Sun™ Cluster 3.0 12/01 Security with the Apache and iPlanet™ Web and Messaging Agents

By Alex Noordergraaf - Enterprise Engineering,
Mark Hashimoto - Sun Cluster Manageability and Serviceability Group, and
Richard Lau - Sun Cluster Quality Assurance Group

Sun BluePrints™ OnLine - December 2001

http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-3571-10
Revision 1.0, 12/05/01
Edition: December 2001

Sun™ Cluster 3.0 12/01 Security with the Apache and iPlanet™ Web and Messaging Agents

Sun™ Cluster 3.0 12/01 software is used by organizations to provide additional assurance that mission-critical services will be available despite unexpected hardware or software failures or usage requirements. The business criticality of Sun Cluster deployments requires that the nodes in a cluster be protected against unauthorized access and misuse by malicious individuals.

To provide a robust environment in which Sun Cluster 3.0 12/01 software can be deployed, very specific requirements have been placed on the configuration of the Solaris™ Operating Environment (Solaris OE) used on Sun Cluster 3.0 nodes. Before the release of Sun Cluster 3.0 12/01 software, no secured configurations were supported. This article takes a first step towards providing secured configurations that use Sun Cluster 3.0 12/01 software by describing how three specific agents can be deployed in a secured configuration that is supported by Sun Microsystems.

These security recommendations are specific to the three Sun Cluster 3.0 agents supported in secured environments: the iPlanet™ Web Server software, the Apache web server, and the iPlanet™ Messaging Server software.

This article contrasts the recommendations made in the Sun BluePrints™ OnLine article “Solaris™ Operating Environment Security: Updated for Solaris 8 Operating Environment” with the functionality required by the Sun Cluster software. This article also describes methods for simplifying the deployment of secured configurations across the potentially many nodes in a cluster and on automated mechanism to deploy them. Solaris™ Security Toolkit software, a free toolkit that automates the hardening of Solaris OE system, is used to harden the Solaris OE images running on the nodes, as well as to install the other security software recommended in this article.

The Solaris Security Toolkit software makes over 80 modifications to the OS of each cluster node. These modifications not only disable unneeded services but also enable optional Solaris OE security enhancements. Executing the Solaris Security Toolkit hardening scripts for Sun Cluster software on a running cluster significantly reduces the number of Solaris OE services and daemons, as well as the number of access points into the cluster.

By reducing access points, disabling unused services, enabling optional security features, and generally improving the overall security of the cluster nodes, you make it much more difficult for an intruder to gain access to the cluster and misuse its resources.

Software Versions

The Solaris OE security hardening recommendations and the security recommendations for the Sun Cluster 3.0 software secured configuration documented in this article are based on the Solaris 8 10/01 OE (Update 6).

The Sun Cluster software qualified to run in the secured environment is Sun Cluster 3.0 12/01 software using either the iPlanet Web Server, the Apache web server, or the iPlanet Messaging Server software. The Apache web server and the iPlanet Web Server software are supported in either scalable or failover modes, while the iPlanet Messaging Server software is only supported in failover mode.

Supportability

The secured Sun Cluster 3.0 12/01 software configuration implemented by the Solaris Security Toolkit `suncluster30u2-secure.driver` is a Sun Microsystems-supported configuration for agents described in this document. Only Sun Cluster 3.0 12/01 implementations using the three agents explicitly described in this article and referenced in the Sun Cluster 3.0 12/01 Release Notes are supported in hardened configurations.

Note – Hardening Sun Cluster 2.x, 3.0, and 3.0 update 1 software is not supported. Only agents described in this article and listed in the Sun Cluster 3.0 12/01 Release Notes are supported in hardened configurations.

While it is not required that you use the Solaris Security Toolkit software (toolkit) to harden the cluster, it is strongly recommended. Using the toolkit, you can easily create an error free, documented, and standardized hardened configuration. In addition, the toolkit provides a mechanism for undoing hardening changes should it become necessary.

Note – Sun Microsystems supports a hardened Sun Cluster 3.0 12/01 cluster, using the agents specified in this document, whether security modifications are performed manually or through the use of the Solaris Security Toolkit software.

Please note that the toolkit is not a supported Sun product; only the end-configuration created by the toolkit is supported. Toolkit support is available through the Sun™ SupportForum discussion group at `http://www.sun.com/security/jass`

Assumptions and Limitations

The configuration described in this article has the following characteristics:

- Solaris 8 OE 10/01 or update 6 software
- Sun Cluster 3.0 12/01 software
- iPlanet web and messaging severs and Apache web server supported
- Solaris OE packages and installation
- Cluster interconnect links
- Solaris Security Toolkit software
- Security modifications
- Solaris OE minimization not supported

The following sections describe each of these characteristics in greater detail.

Solaris 8 OE

This article is based on Solaris 8 OE 10/01 (Update 6). All of the hardening results presented in this article were produced on this version of the Solaris OE. Using versions other than Solaris 8 OE may produce results that are slightly different than those presented in this article.

Sun Cluster 3.0 12/01 Software

Sun Cluster 3.0 12/01 software is the version of Sun Cluster software that supports the configuration described in this article. Previous versions of Sun Cluster software do not support the hardened configurations described in this article and should not be used to deploy these configurations.

iPlanet Web and Messaging Servers and Apache Web Server Supported

Only the following agents are supported in secured configurations:

- iPlanet Web Server software
- Apache web server
- iPlanet Messaging Server software

The iPlanet and Apache web server agents are supported in either scalable or failover mode while the iPlanet Messaging Server software does not have a scalable mode and is correspondingly supported only in failover mode.

Solaris OE Packages and Installation

Sun Cluster 3.0 12/01 software requires only the Solaris OE end user cluster. It is strongly recommended that this Solaris OE cluster be used instead of the entire Solaris OE distribution. Minimizing the number of Solaris OE packages installed directly reduces the number of services to disable, the quantity of patches to install, and the number of potential vulnerabilities on the system.

This article does not discuss how the Solaris OE and Sun Cluster 3.0 12/01 software are installed and configured on the cluster nodes. Sun Cluster 3.0 12/01 software does enable you to automate the installation of the cluster and OS software through JumpStart™ software-based installations. Correspondingly, you can also include the hardening steps performed by the Solaris Security Toolkit software in the JumpStart installation process. This article does not discuss methods for integrating the hardening process documented in this article with JumpStart software-based installations. For information about this topic, refer to the Sun Cluster 3.0 and Solaris Security Toolkit documentation.

Cluster Interconnect Links

It is critical to the overall security of the cluster that cluster interconnect links are kept private and are not exposed to a public network. Sensitive information about the health of the cluster and information about the file system is shared over this link. It is strongly recommended that these interconnects be implemented using separate and dedicated network equipment. The use of VLAN's is discouraged from a security and availability perspective because they typically restrict packets based only on tags added by the switch. There is also minimal, if any, assurance that these tags are valid, and there is no additional protection against directed Address Resolution Protocol (ARP) attacks.

Solaris Security Toolkit Software

The drivers described in this article are included in version 0.3.3 of the Solaris Security Toolkit software. This version, or newer versions, of the software must be used when implementing the recommendations of this article.

The hardening of a Sun Cluster 3.0 node does not have to be performed with the toolkit; however, because it provides an error free, standardized mechanism for performing the hardening process, and because it enables you to undo changes after they are made, it is highly recommended that you use the toolkit.

Security Modification Scope

Solaris OE hardening can be interpreted in a variety of ways. For the purposes of developing a hardened server configuration, the recommendations in this article represent all of the possible Solaris OE hardening. That is, anything that can be hardened, is hardened. Things that are not hardened are not modified for the reasons described in this article. A Solaris OE configuration hardened to the degree described in this article may not be appropriate for all environments. When installing and hardening a specific Solaris OE instance, you can perform fewer hardening operations than are recommended. For example, if your environment requires Network File System (NFS)-based services, you can leave them enabled. However, hardening beyond that which is presented in this article should not be performed and is neither recommended, nor supported.

Note – Standard security rules apply to the hardening of Sun Cluster 3.0 12/01 software installations: *That which is not specifically permitted is denied.*

Minimization

Minimization is the removal of unnecessary Solaris OE packages from the system which reduces the number of components that have to be patched and made secure. While, reducing the number of components reduces entry points to an intruder, minimization is not supported on Sun Cluster 3.0 nodes at this time. Only the Solaris OE hardening tasks discussed in this article are supported modifications for systems with Sun Cluster 3.0 12/01 software running supported agents.

Solaris OE Service Restriction

The typical hardening of a Solaris OE system involves commenting out all of the services in the `/etc/inetd.conf` file and disabling unneeded system daemons from starting. All of the interactive services normally started from `inetd` are then replaced by Secure Shell (SSH). Unfortunately, Sun Cluster 3.0 12/01 software does not permit the entire contents of the `/etc/inetd.conf` file to be commented out. The primary reason for this limitation is that volume management software requires several RPC services to be available. The Sun Cluster 3.0 12/01 software also installs additional RPC- based services. These Sun Cluster software-specific RPC services include the `rpc.pmfd` and `rpc.fed` services.

The security recommendations in this article include all Solaris OE modifications that do not impact required Sun Cluster 3.0 node functionality. This does not mean that these modifications are appropriate for every node. In fact, it is likely that some of the services disabled by the default `suncluster30u2-secure.driver` script will affect some applications. Because applications and their service requirements vary, it is unusual for one configuration to work for all applications.

Note – Consider the role of a secured configuration in the context of the applications and services that the Sun Cluster 3.0 12/01 software will support. The security configuration presented in this article is a high-watermark for system security, as every service that is not required by the Sun Cluster 3.0 12/01 software and agents is disabled. This information should provide you with a clear idea of which services can and cannot be disabled without affecting the behavior of the Sun Cluster 3.0 12/01 software and the three agents.

For information about Solaris OE services and for recommendations about mitigating their security implications, refer to the Sun BluePrints OnLine article “Solaris™ Operating Environment Security: Updated for the Solaris 8 Operating Environment” and the Sun BluePrints OnLine article “Solaris™ Operating Environment Network Settings for Security: Updated for Solaris 8 Operating Environment.” The recommendations in these articles are implemented with the

Solaris Security Toolkit software in standalone and JumpStart modes. In addition, the Sun BluePrints OnLine article “The Solaris™ Security Toolkit - Internals: Updated for version 0.3” describes the functions of each of the toolkit scripts. The following section summarizes the modifications made by the toolkit during a Sun Cluster 3.0 12/01 software hardening run.

Hardening Modifications

Each of the modifications performed by the toolkit to harden Sun Cluster 3.0 nodes falls into one of the following categories:

- `Disable`
- `Enable`
- `Install`
- `Remove`
- `Set`
- `Update`

In addition, the toolkit copies files from the toolkit distribution to increase the security of the system. These system configuration files change the default behavior of `syslogd`, system network parameters, and a variety of other system configurations.

The following sections describe each of these categories and the scripts modifications they perform. For a complete listing of the scripts included in the `suncluster30u2-secure`.driver refer to the Solaris Security Toolkit `Drivers` directory.

Disable Scripts

These scripts disable services on the system. Disabled services include the NFS client and server, the automounter, the DHCP server, printing services, and the window manager. The goal of these scripts is to disable all of the services that are not required by the system.

A total of 30 disable scripts are included with the Sun Cluster 3.0 12/01 software-hardening driver. These scripts impose modifications to disable all, or part, of the following services and configuration files:

- `apache`
- `aspppd`
- `automountd`
- `core generation`
- `ldap_cachemgr`
- `lpsched`
- `mipagent`
- `mountd`
- `sendmail`
- `slp`
- `snmpdx`
- `printd`

- dhcp
- snmpXdmid
- dtlogin
- IPv6
- keyservd
- nfsd
- nscd
- picld
- pmconfig
- pam.conf
- syslogd
- smcboot

Enable Scripts

These scripts enable the security features that are disabled by default on Solaris OE. These modifications include:

- Enabling optional logging for `syslogd` and `inetd`
- Requiring NFS client requests to use privileged ports for all requests
- Enabling process accounting
- Enabling improved sequence number generation per RFC 1948
- Enabling optional stack protection and logging to protect against most buffer overflow attacks

While some of these services are disabled, their optional security features remain enabled so that they are used securely if enabled in the future.

Install Scripts

These scripts create new files to enhance system security. In the Sun Cluster 3.0 driver, the following Solaris OE files are created to enhance the security of the system:

- An empty `/etc/cron.d/at.allow` to restrict access to `at` commands
- An updated `/etc/ftpusers` file with all system accounts to restrict system FTP access
- An empty `/var/adm/loginlog` to log unsuccessful login attempts
- An updated `/etc/shells` file to limit which shells can be used by system users
- An empty `/var/adm/sulog` to log `su` attempts

In addition to creating the preceding files, some install scripts also add software to the system. Specifically, for the Sun Cluster 3.0 nodes, the following software is installed:

- Recommended and Security patch clusters
- MD5 software
- FixModes software

Remove Scripts

Only one remove script is distributed with the Sun Cluster 3.0 driver and it used to remove unused Solaris OE system accounts. The accounts that are removed are no longer used by the Solaris OE and can safely be removed. The accounts that are removed include:

- `smtp`
- `nuucp`
- `listen`
- `nobody4`

Set Scripts

These scripts configure the security features of the Solaris OE that are not defined by default. Fourteen of these scripts are distributed with the Sun Cluster 3.0 driver and they can configure the following Solaris OE security features not enabled by default:

- root password
- `ftpd` banner
- `telnetd` banner
- `ftpd UMASK`
- `login RETRIES`
- power restrictions
- system suspend options
- `TMPFS` size
- user password requirements
- user `UMASK`

Update Scripts

These scripts update the configuration files that are shipped with the Solaris OE but do not have all of their security settings properly set. The following configuration files are modified:

- `at.deny`
- `cron.allow`
- `cron.deny`
- `logchecker`
- `inetd.conf`

Hardening Results

After hardening, the following non-cluster services remain running on a node:

```
# ps -ef | grep -v cluster
UID   PID  PPID  C    STIME TTY      TIME CMD
root    0     0  0   Oct 25 ?       0:01 sched
root    1     0  0   Oct 25 ?       0:00 /etc/init -
root    2     0  0   Oct 25 ?       0:00 pageout
root    3     0  0   Oct 25 ?       4:41 fsflush
root   466    1  0   Oct 25 ?       0:00 /usr/lib/saf/sac -t 300
root   65     1  0   Oct 25 ?       0:01 /usr/lib/sysevent/syseventd
root   67     1  0   Oct 25 ?       0:00 /usr/lib/sysevent/syseventconfd
root   77     1  0   Oct 25 ?       8:22 devfsadmd
root   265    1  0   Oct 25 ?       0:00 /usr/lib/netsvc/yp/ypbind -broadcast
root   252    1  0   Oct 25 ?       0:00 /usr/sbin/rpcbind
root   167    1  0   Oct 25 ?       0:00 /usr/sbin/in.rdisc -s
root   469   466  0   Oct 25 ?       0:00 /usr/lib/saf/ttymon
root   255    1  0   Oct 25 ?       0:00 /usr/sbin/keyserv -d
root   394    1  0   Oct 25 ?       0:00 /usr/lib/utmpd
root   274    1  0   Oct 25 ?       0:00 /usr/sbin/inetd -s -t
root   318    1  0   Oct 25 ?       0:00 /usr/lib/inet/xntpd
root   285    1  0   Oct 25 ?       0:00 /usr/sbin/syslogd -t
root   327   274  0   Oct 25 ?       0:00 rpc.metad
root   396    1  0   Oct 25 ?       0:00 /usr/sbin/nscd
root   373    1  0   Oct 25 ?       0:00 /usr/sbin/cron
root   391    1  0   Oct 25 ?       0:00 /usr/sbin/vold
root   470    1  0   Oct 25 ?       0:00 /usr/lib/sendmail -q15m
root  1060    1  0 13:54:45 ?       0:00 /opt/OBSDssh/sbin/prngd --cmdfile /etc/prngd.conf --seedfile
                                          /var/spool/prngd/p
   root  1086    1  1 13:55:00 ?       0:00 /opt/OBSDssh/sbin/sshd
```

The preceding listing of services may not exactly match your environment. Several configuration modifications were made on this node after the OS was installed. These modifications included the configuration of `xntp`, NIS, and the installation of OpenSSH.

The following output was generated by nmap, a popular freeware security scanning tool:

```
# nmap -p 1-65535 10.6.25.150

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Port       State      Service
22/tcp     open       ssh
111/tcp    open       sunrpc
8059/tcp   open       unknown
8060/tcp   open       unknown
32785/tcp  open       unknown
32786/tcp  open       sometimes-rpc25
32787/tcp  open       sometimes-rpc27
32788/tcp  open       unknown
32789/tcp  open       unknown
32790/tcp  open       unknown
32791/tcp  open       unknown
32804/tcp  open       unknown
32806/tcp  open       unknown
32811/tcp  open       unknown
32821/tcp  open       unknown

Nmap run completed -- 1 IP address (1 host up) scanned in 211 seconds
```

Ports 8059 and 8060 are Sun Cluster 3.0 software-specific ports that accept only connections from other cluster nodes. When a connection request from a non-cluster node is received, the following message is logged to syslog:

```
Oct 30 14:00:52 phys-sps-1 cl_runtime: WARNING: Received a connect request from a node not
configured in the cluster. Nodeid 0 ipaddr 0x8194b556
```

Monitor log files for these types of messages so that appropriate action can be taken when unauthorized access attempts are made against the cluster.

Cluster nodes are added based on the authentication method defined in the Sun Cluster 3.0 12/01 software configuration. It is strongly recommended that you use the strongest possible method of authentication. The available options are discussed in the Node Authentication section below.

Sun Cluster 3.0 Daemons

The Sun Cluster 3.0 12/01 software adds several additional daemons to a system. These include both daemons running on the system, as well as additional RPC services. The following daemons run on a default Sun Cluster 3.0 12/01 software installation:

```
# ps -ef | grep cluster
   root     4     0  0   Oct 25 ?      0:03 cluster
   root   416     1  0   Oct 25 ?      0:00 /usr/cluster/lib/sc/rpc.pmfd
   root    82     1  0   Oct 25 ?      0:00 /usr/cluster/lib/sc/clexecd
   root    83    82  0   Oct 25 ?      0:00 /usr/cluster/lib/sc/clexecd
   root   453     1  0   Oct 25 ?      0:01 /usr/cluster/lib/sc/rgmd
   root   426     1  0   Oct 25 ?      0:00 /usr/cluster/lib/sc/rpc.fed
   root   439     1  0   Oct 25 ?      0:00 /usr/cluster/bin/pnmd
```

A Sun Cluster 3.0 12/01 software installation also installs the following RPC services in the `/etc/inetd.conf` file:

```
# Start of lines added by SUNWscu
100145/1 tli rpc/circuit_v wait root /usr/cluster/lib/sc/rpc.scadmd rpc.scadmd
100151/1 tli rpc/circuit_v wait root /usr/cluster/lib/sc/rpc.sccheckd rpc.sccheckd -S
# End   of lines added by SUNWscu
```

The following RPC services are required by the Sun Cluster 3.0 12/01 software and must be present in the `/etc/inetd.conf` file:

```
# rpc.metad
100229/1      tli    rpc/tcp       wait    root    /usr/sbin/rpc.metad rpc.metad
# rpc.metamhd
100230/1      tli    rpc/tcp       wait    root    /usr/sbin/rpc.metamhd rpc.metamhd
```

The reviewed configuration uses Solstice DiskSuite™ software which requires the following RPC services in the `/etc/inetd.conf` file:

```
# rpc.metamedd - DiskSuite mediator
100242/1      tli    rpc/tcp       wait    root    /usr/sbin/rpc.metamedd rpc.metamedd
# rpc.metacld - DiskSuite cluster control
100281/1      tli    rpc/tcp       wait    root    /usr/sbin/rpc.metacld rpc.metacld
```

If you use Veritas Volume Manager software instead of Solstice DiskSuite software, leave the appropriate Veritas RPC entries in the `/etc/inetd.conf` file enabled.

Terminal Server Usage

Sun Cluster 3.0 software does not require a terminal server as Sun Cluster 2.x software did. This is a significant improvement from a security perspective. Terminal server connections frequently do not use encryption. This lack of encryption allows a malicious individual to sniff the network and 'read' the commands being issued to the client. Frequently, these commands will include an administrator logging in as root and providing the root password.

We strongly recommend that you use a terminal server that supports encryption. Specifically, we recommend the use of a terminal server that implements Secure Shell (SSH). Terminal servers that support SSH are currently available from both Cisco (`http://www.cisco.com`) and Perle (`http://www.perle.com`).

If you cannot use a terminal server that supports encryption, only connect terminal servers to a private management network. While this helps isolate network traffic to the terminal servers, it is not as secure as the use of a terminal server supporting SSH.

Node Authentication

Sun Cluster 3.0 12/01 software provides several options for node authentication. Node authentication is how potential nodes must identify themselves before being allowed to join a cluster. Ensuring that all nodes are properly authenticated is a critical aspect of cluster security. This section discusses what options are available and provides recommendations on what level of node authentication should be used.

The available node authentication options in Sun Cluster 3.0 12/01 software are:

- none (i.e., any system is permitted to join the cluster)
- IP address
- UNIX®
- Diffie-Hellman using DES

In addition, the `scsetup` command provides the following under option `6) New nodes`:

```
*** New Nodes Menu ***

  Please select from one of the following options:

    1) Prevent any new machines from being added to the cluster
    2) Permit any machine to add itself to the cluster
    3) Specify the name of a machine which may add itself
    4) Use standard UNIX authentication
    5) Use Diffie-Hellman authentication

    ?) Help
    q) Return to the Main Menu
```

At a minimum, the node authentication setup should require that new cluster nodes be added manually and not automatically. This would require selecting options 1 to restrict the ability of systems to add themselves and then using option 3 to specify the name of the new cluster node. These two options run `scsetup` with the following commands, which can also be run manually:

```
# scconf -a -T node=.
# scconf -a -T node=phys-sps-1
```

The next consideration is how to validate that a node is who is says it is. There are two alternatives: standard UNIX or Diffie-Hellman authentication. The default is to use UNIX authentication. If a private interconnect is used to connect the nodes and the scconf command has been used to restrict new nodes from joining this is probably adequate. In environments where other systems may attempt to join into the cluster, or if the data on the cluster is particularly sensitive, then the use of Diffie-Hellman authentication is recommended.

Diffie-Hellman authentication uses Secure RPC to authenticate the nodes in the cluster. This requires that the public and private keys be setup properly on each of the nodes. The most effective means to do this is through NIS+ as it simplifies the management and maintenance of these key pairs. It is however possible to use Secure RPC without NIS+. For additional information on Secure RPC and Diffie-Hellman authentication refer to the keyserv(1M), publickey(4), and nis+(1) man pages.

Securing Sun Cluster 3.0 12/01 Software

To effectively secure each node in a cluster, you must make changes to the Solaris OE software running on each node. These changes can be separated into the following distinct areas:

1. Installing additional security software on the Sun Cluster 3.0 nodes
2. Solaris OE modifications to each of the Sun Cluster 3.0 nodes

---

Note – At this point in the process, the appropriate Solaris OE cluster should be installed on the cluster nodes and the required Sun Cluster 3.0 12/01 software and agents should be installed and configured. Only continue on to the installation of the security software if the cluster is installed and running with the appropriate agents.

Installing Security Software

The security recommendations to secure the Sun Cluster 3.0 12/01 environment involve the installation of several software packages. These packages are:

- Solaris Security Toolkit software
- Recommended and Security patch cluster
- FixModes software
- OpenSSH software
- MD5 software

Note – Of the packages described in this section, only the Solaris Security Toolkit software, the FixModes software, and the MD5 software are required. The use of OpenSSH, while strongly recommended, is not required. Commercial versions of SSH, available from `http://www.fsecure.com` or `http://www.ssh.com`, for OpenSSH.

The first step in securing cluster nodes is to install the required software. This section describes how to install or prepare to install each of the software packages.

Installing Solaris Security Toolkit Software

First, download the Solaris Security Toolkit software and install it on each of the nodes. The toolkit is used to automate the Solaris OE hardening tasks described later in this article.

The primary function of the toolkit is to automate and simplify building secured Solaris OE systems based on the recommendations contained in this and the other security-related Sun BluePrints OnLine articles. In the context of this article, a module has been developed specifically to harden Sun Cluster 3.0 nodes. The secondary function of the toolkit is to automate the installation of software such as the FixModes software and the Recommended and Security patch clusters.

The following instructions use file names that are only correct for this release of the toolkit. Use the following procedure to download and install the toolkit:

1. **Download the source file (**`SUNWjass-0.3.3.pkg.Z`**).**

   The source file is located at `http://www.sun.com/security/jass`

2. **Use the** `uncompress` **command to extract the source file into a directory on the server as follows**:

```
# uncompress SUNWjass-0.3.3.pkg.Z
```

3. **Use the** `pkgadd` **command to install the Solaris Security Toolkit software on the server as follows:**

```
# pkgadd -d SUNWjass-0.3.3.pkg SUNWjass
```

   Executing this command creates the `SUNWjass` directory in `/opt`. This subdirectory will contain all the toolkit directories and associated files. The script `make-jass-pkg`, included in toolkit releases since 0.3 allows administrators tp create custom packages using a different installation directory.

Installing Recommended and Security Patch Clusters

The installation procedures presented in this section use the Solaris Security Toolkit software to install the most recent Recommended and Security Patch clusters available from the SunSolve Online℠ Web site. To install these patches with the toolkit, download them and store them, uncompressed, in the `/opt/SUNWjass/Patches` directory on each node.

Sun regularly releases patches to provide Solaris OE fixes for performance, stability, functionality, and security reasons. It is critical to the security of the system that you install the most up-to-date patch clusters. This section describes how to use the Solaris Security Toolkit software to automatically install patches, thereby ensuring that the latest Recommended and Security patch clusters are installed on each node.

1. **To download the latest cluster, go to the SunSolve Online Web site at** `http://sunsolve.sun.com` **and click the Patches link on the top of the left navigation bar.**

Note – Downloading the Solaris OE Recommended and Security patch clusters does not require a SunSolve support contract.

---

2. **Next, select the appropriate Solaris OE version in the Recommended Solaris Patch Clusters box. This example uses Solaris 8 OE.**
3. **After selecting the appropriate Solaris OE version, select the best download option, either HTTP or FTP, with the associated radio button and click the Go button.**
4. **In the Save As window that appears in your browser, save the file locally in preparation for uploading it to the cluster being hardened.**
5. **After downloading the patch cluster, move the file securely to the node being hardened using either the** `scp` **SSH command or the** `sftp` **SSH command. If SSH is not yet installed, use the** `ftp` **command. The** `scp` **command used to copy the file to an domain called** `scnode01` **should appear similar to the following:**

```
% scp 8_Recommended.zip scnode01:/var/tmp
```

6. **Next, you must move the file to the** `/opt/SUNWjass/Patches` **directory and uncompress it. The following commands perform these tasks:**

```
# cd /opt/SUNWjass/Patches
# mv /var/tmp/8_Recommended.zip .
# unzip 8_Recommended.zip
 Archive:  8_Recommended.zip
  creating: 8_Recommended/
   inflating: 8_Recommended/CLUSTER_README
   inflating: 8_Recommended/copyright
   inflating: 8_Recommended/install_cluster
[. . .]
```

Note – If the Recommended and Security patches are not loaded into the appropriate directory, a warning message will be generated during the execution of the toolkit.

Installing FixModes Software

This section describes how to download and install the FixModes software into the appropriate toolkit directory so it can be used to tighten file permissions during the toolkit run. By selectively modifying system permissions it will be more difficult for malicious users to gain additional privileges on the system.

Follow these instructions to download the FixModes software:

1. **Download the FixModes precompiled binaries from** `http://www.sun.com/blueprints/tools/FixModes_license.html`

   The FixModes software is distributed as a precompiled and compressed tar file format called `FixModes.tar.Z`.

2. **Save the downloaded file,** `FixModes.tar.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages`

Note – Do not uncompress the tar archive.

Installing the OpenSSH Software

In any secured environment the use of encryption, in combination with strong authentication, is highly recommended. At a minimum, user interactive sessions should be encrypted. The tool most commonly used to implement this is an implementation of secure shell (SSH) software. You can use either the commercially purchased version of the software or the freeware version of the software.

The use of a SSH variant is strongly recommended when implementing all the security modifications performed by the Solaris Security Toolkit software. The toolkit will disable all non-encrypted user-interactive services and daemons on the system. In particular, services such as `in.rshd`, `in.telnetd`, and `in.ftpd` are disabled. Access to the system can be gained with SSH in a similar fashion to what was provided by RSH, TELNET, and FTP. It is strongly recommended that you install and configure SSH before executing a toolkit run.

For information about compiling and deploying OpenSSH, refer to the Sun BluePrints OnLine article “Building and Deploying OpenSSH on the Solaris™ Operating Environment (July 2001)” available at
`http://www.sun.com/blueprints/0701/openSSH.pdf`

Information about obtaining commercial versions of SSH is provided in the Bibliography section of this article.

Note – The Sun BluePrints OnLine article mentioned above provides recommendations for compiling OpenSSH. However, OpenSSH should not be compiled on the cluster itself and the compilers should not be installed on the cluster. Instead, use a separate Solaris system, running the same Solaris OE version, architecture, and mode (i.e., 64 bit) to compile OpenSSH. If you use a commercial version of SSH, this issue is avoided.

Installing MD5 Software

This section describes how to download and install the MD5 software used to validate MD5 digital fingerprints on Sun Cluster 3.0 nodes. This ability to validate the integrity of Solaris OE binaries provides a robust mechanism for detecting system binaries that may have been altered by unauthorized users of the system. By modifying system binaries, attackers can gain back-door access to the system.

Once it is installed, you can use the Solaris Fingerprint Database to verify the integrity of the executables that are included in the package. For more information about the Solaris Fingerprint Database, refer to the Sun BluePrint OnLine article “The Solaris Fingerprint Database - A Security Tool for Solaris Software and Files” available at `http://www.sun.com/blueprints/0501/Fingerprint.pdf`. This article also provides information about additional tools that can be used to simplify the process of validating system binaries against the database of MD5 checksums maintained by Sun at SunSolve Online Web site.

It is strongly recommended that you use these tools, in combination with the MD5 software installed in this section, to frequently validate the integrity of the Solaris OE binaries and files on the cluster nodes. In addition, ensure that MD5 signatures generated on the server are protected until they are sent to the Solaris FingerPrint Database for validation. After they have been used, delete the MD5 signatures until they are regenerated for the next validation check.

To install the MD5 program (Intel and SPARC™ Architecture), follow these steps:

1. **Download the MD5 binaries from**
   `http://www.sun.com/blueprints/tools/md5_license.html`

   The MD5 programs are distributed as a compressed tar file.

2. **Save the downloaded file,** `md5.tar.Z`**, to the Solaris Security Toolkit** `Packages` **directory in** `/opt/SUNWjass/Packages`

Note – Do not uncompress the tar archive.

After the MD5 software has been saved to the `/opt/SUNWjass/Packages` directory, it is installed during the execution of the Solaris Security Toolkit software.

Sun Cluster 3.0 Node Solaris OE Modifications

By default, the Solaris OE configuration of a Sun Cluster 3.0 node has many of the same issues as other Solaris OE default installations. This includes having many potentially insecure daemons enabled by default. Some of these insecure services include `in.telnetd`, `in.ftpd`, `in.rsh`, `fingerd`, and `sadmind`. For a complete list of default Solaris OE services, refer to the Sun BluePrints OnLine article "Solaris Operating Environment Security: updated for Solaris 8 OE." This article describes the security issues associated with these default Solaris OE services and daemons.

This article recommends that all unused services be disabled. Based on the Solaris OE installation cluster (`SUNWCall`) typically used for an Sun Cluster 3.0 node, there are over 80 recommended Solaris OE configuration changes to improve the security configuration of the Solaris OE image running on each node. While the `SUNWCall` Solaris cluster is typically used for cluster installations, only the `SUNWuser` cluster is required. It is strongly recommended that you limit the number of Solaris services and daemons installed by using the Solaris OE cluster that contains the fewest number of packages.

To simplify the implementation of these recommendations, a customized module, or driver, has been added to the Solaris Security Toolkit software. This driver can automatically perform the recommended modifications to the Solaris OE of the nodes. These new Solaris Security Toolkit drivers are available in version 0.3.3 of the toolkit software.

The recommendations for securing the Sun Cluster 3.0 nodes closely follow the hardening described in the Sun BluePrints OnLine article "Solaris Operating Environment Security - Updated for Solaris 8 Operating Environment."

There are several exceptions to these recommendations due to functionality that is required by the Sun Cluster 3.0 nodes and due to supportability constraints. For example:

- The Remote Procedure Call (RPC) system startup script is not disabled because RPC is used by the volume management software.

- The Solaris Basic Security Module (BSM) is not enabled because the BSM subsystem is difficult to optimize for appropriate logging levels and produces log files that are time-consuming to interpret. This subsystem should only be enabled in sites that have the expertise and resources to manage the generation and data reconciliation tasks required to use BSM effectively.
- Solaris OE minimization is currently not supported for use with Sun Cluster 3.0 software.

Now that all software is installed, each of the Solaris OE images running on each of the Sun Cluster 3.0 nodes can be secured.

Note – Before implementing the security recommendations in the following sections, note that all non-encrypted access mechanisms to the systems (such as TELNET and RSH) will be disabled. The hardening steps will not disable console serial access over the serial port.

Executing the Solaris Security Toolkit Software

This section explains the process the Solaris Security Toolkit software uses to harden each server in a web server cluster. No changes to the default `suncluster30u2-secure.driver` script are required for these agents.

The the `suncluster30u2-secure.driver` script lists all security-specific scripts appropriate for a Sun Cluster 3.0 software installation. This script defines files and scripts to be run by the `driver.run` script. This driver is written to harden an already-built Sun Cluster 3.0 software cluster.

The custom driver for Sun Cluster 3.0 nodes performs the following tasks:

- Installs and executes FixModes software
- Installs Recommended and Security patches
- Installs MD5 software
- Makes 80+ modifications to the Solaris OE

Note – Before implementing the security recommendations in this section, it should be understood that all non-encrypted access mechanisms to the nodes will be disabled, such as TELNET, RSH, and FTP. The hardening steps will not disable console serial access over the serial port.

The Solaris Security Toolkit software executes as follows:

```
# cd /opt/SUNWjass
# ./jass-execute -d suncluster30u2-secure.driver
./jass-execute: NOTICE: Executing driver,
suncluster30u2-secure.driver

============================================================
suncluster30u2-secure.driver: Driver started.
============================================================
[...]
```

By executing the `suncluster30u2-secure.driver` script, all of the security modifications included in that script are made on the system. The current release of this driver includes over 80 security modifications to the Solaris OE image running on each node of the cluster.

Note – The `suncluster30u2-secure.driver` automatically executes the FixModes program, which must be installed as described previously, to tighten file system permissions on the system.

Log Files

In addition to displaying the output to the console, a log file is created in the `/var/opt/SUNWjass/run` directory. Each Solaris Security Toolkit software run creates another run directory in `/var/opt/SUNWjass/run`. The names of these directories are based on the date and time the run begins.

Caution – Do not modify the contents of the `/var/opt/SUNWjass/run` directories under any circumstances. Modifying the files contained in these directories may corrupt the contents and cause unexpected errors when using Solaris Security Toolkit software features such as `undo`.

Verifying Node Hardening

Once the hardening process has been completed and a node has been hardened, reboot the node and verify its configuration by having it assume the appropriate Sun Cluster 3.0 software role. This must be done before you harden any other nodes in the cluster.

Note – Do not harden other Sun Cluster nodes before verifying that the hardened configuration of each node functions properly in your environment.

Once the hardened node has taken control of the cluster, and you have verified its functionality, you can individually harden the other nodes. Do not harden all nodes simultaneously. After verifying each node, perform the entire software installation and the hardening process described above on each of the other nodes, in turn.

Note – We recommend that you disable the failover before hardening any of the nodes, and you should re-enable failover only after each node has been hardened, rebooted, and tested. This is to avoid having the cluster software fail over to a hardened node before it has been fully hardened and before the hardened configuration has been validated.

Hardening Results

After the preceding hardening steps are completed, the number of daemons and services running on each of the nodes is significantly less.

On the node where these recommendations were tested, the number of Solaris TCP services listed by `netstat` decreased from 31, prior to running the toolkit, to 7. Similarly, the number of UDP IPv4 services listed by `netstat` went from 57 to 6. By reducing the number of services available, the exposure points of this system are significantly reduced and the security of the entire cluster is dramatically improved.

Maintaining a Secure System

Maintaining a secure system requires vigilance, as the default security configuration for any system tends to become increasingly open over time. In the case of a cluster, this is particularly true because of the sensitivity of information contained on and offered by it. An in-depth discussion on ongoing system maintenance is beyond the scope of this article, but several areas are introduced to raise your awareness.

First, keep in mind that Solaris OE patches can install additional software packages as part of their installation and may overwrite system configuration files. Be sure to review the security posture of a system after, and ideally before, any patch installation is performed. The Solaris Security Toolkit software can assist you with this, as it was built to support multiple runs on a system. Running it after any patch installation, with the correct drivers, will ensure that added software is disabled. Also perform a manual review of the system because the version of the Solaris Security Toolkit software being used may not support the new features added by the installed patches.

Secondly, monitor the system on an ongoing basis to ensure that unauthorized behavior is not taking place. Reviewing system accounts, passwords, and access patterns can provide a great deal of information about what is being done on the system.

Thirdly, deploy and maintain a centralized syslog repository to collect and parse syslog messages from the cluster nodes. A tremendous amount of information can be logged, and valuable information obtained, by gathering and reviewing these logs.

Lastly, your organization should have a comprehensive vulnerability and audit strategy in place to monitor and maintain system configurations. This is particularly important in the context of maintaining systems in secure configurations over time.

Solaris Security Toolkit Software Backout Capabilities

The Solaris Security Toolkit software can be run multiple times and allows administrators to automatically undo or backout modifications made during a toolkit run.

In addition to displaying the output to the console, a log file is created in the `/var/opt/SUNWjass/run` directory. Each Solaris Security Toolkit software run creates another run directory in `/var/opt/SUNWjass/run`. The names of these directories are based on the date and time the run was begun.

The files stored in the `/var/opt/SUNWjass/run` directory are used not only to track modifications performed on the system, but are also used for the `jass-execute` "undo" functionality. A run, or series of runs, can be undone with the `jass-execute -u` command. For example, on a system where seven separate toolkit runs were performed, they could all be undone with the following command:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1.  December 10, 2001 at 19:45:15 (//var/opt/SUNWjass/run/20011210194515)
2.  December 10, 2001 at 19:25:22 (//var/opt/SUNWjass/run/20011210192522)
3.  December 10, 2001 at 19:07:32 (//var/opt/SUNWjass/run/20011210190732)
4.  December 10, 2001 at 19:04:36 (//var/opt/SUNWjass/run/20011210190436)
5.  December 10, 2001 at 18:30:35 (//var/opt/SUNWjass/run/20011210183035)
6.  December 10, 2001 at 18:29:48 (//var/opt/SUNWjass/run/20011210182948)
7.  December 10, 2001 at 18:27:44 (//var/opt/SUNWjass/run/20011210182744)
8.  Restore from all of them
Choice?  8
./jass-execute: NOTICE: Restoring to previous run
//var/opt/SUNWjass/run/20011210194515

================================================================
undo.driver: Driver started.
================================================================
[...]
```

For more information about the Solaris Security Toolkit software, refer to the `/opt/SUNWjass/Documentation` directory or refer to `http://www.sun.com/security/jass`

Conclusion

Sun Cluster 3.0 software is used to provide mission-critical capabilities to an organization. While the Sun Cluster 3.0 software addresses issues such as fault tolerance, failover, and performance, it is very important that the systems running Sun Cluster 3.0 software are protected against malicious misuse and other attacks such as denial of service. The most effective mechanism for doing this is to configure the nodes in a cluster so that they can protect themselves against attack.

This article describes a supported procedure by which certain Sun Cluster 3.0 12/01 software agents can be run on secured and hardened Solaris OE systems. By implementing these recommendations for the iPlanet Enterprise Server, Apache Web server, and iPlanet Messaging Server, those systems will increase their reliability, availability, and serviceability as the servers will not be as susceptible to attack. This article takes the recommendations made in other Solaris OE security Sun BluePrints articles and provides a specific configuration for the supported agents to improve the overall security posture. This improvement in overall security is made by dramatically reducing potential access points to the Sun Cluster 3.0 nodes and installing secure access mechanisms. In addition, the implementation of these recommendations can be automatically installed by Solaris Security Toolkit software.

Bibliography

- Deeths, David and Brunette, Glenn, "Using NTP to Control and Synchronize System Clocks - Part II: Basic NTP Administration and Architecture," Sun BluePrints OnLine, August 2001, `http://sun.com/blueprints/0801/NTPpt2.pdf`
- Noordergraaf, Alex, "Building Secure N-Tier Environments," Sun BluePrints OnLine, October 2000, `http://sun.com/blueprints/1000/ntier-security.pdf`
- Noordergraaf, Alex, "Solaris™ Operating Environment Minimization for Security: Updated for the Solaris 8 Operating Environment," Sun BluePrints OnLine, November 2000, `http://sun.com/blueprints/1100/minimize-updt1.pdf`
- Noordergraaf, Alex and Brunette, Glenn, "The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for version 0.3," Sun BluePrints OnLine, June 2001, `http://sun.com/blueprints/0601/jass_conf_install-v03.pdf`
- Noordergraaf, Alex and Brunette, Glenn, "The Solaris™ Security Toolkit - Quick Start: Updated for version 0.3," Sun BluePrints OnLine, June 2001, `http://sun.com/blueprints/0601/jass_quick_start-v03.pdf`
- Noordergraaf, Alex and Watson, Keith, "Solaris™ Operating Environment Security: Updated for the Solaris 8 Operating Environment," Sun BluePrints OnLine, April 2001, `http://sun.com/blueprints/0401/security-updt1.pdf`
- Reid, Jason M and Watson, Keith, "Building and Deploying OpenSSH in the Solaris™ Operating Environment," Sun BluePrints OnLine, July 2001, `http://sun.com/blueprints/0701/openSSH.pdf`

■ Watson, Keith and Noordergraaf, Alex, “Solaris™ Operating Environment Network Settings for Security: Updated for the Solaris 8 Operating Environment,” Sun BluePrints OnLine, December 2000, `http://sun.com/blueprints/1200/network-updt1.pdf`

Author’s Bio: Alex Noordergraaf

Alex Noordergraaf has over 10 years experience in the area of computer and network security. As a Senior Staff Engineer in the Enterprise Engineering group at Sun Microsystems, he is developing, documenting, and publishing security best practices through the Sun BluePrints OnLine program. Published article topics include: Sun Fire™ Midframe System Controller security, secure N-Tier environments, Solaris OE minimization, Solaris OE network settings, and Solaris OE security. In addition, he co-authored the recently published book JumpStart Technology- Effective Use in the Solaris Operating Environment. Alex is also one of the authors of the very popular freeware Solaris Security Toolkit (JASS) software.

Prior to his role in Enterprise Engineering, he was a Senior Security Architect with Sun Professional Services where he worked with many Fortune 500 companies on projects that included Security Assessments, Architecture Development, Architectural Reviews, and Policy/Procedure review and development. In addition to providing billable services to customers, he developed and delivered an Enterprise Security Assessment methodology and training curriculum to be used worldwide by the SunPS^{SM} organization. His customers have included major telecommunication firms, financial institutions, ISPs, and ASPs.

Author’s Bio: Mark Hashimoto

Mark Hashimoto has been with Sun Microsystems in Menlo Park, California, for the past three years. Currently, he is developing the user interface components for the Sun Cluster Products group. Mark was also one of the originators of the SunPlex™ Manager GUI tool. Mark holds a Master’s degree in Computer Science from the University of Arizona.

Author’s Bio: Richard Lau

Richard Lau has three years working experience. As part of the Sun Cluster QA group of Sun Microsystems, his duties include Sun Cluster 2.2 patch testing, testing new features, and performing regression tests for Sun Cluster 3.0 products.