomeranz's "Building Bastion Hosts with Solaris: Step by Step"[1] and is as follows:

- hardware - Sun SPARCstation IPX (sun4c architecture);
- software - Base OS: Solaris 7 (SPARC) 5/99 release; and,
- patches - Solaris 7 Recommended Security Patch (available from [Sunsolve](#).)

Additional software includes:

- Secure Shell (OpenSSH-2.3.0p1)
- OpenSSL (0.9.6)
- S/Key (1.1.3)
- sendmail (8.11.2)
- sudo (1.6.5)
- noshell (1.0)
- fix-modes
- ifstatus (2.2)
- logcheck (1.1.1)
- secureip (1.0)

A brief note on the additional software: the software packages were compiled on a different sun4c architecture system and built in a tar format. When installed, they install into /opt/local (except for sendmail, fix-modes, and the configuration and initialization files for Secure Shell, sudo, and S/

Key). The secureip package is available from ftp://ftp.mfi.com/pub/sysadmin/2000/nov_sup2000.tar.Z.

Sun provides very good documentation for setting up a JumpStart server. The procedure for configuring a Solaris 7 JumpStart server can be found in the [Solaris 7 Advanced Installation Guide](#). Another good reference with regards to JumpStart is the book "Automating Solaris Installations: A Custom JumpStart Guide" by Paul Anthony Kasper and Alan L. McClellan. While some of the information in this book is a bit dated, the text provides some very useful tips on how to eliminate all prompting during a JumpStart installation.

The first step in setting up a secure server is to ensure that the install environment is secure. The only way to ensure a secure install environment is to make sure that the environment is isolated from "dirty" networks, networks that have normal user traffic traversing the wire. This level of isolation can be achieved by performing all installs with the boot/install server and the JumpStart client connected to an isolated hub or switch. This prevents malicious snooping by potential attackers, as well as solving the problem of Solaris accessibility during the install.

In order to fully automate the JumpStart process, either NIS or NIS+ must be running as a name service or you must provide a custom sysidcfg file for the host. While a discussion of the security implications of running NIS or NIS+ is beyond the scope of this article, the isolation of the install network essentially eliminates the associated risks. Because of the need to provide the installing system with information such as the OS language to be used, the time-zone, and the date and time, the JumpStart process cannot be fully automated without NIS, NIS+, or the custom sysidcfg file. If you truly wish to completely automate the install process, refer to Automating Solaris Installations by Paul Anthony Kasper and Alan L. McClellan [2].

When using JumpStart, there are two possible methods of providing the OS with distribution media:

- from an exported CD-ROM, or
- copying the CD-ROM to a directory on the local disk and exporting that directory.

Given sufficient disk space, the second option is preferable in an isolated environment. However, in a non-isolated environment, the first option is better because the installing OS resides on read-only media. For this example, the OS media was copied to the local disk to the /opt/jumpstart/OS directory.

The install server is configured using the script setup_install_server in the CD-ROM's /Solaris_7/

Solaris_2.7/Tools directory (where CD_MNT_PT is the mount point for the CD-ROM). Once the install server has been setup and configured, the JASS toolkit should be installed. The latest version of the JASS toolkit can be found at [Sun Blueprints](#).

As mentioned in the introduction to this article, the focus of this discussion is the use of the toolkit during JumpStart system installation. The JumpStart Architecture and Security Scripts (JASS) toolkit, as the name implies, is primarily designed to be used during Solaris installation. However the toolkit also has a standalone mode that gives system administrators the ability to run the toolkit against systems already in production. For more information regarding standalone use please refer to " [JumpStart Architecture and Security Scripts for the Solaris Operating Environment - Part 2: Updated for Toolkit version 0.2](#)" by Alex Noordergraaf and Glenn Brunette [3].

To install the JASS toolkit, perform the following steps:

```
root@install#: cd /
root@install#: zcat jass-0.2.tar.Z | tar -xvf -
root@install#: mv jass-0.2 jumpstart (or cp -pr jass-0.2/* jumpstart)
```

The JASS toolkit is now installed. The toolkit authors provide a sample JumpStart rules file, called rules.sample, in the top level directory of the kit. This file contains example distribution configurations. For the example in this article, the "Minimal-Distribution, Hardened Example" was chosen. This provides a minimized OS as well as some additional hardening. Once the distribution is chosen, the next step is to add the information for the JumpStart client to the server. This involves modifying the following files:

- /etc/ethers - contains the ethernet address of the JumpStart client; and,
- /etc/hosts - provides for hostname to IP address mapping for the client

For the example used in this discussion, the hosts file is:

```
#
# Internet host table
#
127.0.0.1      localhost
192.168.100.1  hyperion.cisco.com      hyperion      loghost timehost
192.168.100.254 s7.cisco.com      s7
192.168.100.2  titan.cisco.com        titan
192.168.100.3  dione      dione.cisco.com
```

and the ethers file is:

```
08:00:20:0C:26:C9 dione
```

hyperion is the install host and dione is the JumpStart client. Once these two files have been modified, the next step is to use the `add_install_client` command in the `/opt/jumpstart/OS/Solaris_7/Solaris_2.7/Tools` to add the JumpStart client to the install server's database. The command `add_install_client` performs a variety of tasks, including starting the `in.rarpd` server and the `rpc.bootparamd` server, reconfiguring `inetd` to start a `tftp` server, adding the install client to the `/etc/bootparams` file, and exporting the OS directory. The directory where the JASS toolkit is installed must also be exported, but this step must be performed by hand.

To ensure that security patches will be installed, download the patches zip file from [SunSolve](#) (for Solaris 7, the file is called `7_Recommended.zip`) and unzip the file in the `/jumpstart/Patches` directory. The JASS toolkit will automatically pick up the existence of the patches in the `Patches` directory and install them after the OS has been installed.

Before actually booting the JumpStart client, there are several more steps that need to be undertaken. The most important step is to run the `check` program against the rules file to produce the `rules.ok` file. The `check` program can be found in the `<OS_install_directory>/Solaris_7/Solaris_2.7/Misc/jumpstart_sample` directory in Solaris 7 and 8. In Solaris 2.6 the `check` program is found in the `<OS_install_directory>/Solaris_2.6/Tools/jumpstart_sample` directory.

Once the `rules.ok` file has been produced, the next step in using the JASS toolkit is to edit the `/jumpstart/Drivers/user.init` file. This script provides a mechanism to specify user functions that will be used by the toolkit during the installation[4].

Two important environment variables to change in the `user.init` file are: `JASS_PACKAGE_MOUNT` and `JASS_PATCH_MOUNT`. By default, the JASS toolkit defines them as `192.168.11.33:/jumpstart/Packages` and `192.168.11.33:/jumpstart/Patches` respectively. The only thing that needs to change is the IP address of the install server. `JASS_PACKAGE_MOUNT` defines the NFS location of the `Packages` directory while `JASS_PATCH_MOUNT` defines the NFS location of the `Patches` directory.

Another environment variable that may be useful to change is the `JASS_ROOT_PASSWD`. This variable contains the encrypted root passwd to use in the `/etc/shadow` file. By default, this passwd is set in the `set-root-password.fin` finish script and has the value `'JdqZ5HrSDYM.o'`. This is the

encrypted form of the password 't001k1t' as mentioned in "JumpStart Architecture and Security Scripts for the Solaris Operating Environment - Part 3: Updated for Toolkit version 0.2"[4]. While it may seem easier to simply change the default value of the root password in the finish script, there is the possibility that a future upgrade of the toolkit may overwrite that script. The user.init will not be replaced during upgrades of the toolkit. This makes it a much better candidate for putting in site-specific changes such as changes to JASS_ROOT_PASSWD.

If additional packages are to be installed (as was done with this example) into the system, it is necessary to place those packages in the /jumpstart/Packages directory and provide a finish script to install them. By default, the JASS toolkit comes with a finish script to install Casper Dik's fix-modes program. This script provides a perfect starting point for writing additional finish scripts for installing other packages and was used to write the finish scripts for installing the above software.

The following finish scripts are not part of the default JASS toolkit package from Sun but were created to extend the capabilities of the JASS toolkit:

```
remove-packages.fin,  
install-sendmail.fin  
install-openssl.fin  
install-openssh.fin  
install-skey.fin  
install-sudo.fin  
install-noshell.fin  
install-ifstatus.fin  
install-logcheck.fin  
install-secureip.fin
```

These scripts were added to the SCRIPTS variable of the driver file /jumpstart/Drivers/hardening.driver on the install server. In the installation of the mail server in this article, the finish script disable-sendmail.fin was not run in order to later remove the Solaris sendmail packages without error.

Once the user.init script is customized, it is possible to begin the system installation. This is done by issuing the command:

```
boot net - install
```

at the boot PROM level of the system (a note of caution, with older boot PROMs it may be necessary to issue the 'n' command first in order to get into "new" mode).

Once that is done the rest is essentially hands-free, as can be seen from the output of the installation of the [example system](#).

When the system has finished installing and reboots, the pkginfo for this system is as follows:

```
# pkginfo
```

```
system      SUNWadmr      System & Network Administration Root
system      SUNWcar      Core Architecture, (Root)
system      SUNWcsd      Core Solaris Devices
system      SUNWcsl      Core Solaris, (Shared Libs)
system      SUNWcsr      Core Solaris, (Root)
system      SUNWcsu      Core Solaris, (Usr)
system      SUNWdfb      Dumb Frame Buffer Device Drivers
system      SUNWdtcor    Solaris Desktop /usr/dt filesystem anchor
system      SUNWesu      Extended System Utilities
system      SUNWfns      Federated Naming System
system      SUNWkey      Keyboard configuration tables
system      SUNWkvm      Core Architecture, (Kvm)
system      SUNWlibc     SPARCompilers Bundled libc
system      SUNWlibms    Sun WorkShop Bundled shared libm
system      SUNWloc      System Localization
system      SUNWnistr    Network Information System, (Root)
system      SUNWnису     Network Information System, (Usr)
system      SUNWntpr     NTP, (Root)
system      SUNWntpu     NTP, (Usr)
system      SUNWploc     Partial Locales
system      SUNWploc1    Supplementary Partial Locales
system      SUNWsolnm    Solaris Naming Enabler
system      SUNWswmt     Install and Patch Utilities
system      SUNWxcu4     XCU4 Utilities
system      SUNWxwdv     X Windows System Window Drivers
system      SUNWxwice    ICE components
system      SUNWxwmod    OpenWindows kernel modules
system      SUNWxwplt    X Window System platform software
system      SUNWxwrtl    X Window System & Graphics Runtime Library
Links in /usr/lib
```

```
# uname -a
```

```
SunOS dione 5.7 Generic_106541-14 sun4c sparc SUNW,Sun_4_50
```

```
#
```

Conclusion

The JASS toolkit provides system administrators with a wonderful tool to improve the JumpStart

process. By providing the ability to install systems that are hardened from the start, the JASS toolkit has reduced the amount of time it takes to secure a system and place it into production. Furthermore, with the ability to reinstall a hardened system with relative ease the JASS toolkit provides the capability to recreate systems that have failed.

References

[1] "Building Bastion Hosts with Solaris: Step by Step", Hal Pomeranz, SANS Network Security '98, October 1998

[2] Automating Solaris Installations, Paul Anthony Kasper and Alan L. McClellan, Prentice Hall/SunSoft Press, 1995

[3]" [JumpStart Architecture and Security Scripts for the Solaris Operating Environment - Part 2: Updated for Toolkit version 0.2](#)", Alex Noordergraaf and Glenn Brunette, Sun Blueprints, November 2000

[4]" [JumpStart Architecture and Security Scripts for the Solaris Operating - Part 3: Updated for Toolkit version 0.2](#)", Alex Noordergraaf and Glenn Brunette, Sun Blueprints, November 2000

Ido Dubrawsky has been working in UNIX and network administration field for almost 8 years. He is currently employed by Cisco Systems in the Cisco Secure Consulting Service as a Network Security Engineer.

Relevant Links

[JumpStart for Solaris Systems, Part One](#)
Ido Dubrawsky

[Sun Blueprints Online](#)
Sun

[Solaris Jumpstart Automated Installation](#)
Kevin Amarin

[Privacy Statement](#)

Copyright 2006, SecurityFocus