



Securing the Sun Fire™ 12K and 15K Domains

*Alex Noordergraaf and Dina K. Nimeh,
Enterprise Server Products*

Sun BluePrints™ OnLine—February 2003



<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.: 817-1357-10
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, Sun Fire, Sun BluePrints, Solaris Security Toolkit, JumpStart, Sun Quad FastEthernet, SunSolve OnLine, Sun Cluster, Sun Enterprise, Sun PS, and Sun SupportForum 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 intellectuels relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuels 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, Sun Fire, Sun BluePrints, Solaris Security Toolkit, JumpStart, Sun Quad FastEthernet, SunSolve OnLine, Sun Cluster, Sun Enterprise, Sun PS, et Sun SupportForum 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 Sun Fire™ 12K and 15K Domains

This Sun BluePrints™ OnLine article documents security modifications that you can implement on Sun Fire™ 12K and 15K domains without adversely affecting its behavior. The configuration changes described in this article enable Solaris™ Operating Environment (OE) security features and disable other potentially insecure services and daemons.

This article is one in a series that provides recommendations for enhancing the security of a Sun Fire system. Before securing the domains, we recommend that you use the Sun BluePrints OnLine article “Securing the Sun Fire 12K and 15K System Controller” to secure Sun Fire 12K and 15K system controllers.

This article contains the following topics:

- “Goal” on page 2
- “Background Information” on page 3
- “Securing Sun Fire Domains” on page 12
- “Verifying Domain Hardening” on page 24
- “About the Authors” on page 28
- “Related Resources” on page 29

Goal

The Sun Fire 12K and 15K servers are the largest Sun servers currently sold and are used for projects and deployments ranging from server-consolidation projects in financial institutions to extremely sensitive data-storage applications at government agencies. Such deployments require that systems be secured against unauthorized access and misuse by malicious individuals.

Sun Fire domains introduce a variable to Solaris OE systems through platform-specific software components (for example, daemons) and services. These platform-specific software components impact the processes and procedures that must be used to secure the Solaris OE configuration running on Sun Fire domains. To properly secure Sun Fire domains, you must understand the impact of these new software components and have access to a well-documented and well-supported configuration to identify which modifications are appropriate and which would not be appropriate.

The goal of this Sun BluePrints OnLine article is to provide a sample baseline security configuration for Sun Fire domains by describing and implementing all supported Solaris OE security modifications. After reading about the Sun tested and supported configuration in this article, you'll understand how the configuration of a secured Sun Fire domain differs from the secured configurations of other Sun systems.

If your system requires any of the services that we recommend disabling, then the sample configuration in this article may not be appropriate. Other configurations that do not implement all of the security modifications in this article are acceptable. However, we recommend that you carefully evaluate services and daemons not disabled to verify that they are required and that they are carefully protected against misuse.

To automate the installation of security software and implementation of security modifications, we provide a customized driver in the Solaris™ Security Toolkit.

Background Information

The following sections provide helpful information for understanding security issues involving Sun Fire domains, hardware and software requirements, and other topics. This section contains the following topics:

- “Assumptions and Limitations” on page 3
- “Obtaining Support” on page 5
- “Default Domain Software and Configurations” on page 5
- “Domain Security Options in SMS 1.3” on page 8
- “Solaris OE Defaults and Modifications” 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 Fire domains.

Our recommendations assume a platform based on the following characteristics:

- Solaris 8 OE 2/02 (Update 7) software or newer
- System Management Services (SMS) 1.3 software
- SUNWCall Solaris OE cluster
- Sun Quad FastEthernet™ card installed in each domain
- Solaris OE minimization is not discussed in this article, but is supported

Note – The examples in this article are for a domain running Solaris 9 OE.

Using other software versions and platform characteristics may produce results that vary from those presented 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 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 hardening Sun Fire domains: *That which is not specifically permitted is denied.*

Solaris OE hardening can be interpreted in many ways. For purposes of hardening Sun Fire domains, we address hardening all possible Solaris OE options. That is, anything that can be hardened, is hardened. When there are good reasons for leaving services and daemons as they are, we do not harden or modify them.

You can harden Sun Fire domains automatically during a JumpStart™ installation of the operating system (OS), or you can harden it after the installation of the OS. This article documents the process for manually hardening a domain after the OS installation, because addressing the JumpStart environment is beyond the scope of this article.

For information about setting up a JumpStart server and integrating a JumpStart server with the Solaris Security Toolkit software, refer to the Sun BluePrints OnLine article “Building a JumpStart™ Infrastructure” or to the Solaris Security Toolkit documentation.

In this article, we do not describe the installation of the Solaris 9 OE, installation of the SUNWCall cluster, and the initial configuration of Sun Fire 12K or 15K domain software. Refer to the product documentation for more information on how to install domain software. Instead, in this article, we focus on the tasks for securing a domain. These tasks include installing security-related software, installing the latest patch clusters, and hardening the OS. This hardening is critical to the security of the domain, because the default configuration of Solaris OE may not provide the required level of security.

Note – Although this article focuses on domains built using the SUNWCall Solaris OE installation cluster, using this cluster is not required. Other Solaris OE installation clusters containing fewer packages can be installed on Sun Fire domains. Also, individual packages can be removed from these clusters. Solaris OE minimization is supported on Sun Fire domains just as it is on other Sun systems.

Obtaining Support

Sun Fire 12K and 15K domain configurations implemented by the Solaris Security Toolkit domain driver are Sun supported configurations.

The Solaris Security Toolkit provides an error free, standardized mechanism for performing the hardening process, and it enables you to undo most changes after they are made. Although we do not require that you use the Solaris Security Toolkit to harden domains, we strongly recommend it.

Note – Sun supports hardened and minimized domains whether security modifications are performed manually or by using the Solaris Security Toolkit software.

Please note that the Solaris Security Toolkit is not a supported Sun product; only the end-configuration created by the Solaris Security Toolkit is supported. Solaris Security Toolkit support is available through the Sun™ SupportForum discussion group at:

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

Default Domain Software and Configurations

This section describes the default packages, daemons, startup scripts, and other configurations of Sun Fire domains. Although not all of these affect the security of the system directly, from a security perspective, you should always be aware of them and their impact on the system.

Default Packages

The following Sun Fire domain-specific packages are installed as part of the SUNWCall cluster:

system	SUNWdrctx	Dynamic Reconfiguration Modules for Sun Fire 15000 (64-bit)
system	SUNWscmkr	Init script & links for Sun Fire 15000 Key Management daemon
system	SUNWscmku	Key Management daemon for Sun Fire 15000
system	SUNWscmx	Key Management Modules for Sun Fire 15000 (64-Bit)

The Sun Fire domain software does not change the `/etc/passwd`, `/etc/shadow`, or `/etc/group` files. This behavior differs from the Sun Fire System Management Services (SMS) software on the system controller (SC), which modifies these files.

Default Daemons

The Sun Fire domain-specific daemons are as follows:

```
root  11   1 0 17:28:32 ? 0:00 /platform/SUNW,Sun-Fire-15000/lib/cvcd
root  121  1 0 17:28:46 ? 0:00 /usr/platform/SUNW,Sun-Fire-15000/lib/sckmd
```

Dynamic Reconfiguration Daemons

Although they are not Sun Fire 12K nor 15K domain-specific, the following daemons are used for dynamic reconfiguration on Sun Fire domains.

Do not disable the following daemons:

```
root  324   1 0 07:47:24 ?      0:00 /usr/lib/efcode/sparcv9/efdaemon
root   58   1 0 05:32:57 ?      0:00 /usr/lib/sysevent/syseventd
root   60   1 0 05:32:57 ?      0:00 /usr/lib/sysevent/syseventconfd
root   65   1 0 05:32:59 ?      0:00 devfsadmd
root  371   1 0 05:33:12 ?      0:00 /usr/lib/saf/sac -t 300
root  631  295 0 16:30:34 ?      0:00 /usr/lib/dcs
```

Startup Scripts

Sun Fire daemons are started by several startup scripts including the `/etc/init.d/cvc` and `/etc/init.d/sckm` scripts.

Domain-to-System Controller Communication

The additional network used on Sun Fire domains to communicate with the Sun Fire system controller (SC) is defined similarly to regular network connections through an `/etc/hostname.*` entry.

This `/etc/hostname.dman0` entry sets up the I1 or domain-to-SC management network (MAN). The IP address in our example, 192.168.103.2, is defined for this domain as follows:

```
# more /etc/hostname.dman0
192.168.103.2 netmask 255.255.255.224 private up
```


From a security perspective, the network between the domains and the SCs, in addition to any network connection between the domains, is of concern. The I1 network mitigates these concerns by permitting only SC-to-domain and domain-to-SC communication.

The I1 network is implemented as separate point-to-point physical network connections between the SCs and each of the 9 domains supported by a Sun Fire 12K system or 18 domains supported by a Sun Fire 15K system. Each of these connections terminates at separate I/O boards on each domain and SC.

On the SCs, these multiple separate networks are consolidated into one meta-interface to simplify administration and management. The MAN driver software performs this consolidation, enforces domain separation, and fails over to redundant communication paths.

Direct communication between domains over the I1 network is not permitted by the hardware implementation of the I1 network. By implementing the network in this manner, each SC-to-domain network connection is physically isolated from other connections.

The network configuration appears as follows:

```
dman0: flags=1008843<UP,BROADCAST,RUNNING,MULTICAST,PRIVATE,IPv4>
mtu 1500 index 2 inet 192.168.103.2 netmask fffffffe0 broadcast
192.168.103.31 ether 8:0:20:be:f8:f4
```



Caution – Although the `dman0` network supports regular Internet Protocol (IP)-based network traffic, it should only be used by Sun Fire management traffic. Any other use of this internal network may affect the reliability, availability, serviceability, and security (RASS) of the entire platform. Refer to the `scman (7D)` and `dman (7D)` man pages for more information.

System Controller-to-Domain Communication

All Sun Fire SC-to-domain communication over the MAN network is authenticated through IPsec. The IPsec protocol suite provides authentication services at the IP layer as defined by the Internet Engineering Task Force (IETF). For additional information about IPsec, refer to RFC 2411 at <http://www.ietf.org>.

Unauthorized attempts to access Sun Fire domains or SC-specific daemons generate `syslog` messages indicating that an access attempt was made. The `syslog` message is generated by IPsec because the request fails the authentication check required for all MAN-based traffic. A log message appears as follows:

```
Sep 20 08:04:26 sun15-a ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 192.168.181.252, Destination 010.001.073.042.
```

The configuration of IPsec on the domain is maintained in the `/etc/inet/ipsecinit.conf` file, which, by default, contains at least the following entries requiring that all communication to the domain-side daemons be authenticated using IPsec:

```
{ dport sun-dr ulp tcp } permit { auth_algs md5 }
{ sport sun-dr ulp tcp } apply { auth_algs md5 sa unique }
{ dport cvc_hostd ulp tcp } permit { auth_algs md5 }
{ sport cvc_hostd ulp tcp } apply { auth_algs md5 sa unique }
```

For more detailed information on this file, refer to the `ipsecconf(1m)` man page.

Domain Security Options in SMS 1.3

To improve network performance on the MAN network, sequential MAC addresses are used by default on each of the up to 18 domains. With this configuration, it is straightforward to determine what the MAC address is of any given domain. It is, therefore, possible for a domain to broadcast gratuitous Address Resolution Protocol (ARP) information containing erroneous MAC addresses. The SC accepts these malicious MAC packets and uses them to misroute packets destined for domains. To protect against this type of ARP spoofing attack and other IP-based attacks, two options are available in SMS 1.3:

- Disable ARP on the I1 MAN network between the SCs and domains.
- Disable all IP traffic between the SC and a domain by excluding that domain from the SCs MAN driver

Disabling ARP on the MAN network provides some protection against ARP attacks, but it still leaves all other IP functionality present in the I1 network. If more stringent security is required, disabling all IP traffic between the SCs and one or more individual domains on the I1 network may be necessary. Instructions for implementing these two options are provided later in this article.

If a domain is excluded from the MAN network, the domain-to-SC network interface `dman0` is not configured at installation time. Even if the `dman0` interface is manually configured, the domain cannot communicate with the SC because the domain is excluded from the SC perspective. This solution provides excellent protection for a Sun Fire 12K or 15K chassis against malicious domains attempting to attack either the SC or other domains in the chassis. We recommend this solution for environments that require strongly enforced separation between domains and the SCs.

The Solaris Security Toolkit supports disabling ARP on the I1 MAN network as an option. You can modify a copy of the Sun Fire domain module of the `sunfire_15k_domain-secure.driver` to use the `s15k-static-arp.fin` hardening script. This hardening script is not enabled by default.

When all IP traffic between SCs and domains is disabled by the SC configuration, some functionality over the MAN network is not available. The unavailable services are as follows:

- Dynamic reconfiguration (DR) from the SC: commands such as `addboard`, `removeboard`, `deleteboard`, and `rcfgadm` cannot be used for domains excluded from the I1 MAN network
- I1 MAN domain-console access from the SC
- IP-based services from the SC such as network time protocol (NTP) and JumpStart or flash-based OS installations
- The use of `showdevices`, from the SC, to display devices associated with domains

Domain-side DR is available for domains that are excluded from the MAN network. Console access to the domains is available because console traffic can use either the internal I1 MAN network or an input output static random access memory (IOSRAM)-based communication path. The IOSRAM interface is totally separate from the TCP/IP-based MAN connection. Services using the IOSRAM interface, such as domain booting, remain available even if IP traffic to one or more domains is disabled.

Ultimately, security policy and enterprise application requirements may be the deciding factor as to which option is most suitable. Disabling ARP on the MAN network provides some protection for domains against ARP attacks, but it still leaves all the functionality present in the MAN network. If more stringent security is required, disable all IP traffic between the SCs and one or more individual domains on the MAN network.

To enforce strict separation between a domain and all other domains and SCs in a Sun Fire high-end chassis, we recommend that the domain be excluded from the MAN network. This change can be performed only on the SC. For instructions on how to make these SC modifications, refer to the BluePrint OnLine article titled “Securing Sun Fire 12K and 15K System Controllers.”

Solaris OE Defaults and Modifications

The Solaris OE configuration of Sun Fire domains 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 Sun BluePrints OnLine article titled “Solaris Operating Environment Security: Updated for Solaris 9 Operating Environment.”

Based on the Solaris OE installation cluster (SUNWCall) typically used for Sun Fire domains, over 100 Solaris OE configuration modifications are recommended to improve the security configuration of the Solaris OE image running on Sun Fire domains.

Implementing these modifications is automated when you use the driver script `sunfire_15k_domain-secure.driver` available in the Solaris Security Toolkit. An updated version of this driver is available in the Solaris Security Toolkit version 0.3.10 and newer.

Disabling Unused Services

We recommend that you disable all unused services. Reducing services offered by Sun Fire domains to the network decreases the access points available to an intruder. The modifications to secure Sun Fire domains result in reducing the number of TCP, UDP, and RPC services available from a domain.

The security recommendations in this article include all Solaris OE modifications that do not impact required Sun Fire domain functionality. This does not mean these modifications are appropriate for every domain. In fact, it is likely that some of the services disabled by the default `sunfire_15k_domain-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 – A secured configuration must be considered in the context of the application and services provided. The secured configuration implemented in this article is a *high-water mark* for system security; every service not required is disabled. Using the information in this article, you can determine clearly what can be disabled without adversely affecting the behavior of Sun Fire domains in your environment.

Recommendations and Exceptions

Our recommendations for securing Sun Fire domains follow closely with the hardening described in the Sun BluePrints OnLine article titled “Solaris Operating Environment Security, Updated for Solaris 9 Operating Environment.”

Solaris Basic Security Module (BSM) is *not enabled*. The BSM subsystem can be difficult to optimize for appropriate logging levels and produces log files which may be time consuming 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.

For more information on how to configure BSM, refer to the Sun BluePrint OnLine article titled “Auditing in the Solaris 8 Operating Environment.”

Mitigating Security Risks of Solaris OE Services

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

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

The recommendations in these articles are implemented with the Solaris Security Toolkit software in standalone and JumpStart modes.

Using Scripts to Perform Modifications

You can implement the recommendations using the Solaris Security Toolkit in either standalone or JumpStart mode. The three drivers used by the Solaris Security Toolkit to harden Sun Fire domains are as follows:

- `sunfire_15k_domain-secure.driver` (executes the other drivers)
- `sunfire_15k_domain-config.driver`
- `sunfire_15k_domain-hardening.driver`

The modifications performed by these drivers are organized into the following categories:

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

For more detailed information about each of the scripts used to harden domains, refer to the `sunfire_15K-domain` drivers mentioned previously or the Solaris Security Toolkit documentation available from:

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

Securing Sun Fire Domains

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 Sun Fire domains, changes are required to the Solaris OE software running on Sun Fire domains.

To secure Sun Fire domains, perform the following:

- “Adding Security Software” on page 12
- “Customizing the Solaris Security Toolkit Driver” on page 18 (optional)
- “Overriding Solaris Security Toolkit Defaults” on page 21 (optional)
- “Installing Downloaded Software and Implementing Modifications” on page 21

Adding Security Software

The first stage in hardening Sun Fire domains requires downloading and installing additional software security packages. This section covers the following tasks:

- “Install Solaris Security Toolkit Software” on page 13
- “Download Recommended Patch Cluster Software” on page 14
- “Download FixModes Software” on page 15
- “Download OpenSSH Software” on page 16
- “Download the 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. On Solaris 9 OE systems, the version of Secure Shell bundled with the OE can be used instead of OpenSSH. Also, on both Solaris 8 OE and Solaris 9 OE systems, a commercial version of Secure Shell can be used. You must install a Secure Shell product on Sun Fire domains.

Install Solaris Security Toolkit Software

The Solaris Security Toolkit software must be downloaded first, then installed on Sun Fire domains. Later, you'll use the Solaris Security Toolkit software to automate installing other security software and implementing the Solaris OE modifications for hardening the domains.

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 filenames that are correct only for version 0.3.10 and newer of the Solaris Security Toolkit software.

▼ To Download Solaris Security Toolkit Software

1. Download the latest version of the source file from:

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

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

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

Where `SUNWjass-0.3.10.pkg.Z` is the file name of the most current release.

3. Install the Solaris Security Toolkit software onto the server by using the `pkgadd` command:

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

Where `SUNWjass-0.3.10.pkg` is the file name of the most current release.

Executing this command creates the `SUNWjass` subdirectory in `/opt`. This subdirectory contains all Solaris Security Toolkit 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.

Download Recommended Patch Cluster 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 patches are installed. Ensure that the latest Solaris OE Recommended and Security Patch Cluster is installed on the Sun Fire domains. This section describes how to download the latest patch cluster.

Downloading the latest patch cluster does not require a SunSolve OnLineSM 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.

▼ To Download Recommended Patch Cluster Software

1. **Download the latest patch from the SunSolve OnLine Web site at:**

`http://sunsolve.sun.com`

2. **Click on the Patches link at the top of the left navigation bar.**
3. **Click on Recommended and Security Patches in the Download box.**
4. **Select the download option for the appropriate Solaris OE version, either HTTP or FTP, by clicking on the appropriate link.**

In our example, we selected Solaris 9 OE using HTTP download.

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

5. **Save the file locally.**
6. **Move the file securely to the Sun Fire 12K or 15K domains with the `scp` command, or `ftp` if Secure Shell is not available.**

If you use the `scp` command, it should be similar to the following example:

```
% scp 9_Recommended.zip sun15-a:/var/tmp
```


7. Move the file to the `/opt/SUNWjass/Patches` directory and uncompress it as follows:

```
# cd /opt/SUNWjass/Patches
# mv /var/tmp/9_Recommended.zip .
# unzip 9_Recommended.zip
Archive:      9_Recommended.zip
  creating:  9_Recommended/
  inflating: 9_Recommended/CLUSTER_README
  inflating: 9_Recommended/copyright
  inflating: 9_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.

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 of Sun Fire domains. More restrictive permissions make it even more difficult for malicious users to gain privileges on a system.

▼ To Download FixModes Software

1. Download the FixModes pre-compiled binaries from:

http://www.sun.com/blueprints/tools/FixModes_license.html

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

2. Once downloaded, move the file securely to the Sun Fire 12K or 15K domains with the `scp` command, or `ftp` if Secure Shell is not available.

The `scp` command used should be similar to the following command:

```
% scp FixModes.tar.Z sun15-a:/var/tmp
```

3. **Save the file, `FixModes.tar.Z`, in the Solaris Security Toolkit Packages directory in `/opt/SUNWjass/Packages` with the following commands:**

```
# cd /opt/SUNWjass/Packages
# mv /var/tmp/FixModes.tar.Z .
```



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.

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 Secure Shell 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 must implement a Secure Shell software product.

Information on where to obtain commercial versions of Secure Shell is provided in “Related Resources” on page 29.

Note – If a domain is running Solaris 9 OE, we recommend that you use the Sun-provided implementation of Secure Shell bundled with the OE. If using the Solaris version of Secure Shell, omit the OpenSSH installation steps in this section.

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`.

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

Access to the system can be gained with Secure Shell similarly to what is provided by RSH, Telnet, and FTP.

▼ To Download OpenSSH Software

- Obtain the following Sun BluePrints online article and use the instructions in the 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/blueprints/0701/openssh.pdf>

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



Caution – Do not compile OpenSSH, and do not install compilers on Sun Fire 12K or 15K domains just to compile OpenSSH. 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 the Secure Shell bundled with Solaris 9 OE or a commercial version of Secure Shell, then no compilation is required. Understand however, that omitting compilers does not provide significant protection against determined attackers, because they could use previously compiled tools.

Download the MD5 Software

The MD5 software validates MD5 digital fingerprints on the Sun Fire domains. 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 Download the MD5 Software

1. Download the MD5 binaries from the following web site:

http://www.sun.com/blueprints/tools/md5_license.html

The MD5 programs are distributed as a compressed tar file.

2. Move the file `md5.tar.Z` securely to the Sun Fire 12K or 15K domains with the `scp` command, or `ftp` if `scp` is not available.

The `scp` command used should be similar to the following

```
% scp md5.tar.Z sun15-a:/var/tmp
```

3. **Copy the 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 is saved to the `/opt/SUNWjass/Packages` directory, the execution of the Solaris Security Toolkit installs the 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.”

4. **(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” article.

Customizing the Solaris Security Toolkit Driver

If you determine that your system requires some of the services and daemons disabled by the Solaris Security Toolkit, or you want to enable any of the inactive scripts available in the Solaris Security Toolkit, do so before executing the Solaris Security Toolkit.

As described earlier in this article, the SMS 1.2 and SMS 1.3 software provides capabilities for securing the MAN network, which are as follows:

- Disable ARP on the I1 MAN network.
- Disable all I1 MAN IP traffic for one or more domains.

Disabling all I1 IP traffic to domains can only be done on the SC. Refer to the BluePrint OnLine article titled “Securing Sun Fire 12K and 15K System Controllers” for details on how this is done.

Disabling ARP on the MAN network can only be done for an entire chassis. It is not possible to make this change only for certain domains. It must be done on all domains having IP connectivity to the I1 network.



Caution – When disabling ARP on a SunFire 12K or 15K system, it is critical that the necessary configuration changes be made to *all domains and both SCs* at the same time. Making the changes only on certain domains or SCs causes the system to malfunction.

Using the Solaris Security Toolkit to disable ARP on the domains requires modifications to the default files distributed with the Solaris Security Toolkit.

Note – We recommend that the SCs be secured first, particularly when implementing static ARP between the SCs and domains. If the SCs are not secured and validated, do not proceed with implementing static ARP. Complete the hardening process of the SCs first.

▼ To Disable ARP on the I1 MAN Network

1. To add the necessary features or customize the hardening required for your system, edit a copy of the `sunfire_15k_domain-hardening.driver` file..

```
# cd /opt/SUNWjass/Drivers
# vi sunfire_15k_domain-hardening.driver
```



Caution – To preserve your changes for future updates and prevent the Solaris Security Toolkit from overriding your changes, modify only a copy of the driver. Keep the original Solaris Security Toolkit driver as a master.

2. If ARP is being disabled on the I1 MAN network, uncomment `s15k-static-arp.fin` from the driver by removing the `#` symbol in front of the script. After you edit the line, it should appear as follows in the `JASS_SCRIPTS` definition:

```
s15k-static-arp.fin
```

3. Review the IP Address for the I1 MAN interface and matching MAC address of the SC in the `sms_domain_arp` file.

This file is in the `/opt/SUNWjass/Files/etc` directory. The Solaris Security Toolkit uses the following initial values in this file:

192.168.103.1	08:00:20:63:49:1e
---------------	-------------------

a. If your site configuration for the MAN network uses a different IP Address for the I1 MAN interface of the SC, replace the `192.168.103.1` value with the IP address of the I1 MAN interface used in your environment.

b. If your site configuration requires a different MAC address than the initial `08:00:20:63:49:1e` value, replace it with the MAC address that matches the IP Address for the I1 MAN interface on all domains and both SCs.

All the domains must use the same `/etc/sms_domain_arp` file.



Caution – The IP address of the main SC in this file must match the IP address chosen as the IP Address of the SC on the I1 MAN network. Any mismatches cause MAN network failures. These failures can adversely affect the reliability, availability, serviceability, and security of the platform.

4. Reboot the domains to implement the modified settings.

You must reboot the domains for these settings to take effect.

Overriding Solaris Security Toolkit Defaults

If there are some services that must remain enabled, and the Solaris Security Toolkit automatically disables them, you can override the defaults before executing the driver.

▼ To Override Defaults

- **To prevent the Solaris Security Toolkit from disabling a service, comment out the call to the appropriate finish script in the driver.**

For example, if your environment requires Network File System (NFS)-based services, you can leave them enabled. Comment out the `disable-nfs-server.finish` and `disable-rpc.finish` scripts by appending a `#` sign before them in the copy of the `sunfire_15k_domain-hardening.driver` script.

For more information about editing and creating driver scripts, refer to the Solaris Security Toolkit documentation.

Installing Downloaded Software and Implementing Modifications

The Solaris Security Toolkit version 0.3.10 and newer provides a driver (`sunfire_15k_domain-secure.driver`) for automating the installation of security software and Solaris OE modifications. The driver performs the following tasks:

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

Note – The actions performed by each of the scripts is described in the Solaris Security Toolkit documentation. The hardening described is performed in standalone mode, not JumpStart mode, because the Sun Fire domains were built using an interactive Solaris OE installation. For details on the differences between standalone mode and JumpStart mode, refer to the Solaris Security Toolkit documentation.

Note – During the installation and modifications implemented in this section, all non-encrypted access mechanisms to Sun Fire domains—such as Telnet, RSH, and FTP—are disabled. The hardening steps do not disable domain console access from Sun Fire 12K or 15K SCs.

▼ To Install Downloaded Software and Implement Changes

- **Execute the `sunfire_15k_domain-secure.driver` script as follows:**

```
# cd /opt/SUNWjass
# ./jass-execute -d sunfire_15k_domain-secure.driver
./jass-execute: NOTICE: Executing driver,
sunfire_15k_domain-secure.driver

=====
sunfire_15k_domain-secure.driver: Driver started.
=====
[...]
```

▼ To View the Contents of the Driver File

- **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>

▼ To Undo a Solaris Security Toolkit Run

Each Solaris Security Toolkit 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.



Caution – 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.

- **To undo a run or series of runs, use the `jass-execute -u` command.**

For example, on a system where seven separate Solaris Security Toolkit runs are performed, you could undo them by using the following command and options:

```
# pwd
/opt/SUNWjass
# ./jass-execute -u
Please select from one of these backups to restore to
1.  December 10, 2002 at 19:45:15 (/var/opt/SUNWjass/run/20021210194515)
2.  December 10, 2002 at 19:25:22 (/var/opt/SUNWjass/run/20021210192522)
3.  December 10, 2002 at 19:07:32 (/var/opt/SUNWjass/run/20021210190732)
4.  December 10, 2002 at 19:04:36 (/var/opt/SUNWjass/run/20021210190436)
5.  December 10, 2002 at 18:30:35 (/var/opt/SUNWjass/run/20021210183035)
6.  December 10, 2002 at 18:29:48 (/var/opt/SUNWjass/run/20021210182948)
7.  December 10, 2002 at 18:27:44 (/var/opt/SUNWjass/run/20021210182744)
8.  Restore from all of them
Choice? 8
./jass-execute: NOTICE: Restoring to previous run
/var/opt/SUNWjass/run/20021210194515

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

Note – By default, the Solaris Security Toolkit overwrites any files backed up during earlier runs being undone. In some cases, this action overwrites changes made to files since the run was performed. If you have concerns about overwriting changes, use the `-n` (no force) option to prevent modified files from being overwritten. Refer to the Solaris Security Toolkit documentation for more details about this option.

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

Note – Software installations and actions performed by other software are not undone by the Solaris Security Toolkit undo feature. For example, the installation of OpenSSH, FixModes, and MD5 is not undone. In addition, the modifications performed by FixModes are not automatically undone.

Verifying Domain Hardening

After you complete the hardening process for each domain, reboot the domain and test the configuration by having the domain perform the tasks it should be capable of. At a minimum, make sure that each of the services provided by a hardened domain are running and functioning properly.

Check any additional software installed on the domain to validate that it is functioning properly. Ideally, use existing quality assurance or acceptance testing and scripts to verify that hardened domain is working properly and that the hardening process has not adversely affected any required features.

For our sample configuration, the modifications reduced the TCP and UDP services listening from 93 to 4. Similarly, the registered RPC services went from 149 to 0. These results represents a significant improvement in the security of the Solaris OE on each domain.

After we hardened each domain, installed appropriate versions of Secure Shell, and the rebooted the system, the only network services that are available in our sample configuration are as follows:

```
# netstat -a
UDP: IPv4
  Local Address          Remote Address      State
-----
  *.*                   Unbound

TCP: IPv4
Local Address  Remote Address  Swind  Send-Q  Rwind  Recv-Q  State
-----
*.*           *.*           0      0      24576  0      IDLE
*.cvc_hostd   *.*           0      0      24576  0      LISTEN
*.sun-dr      *.*           0      0      24576  0      LISTEN
*.32772       *.*           0      0      24576  0      LISTEN
*localhost.smtp *.*           0      0      49152  0      LISTEN
*.22          *.*           0      0      24576  0      LISTEN

TCP: IPv6
Local Address  Remote Address  Swind  Send-Q  Rwind  Recv-Q  State  If
-----
*.*           *.*           0      0      24576  0      IDLE
*.cvc_hostd   *.*           0      0      24576  0      LISTEN
*.sun-dr      *.*           0      0      24576  0      LISTEN
*.22          *.*           0      0      24576  0      LISTEN

Active UNIX domain sockets
Address  Type          Vnode      Conn  Local Addr      Remote Addr
```

After hardening, the daemons left running are as follows:

```
[sun15-a/] uname -a
SunOS sun15-a 5.9 Generic_112233-03 sun4u sparc SUNW,Sun-Fire-15000
[sun15-a/] ps -ef
  UID    PID  PPID  C   STIME TTY      TIME CMD
root     0     0  0   Dec 06 ? 0:02  sched
root     1     0  0   Dec 06 ? 0:00  /etc/init -
root     2     0  0   Dec 06 ? 0:00  pageout
root     3     0  0   Dec 06 ? 7:09  fsflush
root  1158     1  0   Dec 06 ? 0:00  /usr/lib/saf/sac -t 300
root    219     1  0   Dec 06 ? 0:00  /usr/lib/utmpd
root     63     1  0   Dec 06 ? 0:00  devfsadmd
root    11     1  0   Dec 06 ? 0:00  /platform/SUNW,Sun-Fire-15000/lib/cvcd
root    54     1  0   Dec 06 ? 0:00  /usr/lib/sysevent/syseventd
root    60     1  0   Dec 06 ? 0:02  /usr/lib/picl/picld
root   115     1  0   Dec 06 ? 0:00  /usr/platform/SUNW,Sun-Fire-15000/lib/
sckmd
root   151     1  0   Dec 06 ? 0:00  /usr/sbin/inetd -s
root   252     1  0   Dec 06 ? 0:00  /usr/lib/efcode/sparcv9/efdaemon
root   187     1  0   Dec 06 ? 0:00  /usr/sbin/syslogd
root   190     1  0   Dec 06 ? 0:00  /usr/sbin/cron
root   238     1  0   Dec 06 ? 0:00  /usr/lib/sendmail -bd -q15m
smmsp 6045     1  0   08:55:45 ? 0:00  /usr/lib/sendmail -Ac -q15m
root  1163     1  0   Dec 06 ? 0:00  /usr/lib/ssh/sshd
```

We perform an additional check to validate the services available on the domain using nmap, as follows:

```
# ./nmap -p 1-65535 -sS -sU 10.0.0.200
```

Using the popular freeware network scanner nmap command, this port scan is performed from a system external to the Sun Fire 12K or 15K frame. For more information about the nmap command, refer to <http://www.insecure.org/nmap>.

Our scan verified that only the following network services are available from outside the frame of the Sun Fire 15K domain:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Interesting ports on sun15-a.blueprints.Sun.COM (10.0.0.200):
Port      State      Service
22/tcp    open       ssh
442/tcp   filtered   cvc_hostd
665/tcp   filtered   sun-dr

Nmap run completed -- 1 IP address (1 host up) scanned in 3 seconds
```

The scan generated the following syslog error messages:

```
Sep 20 08:04:26 sun15-a ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 129.148.181.252, Destination 010.000.000.020.

Sep 20 08:04:27 sun15-a last message repeated 1 time

Sep 20 08:04:28 sun15-a sshd[357]: [ID 800047 auth.error] error:
setsockopt SO_KEEPALIVE: Invalid argument

Sep 20 08:04:29 sun15-a ip: [ID 993989 kern.error]
ip_fanout_tcp_listen: Policy Failure for the incoming packet (not
secure); Source 129.148.181.252, Destination 010.000.000.020.

Sep 20 08:04:30 sun15-a last message repeated 1 time
```

These error messages were generated by the IPsec authentication mechanism on the domain when scanned by nmap. Error messages are produced because the nmap IP packets did not conform to the IPsec security policies used to protect those ports. IPsec is used to authenticate all Sun Fire system traffic accepted by Sun Fire daemons and traffic that should traverse the I1 or MAN internal network.

About the Authors

Alex Noordergraaf

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 SunPSSM. 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.

Dina K. Nimeh

Dina Nimeh is a Senior Software Engineer with 15 years of experience in many areas from device drivers to databases. For the past four years, Dina has focused on secure software development and the deployment of security system solutions such as vulnerability assessment tools, intrusion detection systems, and public key infrastructures. Currently, she works with the Enterprise Systems Group at Sun Microsystems.

Related Resources

- 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 a JumpStart™ Infrastructure,” Sun BluePrints OnLine, April 2001, <http://sun.com/blueprints/0401/BuildInf.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.
- 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 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.
- Noordergraaf, Alex and Brunette, Glenn. “The Solaris Security Toolkit - Release Notes: Updated for version 0.3,” Sun BluePrints OnLine, June 2001, http://sun.com/blueprints/0601/jass_release_notes-v03.pdf.
- Noordergraaf, Alex and Nimeh, Dina K. “Securing the Sun Fire™ 12K and 15K System Controller,” Sun BluePrints OnLine, February 2003, <http://sun.com/blueprints/0203/817-1358.html>.
- 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>.
- Sun Microsystems, Inc. *System Management Services (SMS) 1.2 Administrator Guide*, Part No 816-5318-10, Sun Microsystems, Inc., January 2003, Revision A, <http://docs.sun.com>.

- Sun Microsystems, Inc. *System Management Services (SMS) 1.2 Reference Guide*, Sun Microsystems, Part No 816-5319-10, Sun Microsystems, Inc., January 2003, Revision A, <http://docs.sun.com>.