



# Securing the Sun™ Cluster 3.x Software

---

*Alex Noordergraaf, Enterprise Server Products*

*Sun BluePrints™ OnLine—February 2003*



<http://www.sun.com/blueprints>

**Sun Microsystems, Inc.**  
4150 Network Circle  
Santa Clara, CA 95045 USA  
650 960-1300

Part No.: 817-1079-10  
Revision 1.0  
Edition: February 2003

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, Solaris, Solaris Secure Shell, Sun BluePrints, Sun Cluster, JumpStart, Sun Professional Services, Solaris Security Toolkit, SunPS, ORACLE, Solstice DiskSuite, SunSolve, Sun Cluster, Sun Enterprise, Sun PS, and SunSolve Online, are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

---

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, Solaris, Solaris Secure Shell, Sun BluePrints, Sun Cluster, JumpStart, Sun Professional Services, Solaris Security Toolkit, SunPS, ORACLE, Solstice DiskSuite, SunSolve, et SunSolve Online sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.



Please  
Recycle



Adobe PostScript

# Securing the Sun Cluster 3.x Software

---

This article describes how to secure the Solaris™ Operating Environment (Solaris OE) and the Sun™ Cluster 3.x software. To provide a robust environment where Sun Cluster 3.x software can be deployed, very specific requirements are placed on the configuration of the Solaris OE. Before the release of Sun Cluster 3.0 (12/01) software, no secured configurations were supported.

By implementing the recommendations for the supported agents, you can increase the reliability, availability, serviceability, and security (RASS) of systems running the Sun Cluster 3.x software. These objectives are accomplished by securing the servers so that they are not as susceptible to attacks.

This article contains the following topics:

- “Background Information” on page 2
- “Securing Sun Cluster 3.x Nodes” on page 12
- “Maintaining a Secure System” on page 25
- “About the Author” on page 26
- “Acknowledgements” on page 26
- “Related Resources” on page 27

---

## Background Information

This section contains the following topics:

- “Assumptions and Limitations” on page 2
- “Qualified Software Components” on page 3
- “Support” on page 6
- “Using the Solaris Security Toolkit Software” on page 6
- “Solaris OE Defaults and Modifications” on page 6
- “Sun Cluster Software Daemons and Services” on page 9
- “Terminal Server Requirements” on page 10
- “Node Authentication Options” on page 10

## Assumptions and Limitations

In this article, our recommendations are based on several assumptions and limitations as to what can be done to secure Sun Cluster 3.x nodes using a Sun supported configuration. Our recommendations assume a platform based on Solaris OE version 8 or 9 and the Sun Cluster 3.x software. We use the Sun Cluster 3.1 software version in this article.

---

**Note** – Before the release of Sun Cluster 3.0 (12/01) software, no secured configurations were supported.

---

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.

Be aware that hardening Solaris OE configurations to the level described in this article might not be appropriate for your environment. For some environments, you may want to perform fewer hardening operations than recommended. The configuration remains supported in these cases; however, additional hardening beyond what is recommended in this article is not supported.

Minimizing the Solaris OE or removing Solaris OE packages to minimize security exposure is not a supported option on Sun Cluster 3.x nodes at this time. Only the hardening tasks described in this article are supported for Solaris OE systems with Sun Cluster 3.x software running supported agents.

---

**Note** – Standard security rules apply to hardening cluster nodes: *That which is not specifically permitted is denied.*

---

## Qualified Software Components

The configurations described in this article have the following minimum software requirements:

- Solaris 8 OE (2/02) software
- Solaris OE packages and installation
- Sun Cluster 3.1 software
- Supported agents
- ORACLE RAC and r\* service limitations
- Cluster interconnect links
- Solstice DiskSuite™ software

The following subsections describe each of these components.

### Solaris 8 OE

The use of Solaris 9 OE as the core OE for secured Sun Cluster 3.x nodes is supported.

However, this article is based on Solaris 8 OE (2/02). 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 might produce results that are slightly different than those presented in this article.

### Solaris OE Packages and Installation

Sun Cluster 3.x software requires only the Solaris OE *End User* cluster. It is strongly recommended that this Solaris OE cluster be used instead of the *Entire 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.

---

**Note** – This article neither addresses how to install the Solaris OE and Sun Cluster 3.x software, nor how to configure the cluster nodes.

---

Sun Cluster 3.x software allows you to automate the installation of the cluster and Solaris OE software through JumpStart™ software. Correspondingly, you can include the hardening steps performed by the Solaris Security Toolkit software in the JumpStart installation process. This article does not describe methods for integrating the hardening process documented in this article with JumpStart software. For information about this topic, refer to the Sun Cluster 3.x and Solaris™ Security Toolkit documentation.

## Sun Cluster 3.x Software

All Sun Cluster 3.x versions support the hardened configurations described in this article.

Sun Cluster 3.x software provides mission-critical capabilities to an organization. While the Sun Cluster 3.x software addresses issues such as fault tolerance, failover, and performance, it is very important that the systems running Sun Cluster 3.x 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 protect themselves against attack.

## Supported Agents

The most current listing of agents, and their corresponding software product versions, supported in a hardened configuration, is available in the Release Notes distributed with the Sun Cluster 3.x software. When determining the versions of supported software, refer to the Release Notes for the version of Sun Cluster 3.x software being used.

## ORACLE RAC and r\* Service Limitations

During ORACLE RAC installation, if an option is chosen to install RAC on all the cluster nodes, then ORACLE Installer uses `rsh` and `rcp` to copy files to other cluster nodes. Also, other ORACLE configuration tools (for example, `netca`) use `rsh` to modify configuration files on other cluster nodes.

---

**Note** – When using the Solaris Security Toolkit Sun Cluster 3.x driver, both `rsh` and `rcp` are disabled by default. These services are insecure and should not be left enabled on a secured cluster.

---

It is possible to install a cluster on each node and set up configuration files manually on each node, if an administrator does not want to change security settings.

In sites where the availability of `rsh` and `rcp` is critical, a secure mechanism provides the same functionality (equivalent to `rsh`, `rsh: ssh`, and `scp`) through the Secure Shell (SSH), if configured properly. These commands provide an encrypted and authenticated mechanism for ORACLE software to perform tasks on remote machines.

Configure SSH to permit remote login without passwords, then replace the system-provided `rsh` and `rsh: rcp` binaries with links to the SSH commands. In this way, you can provide secure `rsh` and `rsh: rcp` link functionality. This approach simplifies the installation and configuration of ORACLE RAC while still maintaining a secure posture.

## 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.

We strongly recommend that these interconnects be implemented using separate and dedicated network equipment. From a security and availability perspective, we discourage the use of VLANs because they typically restrict packets based only on tags added by the switch. Minimal, if any, assurance is provided for validating these tags, and no additional protection against directed Address Resolution Protocol (ARP) attacks is gained.

## Solstice DiskSuite Software

The configuration in this article assumes the use of Solstice DiskSuite software instead of VERITAS Volume Manager. If VERITAS Volume Manager is used, then the entries added by VERITAS to the `/etc/inetd.conf` file should be left enabled and the Solstice DiskSuite software entries disabled.

## Support

The secured Sun Cluster 3.x software configuration implemented by the Solaris Security Toolkit `suncluster3x-secure.driver` is a Sun Microsystems-supported configuration for agents described in this document. Only Sun Cluster 3.x software implementations using the agents explicitly described in this article and referenced in the Sun Cluster 3.x Release Notes are supported in hardened configurations.

---

**Note** – Hardening Sun Cluster 2.x is not supported. Only agents listed in the Sun Cluster 3.x Release Notes are supported in hardened configurations when the hardening is performed based on the recommendations contained in this article.

---

For information on the supportability of the Solaris Security Toolkit, refer to its documentation.

---

**Note** – Sun Microsystems supports hardening Sun Cluster 3.x clusters whether security modifications are performed manually or through the use of the Solaris Security Toolkit software.

---

## Using the Solaris Security Toolkit Software

The drivers described in this article are included in version 0.3.10 of the Solaris Security Toolkit software. We use this software to implement the hardening. Use this version, or newer versions, of the software when implementing the recommendations of this article. The Solaris Security Toolkit provides an error-free, standardized mechanism for performing the hardening process. Additionally, because it allows you to undo changes after they are made, we highly recommended that you use this software to perform the hardening process.

## Solaris OE Defaults and Modifications

The Solaris OE configuration of a cluster node has many of the same issues as other default Solaris OE configurations. For example, too many daemons are used and other insecure daemons are enabled by default. Some insecure daemons include: `in.telnetd`, `in.ftpd`, `fingered`, and `sadmind`. For a complete list of default Solaris OE daemons and security issues associated with them, refer to the “Solaris Operating Environment Security: Updated for Solaris 9 OE” Sun BluePrints™ OnLine article.

This article recommends that all unused services be disabled. Based on the Solaris OE installation cluster (`SUNWCa11`) typically used for a Sun Cluster 3.x node, there are over 100 recommended Solaris OE configuration changes to improve the security configuration of the Solaris OE image running on each node. While the `SUNWCa11` Solaris OE cluster is typically used for cluster installations, only the `SUNWuser` cluster is required. It is strongly recommended that you limit the number of Solaris OE services and daemons installed by using the Solaris OE cluster that contains the fewest number of packages.

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. All of the interactive services normally started from `inetd` are then replaced by Secure Shell (SSH). This approach cannot be used with Sun Cluster 3.x software.

The primary reason for this limitation is that volume management software requires several remote procedure call (RPC) services to be available. And, the Sun Cluster 3.x software installs additional RPC-based services.

Implementing these modifications is automated when you use the driver script `suncluster3x-secure.driver` available in version 0.3.10 of the Solaris Security Toolkit software.

## Disabling Unused Services

The security recommendations in this article include all Solaris OE modifications that do not affect required Sun Cluster 3.x node functionality. Be aware that these modifications may not be appropriate for every Sun Cluster environment. In fact, it is possible that some of the services disabled by the default `suncluster3x-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. Therefore, the security modifications of each Sun Cluster environment may vary slightly based on the applications being run in that environment.

---

**Note** – Consider the role of a secured configuration in the context of the applications and services that the Sun Cluster 3.x software supports. The security configuration presented in this article is a high watermark for system security, because every service that is not required by the Sun Cluster 3.x software 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.x software.

---

## Recommendations and Exceptions

Our recommendations for securing the server configuration consist of modifying recommendations made in the Sun BluePrints OnLine article “Solaris Operating Environment Security: Updated for Solaris 9 Operating Environment.” We customize the recommendations to provide a configuration specifically for the supported agents.

The recommendations in this article improve the overall security posture of Sun Cluster 3.x nodes. This improvement is made by dramatically reducing access points to the Sun Cluster 3.x nodes and by installing secure access mechanisms. To streamline the implementation of these recommendations, we provide the Solaris Security Toolkit software, which automates many of the changes.

We made the following exceptions to the recommendations provided in the previously mentioned article, due to functionality that is required by the Sun Cluster 3.x software and support constraints:

- RPC system startup script is *not disabled*, because RPC is used by volume management software.
- Solaris basic security module (BSM) is *not enabled*. The BSM subsystem is difficult to optimize for appropriate logging levels and produces log files that are difficult to interpret. This subsystem should only be enabled at sites where you have the expertise and resources to manage the generation and data reconciliation tasks required to use BSM effectively.
- Solaris OE minimization (removing unnecessary Solaris OE packages from the system) is not supported with Sun Cluster 3.x software.

## Mitigating Security Risks of Solaris OE Services

Detailed descriptions of Solaris OE services and recommendations on how to mitigate their security implications are available in the following Sun BluePrints OnLine articles:

- “Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment”
- “Solaris Operating Environment Network Settings for Security: Updated for Solaris 8 Operating Environment”

The recommendations are implemented by the Solaris Security Toolkit in either its standalone or JumpStart modes.

## Sun Cluster Software Daemons and Services

The Sun Cluster 3.x software adds several daemons and services to a system. These include daemons running on the system and additional RPC services. The following daemons run on a default Sun Cluster 3.1 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.pmfcd
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
root 2260 1 0 Dec 12 ? 0:00 /usr/cluster/lib/sc/cl_eventd
root 2356 1 0 Dec 12 ? 0:23 /var/cluster/spm/bin/scguieventd
```

The Sun Cluster 3.1 software installation installs the following additional 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.x 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 qualified 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.metacl - DiskSuite cluster control
100281/1 tli rpc/tcp wait root /usr/sbin/rpc.metacl rpc.metacl
```

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 and disable the unneeded Solstice DiskSuite software entries.

## Terminal Server Requirements

Sun Cluster 3.x software does not require a specific terminal server as Sun Cluster 2.x software did. This change is a significant improvement from a security perspective. Terminal server connections frequently do not use encryption. Lack of encryption allows a malicious individual to sniff the network and “read” the commands being issued to the client. Frequently, these commands 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 a terminal server that implements Secure Shell (SSH).

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

## Node Authentication Options

Node authentication is how potential nodes must identify themselves before being allowed to join a cluster. Sun Cluster 3.x software provides several options for node authentication. Ensuring that all nodes are properly authenticated is a critical aspect of cluster security. This section describes the available node authentication options and provides recommendations on which level of node authentication to use.

The available node authentication options in Sun Cluster 3.x software are as follows:

- None (for example, any system is permitted to join the cluster)
- IP address
- UNIX®
- Diffie-Hellman using DES

In addition, the `scsetup` command provides the following submenu under the New Nodes menu option::

```
*** 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
6) New nodes
?) Help
q) Return to the Main Menu
```

At a minimum, the node authentication should be set up to require that new cluster nodes be added manually rather than automatically. Select option 1 to restrict the ability of systems to add themselves, then use option 3 to specify the name of the new cluster node. These two options run `scconf` with the following commands, which you can 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 it says it is. The two alternatives are standard UNIX or Diffie-Hellman authentication.

The default is to use UNIX authentication. If a private interconnect connects the nodes and the `scconf` command is used to restrict new nodes from joining, this approach is probably adequate.

In environments where other systems may attempt to join the cluster, or if the data on the cluster is particularly sensitive, then we recommend using the Diffie-Hellman authentication method.

Diffie-Hellman authentication uses Secure RPC to authenticate the nodes in the cluster. This authentication requires that the public and private keys be properly set up on each of the nodes. The most effective way to do this task is through NIS+, because it simplifies the management and maintenance of these key pairs. However, it is 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.x Nodes

Building a secure system requires that entry points into the system be limited and restricted, in addition to limiting how authorized users obtain privileges. To effectively secure each node in a cluster, you must make changes to the Solaris OE software running on each node.

Properly securing the Sun Cluster 3.x nodes requires the following:

- “Installing Solaris OE and Sun Cluster Software” on page 12
- “Adding Security Software” on page 12
- “Installing Downloaded Software and Implementing Modifications” on page 18
- “Verifying Node Hardening” on page 20
- “Reviewing the Results” on page 21

## Installing Solaris OE and Sun Cluster Software

At this point in the process, we assume that you have installed the appropriate Solaris OE, Solaris OE cluster on the cluster nodes, and the Sun Cluster 3.x software. Also, we assume that you have configured the software.



---

**Caution** – Install the security software only if the cluster is installed and running with the appropriate agents. (Refer to “Supported Agents” on page 4.)

---

## Adding Security Software

The next stage in hardening Sun Cluster 3.x nodes requires downloading and installing additional software security packages. This section covers the following tasks:

- “To Install Solaris Security Toolkit Software” on page 13
- “To Download Recommended and Security Patch Software” on page 14
- “To Download FixModes Software” on page 15
- “To Download OpenSSH Software” on page 16
- “To Download MD5 Software” on page 17

---

**Note** – Of the software described in this section, the Solaris Security Toolkit, Recommended and Security Patch Cluster, FixModes, and MD5 software are required. The use of a Secure Shell product is strongly recommended and is bundled with Solaris 9 OE. For Solaris 8 OE the use of OpenSSH is recommended, though not required. Instead of OpenSSH, you can substitute a commercial version of Secure Shell, available from a variety of vendors.

---

## ▼ To Install Solaris Security Toolkit Software

The Solaris Security Toolkit version 0.3.10 software must be downloaded first, then installed on each of the nodes. Later, you'll use the Solaris Security Toolkit to automate installing other security software and implementing the Solaris OE modifications for hardening the system.

The primary function of the Solaris Security Toolkit software is to automate and simplify building secured Solaris OE systems based on the recommendations contained in this and other security-related Sun BluePrints OnLine articles.

---

**Note** – The following instructions use file names that are correct only for version 0.3.10 of the Solaris Security Toolkit software.

---

1. **Download the source file (SUNWjass-0.3.10.pkg.Z) from the following web site:**

```
http://www.sun.com/security/jass
```

2. **Extract the source file into a directory on the server using the `uncompress` command:**

```
# uncompress SUNWjass-0.3.10.pkg.Z
```

3. **Install the Solaris Security Toolkit software on the server using the `pkgadd` command:**

```
# pkgadd -d SUNWjass-0.3.10.pkg SUNWjass
```

Executing this command creates the `SUNWjass` subdirectory in `/opt`. This subdirectory contains all Solaris Security Toolkit software directories and associated files. The script `make-jass-pkg`, included in Solaris Security Toolkit software releases since version 0.3, allows administrators to create custom packages using a different installation directory.

## ▼ To Download Recommended and Security Patch Software

Patches are regularly released by Sun to provide Solaris OE fixes for performance, stability, functionality, and security. It is critical to the security of a system that the most up-to-date patch is installed. To ensure that the latest Solaris OE Recommended and Security Patch is installed, this section describes how to download the latest patch cluster and store them uncompressed in the `/opt/SUNWjass/Patches` directory on each node.

Downloading the latest patch cluster does not require a SunSolve<sup>SM</sup> program support contract.

---

**Note** – Apply standard best practices to all patch installations. Before installing any patches, evaluate and test them on non-production systems or during scheduled maintenance windows.

---

1. **Download the latest patch from the SunSolve Online<sup>SM</sup> web site at:**

`http://sunsolve.sun.com`

2. **Click on the “Patches” link, at the top of the left navigation bar.**

3. **Select the appropriate Solaris OE version in the Recommended Solaris Patch Clusters box.**

In our example, we select Solaris 8 OE.

4. **Select the best download option, either HTTP or FTP, with the associated radio button, then click Go.**

A Save As dialog box is displayed in your browser window.

5. **Save the file locally.**

6. **Move the file securely to the node being hardened using the `scp` SSH command, the `sftp` SSH command, or the `ftp` command (if SSH is not yet installed).**

The `scp` command used to copy the file to a domain called `scnode01` should appear similar to the following:

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

## 7. 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
[. . .]
```

Later, using the Solaris Security Toolkit software, you'll install the patch after downloading all the other security packages.

---

**Note** – If you do not place the Recommended and Security Patches software into the `/opt/SUNWjass/Patches` directory, a warning message displays when you execute the Solaris Security Toolkit software.

---

## ▼ To Download FixModes Software

FixModes is a software package that tightens the default Solaris OE directory and file permissions. Tightening these permissions can significantly improve overall security. More restrictive permissions make it even more difficult for malicious users to gain privileges on a system.

### 1. Download the FixModes precompiled binaries from:

[http://www.Sun.COM/blueprints/tools/FixModes\\_license.html](http://www.Sun.COM/blueprints/tools/FixModes_license.html)

The FixModes software is distributed as a precompiled and compressed tar file formatted for SPARC™ based systems. The file name is `FixModes.tar.Z`.

### 2. Save the file, `FixModes.tar.Z`, in the Solaris Security Toolkit software Packages directory in `/opt/SUNWjass/Packages`.



---

**Caution** – Leave the file in its compressed state.

---

Later, using the Solaris Security Toolkit software, you'll install the FixModes software after downloading all the other security packages.

## ▼ To Download OpenSSH Software

In any secured environment, the use of encryption in combination with strong authentication is required to protect user-interactive sessions. At a minimum, user interactive sessions must be encrypted.

The tool most commonly used to implement encryption is SSH software, whether a commercial or open source (freeware) version. To implement all the security modifications performed by the Solaris Security Toolkit software and recommended in this article, you need to implement a SSH software product.

The Solaris Security Toolkit software disables all non-encrypted user-interactive services and daemons on the system, in particular daemons such as `in.rshd`, `in.telnetd`, and `in.ftpd`. Access to the system can be gained with SSH similarly to what is provided by RSH, Telnet, and FTP.

The Solaris 9 OE includes a bundled version of OpenSSH called the Solaris Secure Shell. The use of this software is highly recommended on Solaris 9 OE Sun Cluster environments because Solaris Secure Shell is supported by Sun. If you are using this product, then it is not necessary to perform the steps in this section. If you are not using Solaris Secure Shell on Solaris 9 OE, then use an alternative SSH version so that you can implement all of the recommended security modifications.

---

**Note** – If you choose to use an SSH product other than OpenSSH or the bundled Solaris Secure Shell, install and configure it before or during a Solaris Security Toolkit run.

---

- **Obtain the following online article and use the instructions in that article for downloading the software.**

A Sun BluePrints OnLine article about how to compile and deploy OpenSSH titled “Building and Deploying OpenSSH on the Solaris Operating Environment” is available at:

`http://www.sun.com/security/blueprints`

Later, using the Solaris Security Toolkit software, you’ll install the OpenSSH software after downloading all the other security packages.



---

**Caution** – If possible, do not compile OpenSSH on the cluster nodes and do not install the compilers on the cluster nodes. Use a separate Solaris OE system—running the same Solaris OE version, architecture, and mode (for example, Solaris 8 OE, Sun4u, and 64-bit)—to compile OpenSSH. If you implement a commercial version of SSH, then no compilation is required. The goal is to limit the availability

of compilers to potential intruders. Understand, however, that this does not provide significant protection against determined attackers because they still can install compiled tools.

---

## ▼ To Download MD5 Software

The MD5 software validates MD5 digital fingerprints on the cluster. Validating the integrity of Solaris OE binaries provides a robust mechanism to detect system binaries that are altered or *trojaned* (hidden inside something that appears safe) by unauthorized users. By modifying system binaries, attackers provide themselves with backdoor access onto a system; they hide their presence and cause systems to operate in unstable manners.

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

**1. Download the MD5 binaries from:**

[http://www.sun.com/blueprints/tools/md5\\_license.html](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`



---

**Caution** – 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.

After the MD5 binaries are installed, you can use them to verify the integrity of executables on the system through the Solaris Fingerprint Database. More information on the Solaris Fingerprint Database is available in the Sun BluePrints OnLine article titled “The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files:”

<http://www.sun.com/blueprints/0501/Fingerprint.pdf>

**3. (Optional) Download and install Solaris Fingerprint Database Companion and Solaris Fingerprint Database Sidekick software from the SunSolve Online web site at:**

<http://sunsolve.sun.com>

We strongly recommend that you install these optional tools and use them with the MD5 software. These tools simplify the process of validating system binaries against the database of MD5 checksums. Use these tools frequently to validate the integrity of the Solaris OE binaries and files on the cluster nodes.

These tools are described in the “The Solaris™ Fingerprint Database - A Security Tool for Solaris Software and Files” Sun BluePrints Online article.

## Installing Downloaded Software and Implementing Modifications

Now that all software is downloaded and added to the correct directories, each of the Solaris OE images running on each of the Sun Cluster 3.x nodes can be secured.

The Solaris Security Toolkit version 0.3.10 provides a driver (`suncluster3x-secure.driver`) for automating the installation of security software and Solaris OE modifications. The driver for the cluster nodes performs the following tasks:

- Installs and executes the FixModes software to tighten file system permissions
- Installs the MD5 software
- Installs the Recommended and Security Patch software
- Implements over 100 Solaris OE security modifications

---

**Note** – During the installation and modifications implemented in this section, all non-encrypted access mechanisms to the nodes—such as Telnet, RSH, and FTP—are disabled. The hardening steps do not disable console serial access over serial ports.

---



---

**Caution** – Harden only one cluster node at a time. Before hardening the next node, verify that the hardened configuration functions properly in your environment.

---

## ▼ To Install Downloaded Software and Implement Modifications

1. Disable the failover mode before hardening a node.
2. On *one node only*, execute the `suncluster3x-secure.driver` script as follows:

```
# cd /opt/SUNWjass
# ./jass-execute -d suncluster3x-secure.driver
./jass-execute: NOTICE: Executing driver,
suncluster3x-secure.driver

=====
suncluster3x-secure.driver: Driver started.
=====
[...]
```

By executing the `suncluster3x-secure.driver` script, all of the security modifications included in the script are made on the system. The current release of this driver includes over 100 security modifications to the Solaris OE image running on each node of the cluster.

---

**Note** – The `suncluster3x-secure.driver` automatically executes the `FixModes` program, which must be already downloaded and filed in the correct directory as described previously, to tighten file system permissions on the system.

---

When the Solaris Security Toolkit program executes the `FixModes` program, the following warning messages are displayed:

```
Installing 'fix-modes' into ///opt/FixModes

Executing 'fix-modes' from ///opt/FixModes.
secure-modes: WARNING: Can't find required uid/gid smmsp
secure-modes: WARNING: Can't find required uid/gid smmsp
```

These are known warning messages from `FixModes` that can be safely ignored.

To view the contents of the driver file and obtain information about the Solaris OE modifications, refer to the Solaris Security Toolkit documentation available either in the `/opt/SUNWjass/Documentation` directory or through the web at:

<http://www.sun.com/security/jass>

For information about other scripts in the Solaris Security Toolkit software, refer to the Solaris Security Toolkit documentation available from this URL.

**3. Verify that the node is hardened.**

Refer to “Verifying Node Hardening” on page 20 for detailed instructions.

**4. Re-enable failover *only* after each node is hardened, rebooted, and tested.**

This task keeps the cluster software from failing over to a hardened node before it is fully hardened and before the hardened configuration is validated.

**5. After you complete the hardening process for a node, use the procedure in “Verifying Node Hardening” on page 20 to verify that the configuration.**

## Verifying Node Hardening

After performing the procedures in this article to harden a cluster node, test the configuration and hardening.

The number of daemons and services running on each of the nodes is significantly less after the hardening steps are completed. For the example configuration, our testing resulted in the following:

- On the node where these recommendations were tested, the number of Solaris TCP services listed by `netstat` decreased from 31 to 7.
- 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.

---

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

---

## ▼ To Verify Node Hardening

1. **After you complete the hardening process for a node, reboot the node and verify its configuration by having it assume the appropriate Sun Cluster 3.x software role.**

This step *must* be done before you harden any other nodes in the cluster.



---

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

---

2. **When the hardened node takes control of the cluster, verify the node's functionality.**
3. **After verifying that the node is functioning properly, perform the entire software installation and hardening process on the next node.**

Refer to “Securing Sun Cluster 3.x Nodes” on page 12 for the procedure.



---

**Caution** – Do not harden all nodes simultaneously.

---

## Reviewing the Results

After you harden a node, you can review the results of the Solaris Security Toolkit run, to determine if fewer services are enabled.

## ▼ To Review the Results of a Run

- **Review the run directory in `/var/opt/SUNWjass/run`.**

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

---

**Note** – Do not modify the contents of the `/var/opt/SUNWjass/run` directories under any circumstances. Modifying the files can corrupt the contents and cause unexpected errors when you use Solaris Security Toolkit software features such as `undo`.

---

The files stored in the `/var/opt/SUNWjass/run` directory track modifications performed on the system and enable the `jass-execute undo` feature. You can undo a run, or series of runs, with the `jass-execute -u` command. For example, on a system where two separate Solaris Security Toolkit runs are performed, you could undo them by using the following command:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1. September 25, 2001 at 06:28:12 (/var/opt/SUNWjass/run/
20010925062812)
2. April 10, 2001 at 19:04:36 (/var/opt/SUNWjass/run/
20010410190436)
3. Restore from all of them
Choice? 3
./jass-execute: NOTICE: Restoring to previous run
//var/opt/SUNWjass/run/20010410190436

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

Refer to the Solaris Security Toolkit documentation for details on the capabilities and options available in the `jass-execute` command.

Based on our qualified configuration, we find the following noncluster services remain running on a hardened 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 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/keyserver -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. We made several configuration modifications on this node after the operating system was installed. These modifications include the configuration of `xntp` and NIS, and the installation of OpenSSH.

The following output is generated for our sample configuration 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.x software-specific ports that accept connections only from other cluster nodes. When a connection request from a noncluster 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
```

---

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

---

Cluster nodes are added based on the authentication method defined in the Sun Cluster 3.x software configuration. We recommend that you use the strongest possible method of authentication. The available options are described in “Node Authentication Options” on page 10.

---

## Maintaining a Secure System

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

- Keep in mind that Solaris OE patches install additional software packages as part of their installation and may overwrite your 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 installing patches, as it was built to support multiple runs on a system. Running it after any patch installation, with the correct drivers, ensures 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.

- Monitor the system on an ongoing basis to ensure that unauthorized behavior is not taking place. Review system accounts, passwords, and access patterns; they can provide a great deal of information about what is being done on a system.
- 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.
- Your organization needs to have a comprehensive vulnerability and audit strategy in place to monitor and maintain system configurations. This requirement is particularly important in the context of maintaining systems in secure configurations over time.

---

## About the Author

Alex Noordergraaf has over 10 years experience in the areas of computer and network security. As the Security Architect of the Enterprise Server Products (ESP) group at Sun Microsystems, he is responsible for the security of Sun midframe and high-end servers. He is the co-founder of the popular freeware Solaris Security Toolkit. Before joining ESP he was a Senior Staff Engineer in the Enterprise Engineering (EE) group of Sun Microsystems, where he developed, documented, and published security best practices through the Sun BluePrints program. Published topics include security for Sun Fire servers, Sun™ Cluster software, Sun Fire Midframe servers, Sun Enterprise™ 10000 servers, N-Tier environments, the Solaris OE, and the Solaris OE network settings. He co-authored the Sun BluePrints publication, *JumpStart™ Technology: Effective Use in the Solaris™ Operating Environment*.

Prior to his role in EE, 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. He developed and delivered an enterprise security assessment methodology and training curriculum to be used worldwide by SunPS<sup>SM</sup>. His customers included major telecommunication firms, financial institutions, ISPs, and ASPs. Before joining Sun, Alex was an independent contractor specializing in network security. His clients included BTG, Inc. and Thinking Machines Corporation.

---

## Acknowledgements

Without the support of the Sun Cluster Software Product Marketing, Engineering, and Quality Assurance teams this article would not have been possible. Many thanks to everyone involved including Mark Hashimoto, Richard Lau, Navdeep Parhar, Meenakshi Kaul-Basu, Balaji Pagadala, and Anni Lai.

---

## Related Resources

- Dasan, Vasanthan; Noordergraaf, Alex; and Ordica, Lou. *The Solaris Fingerprint Database - A Security Tool for Solaris Software and Files*, Sun BluePrints OnLine, May 2001, <http://www.sun.com/blueprints/0501/Fingerprint.pdf>.
- 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. "Minimizing the Solaris Operating Environment for Security: Updated for Solaris 9 Operating Environment," Sun BluePrints OnLine, November 2002, <http://sun.com/blueprints/1102/816-5241.html>.
- 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\\_config\\_install-v03.pdf](http://sun.com/blueprints/0601/jass_config_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](http://sun.com/blueprints/0601/jass_quick_start-v03.pdf).
- Noordergraaf, Alex and Brunette, Glenn. *The Solaris Security Toolkit - Internals: Updated for version 0.3*, Sun BluePrints OnLine, June 2001, [http://sun.com/blueprints/0601/jass\\_config\\_install-v03.pdf](http://sun.com/blueprints/0601/jass_config_install-v03.pdf).
- Noordergraaf, Alex and Watson, Keith. "Solaris Operating Environment Security: Updated for the Solaris 9 Operating Environment," Sun BluePrints OnLine, December 2002, <http://sun.com/blueprints/1202/816-5242.html>.
- 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>.

