Fujitsu SPARC M12 and Fujitsu M10/SPARC M10

Security Guide

FUJITSU

ORACLE

Manual Code: C120-E693-02EN
March 2017

Disclaimer: The only warranties granted by Oracle and Fujitsu Limited, and/or any affiliate in connection with this document or any product or technology described herein are those expressly set forth in the license agreement pursuant to which the product or technology is provided.

EXCEPT AS EXPRESSLY SET FORTH IN SUCH AGREEMENT, ORACLE OR FUJITSU LIMITED, AND/OR THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND (EXPRESS OR IMPLIED) REGARDING SUCH PRODUCT OR TECHNOLOGY OR THIS DOCUMENT, WHICH ARE ALL PROVIDED AS IS, AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Unless otherwise expressly set forth in such agreement, to the extent allowed by applicable law, in no event shall Oracle or Fujitsu Limited, and/or any of their affiliates have any liability to any third party under any legal theory for any loss of revenues or profits, loss of use or data, or business interruptions, or for any indirect, special, incidental or consequential damages, even if advised of the possibility of such damages.

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.

Avis de non-responsabilité : les seules garanties octroyées par Oracle et Fujitsu Limited et/ou toute société affiliée de l'une ou l'autre entité en rapport avec ce document ou tout produit ou toute technologie décrits dans les présentes correspondent aux garanties expressément stipulées dans le contrat de licence régissant le produit ou la technologie fournis.

SAUF MENTION CONTRAIRE EXPRESSEMENT STIPULEE AU DIT CONTRAT, ORACLE OU FUJITSU LIMITED ET/OU LES SOCIETES AFFILIEES A L'UNE OU L'AUTRE ENTITE DECLINENT TOUT ENGAGEMENT OU GARANTIE, QUELLE QU'EN SOIT LA NATURE (EXPRESSE OU IMPLICITE) CONCERNANT CE PRODUIT, CETTE TECHNOLOGIE OU CE DOCUMENT, LESQUELS SONT FOURNIS EN L'ETAT. EN OUTRE, TOUTES LES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON, SONT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE. Sauf mention contraire expressément stipulée dans ce contrat, dans la mesure autorisée par la loi applicable, en aucun cas Oracle ou Fujitsu Limited et/ou l'une ou l'autre de leurs sociétés affiliées ne sauraient être tenues responsables envers une quelconque partie tierce, sous quelque théorie juridique que ce soit, de tout manque à gagner ou de perte de profit, de problèmes d'utilisation ou de perte de données, ou d'interruptions d'activités, ou de tout dommage indirect, spécial, secondaire ou consécutif, même si ces entités ont été préalablement informées d'une telle éventualité.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTE AUTRE CONDITION, DECLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISEE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security

This document provides general security guidelines for the Fujitsu SPARC M12 and Fujitsu M10/SPARC M10. This guide is intended to help you ensure security when using these servers with other hardware products such as network switches and network interface cards.

The following sections are in this chapter:

Understanding Security Principles

There are four basic security principles: access, authentication, authorization, and accounting.

- Access
  Physical and software controls are necessary to protect your hardware or data from intrusion.
  - For hardware, access limits usually mean *physical* access limits.
  - For software, access is limited through both physical and virtual means.
  - Firmware cannot be changed except through the update process.
- Authentication
  All platform operating systems provide authentication features that can be set up to ensure that users are who they say they are.

  Authentication provides varying degrees of security through measures such as badges and passwords.
- Authorization
  Authorization allows company personnel to work only with hardware and software that they are trained and qualified to use. To this end, system administrators create systems of Read/Write/Execute permissions to control user access to commands, disk space, devices, and applications.

- Accounting
  Software and hardware features allow customer IT to monitor login activity and maintain hardware inventories.
  - User logins can be monitored through system logs. System Administrator and Service accounts in particular have access to powerful commands and should be carefully monitored through system logs. Logs are typically maintained for a long period, so it is essential to periodically retire log files when they exceed a reasonable size, in accordance with the customer company policy.
  - Customer IT assets are usually tracked through serial numbers. Part numbers are electronically recorded on all cards, modules, and mother boards, and can be used for inventory purposes.

Planning a Secure Environment

Use the following notes before and during the installation and configuration of a server and related equipment.

Hardware Security

Physical hardware can be secured fairly simply: limit access to the hardware and record serial numbers.

- Restrict access
  - Install servers and related equipment in a locked, restricted access room.
  - If equipment is installed in a rack with a locking door, always lock the rack door until you have to service the components within the rack.
  - Hot-plug or hot-swap devices are removed easily and especially require restricted accessibility.
  - Store spare field-replaceable units (FRUs) or customer-replaceable units (CRUs) in a locked cabinet. Restrict access to the locked cabinet to authorized personnel.
- Record serial numbers
  - Security-mark all significant items of computer hardware such as FRUs. Use special ultraviolet pens or embossed labels.
  - Keep a record of the serial numbers of all your hardware.
  - Keep hardware activation keys and licenses in a secure location that is easily accessible to the system manager in system emergencies. The printed documents might be your only proof of ownership.

Software Security

Most hardware security is implemented through software measures.

- When a new system is installed, change all default passwords. Most types of equipment use default passwords, such as `changeme`, that are widely known and would allow unauthorized access to the equipment. Also, devices such as network switches can have multiple user accounts by default. Be sure to change all account passwords.
- Use a dedicated network for service processors to separate them from the general network.
- Protect access to USB consoles. Devices such as system controllers, power distribution units (PDUs), and network switches can have USB connections, which can provide more powerful access than SSH connections.
- Refer to the documentation that came with your software to enable any security features available for the software.
- A server can boot securely with WAN Boot or iSCSI Boot.
  - For an Oracle Solaris 10 release, refer to the *Oracle Solaris Installation Guide: Network-Based Installations* book
  - For an Oracle Solaris 11 release, refer to the *Installing Oracle Solaris 11 Systems* book for WAN Boot information and the *System Administration Guide: Basic Administration* book for iSCSI boot information.

The Oracle Solaris Security Guidelines document provides information on:

- How to harden Oracle Solaris
- How to use Oracle Solaris security features when configuring your systems
- How to operate securely when you add applications and users to a system
- How to protect network-based applications

Oracle Solaris Security Guidelines documents can be found at:

- http://docs.oracle.com/cd/E53394_01/html/E54807/index.html

Firmware Security

Ordinary user accounts cannot edit the OpenBoot PROM (OBP) or other firmware. The Oracle Solaris Operating System uses a controlled firmware update process to prevent unauthorized firmware modifications. Only the superuser can use the update process.

For information for setting OBP security variables, refer to the *OpenBoot 4.x Command Reference Manual* at:

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

XSCF Firmware

XSCF firmware is system management firmware that is preinstalled on some SPARC servers. XSCF enables you to actively manage and monitor components installed in your system. The way you use XSCF affects the security of your system.

To understand more about using this firmware when setting up passwords, managing users, and applying security-related features, including Secure Shell (SSH), Secure Socket Layer (SSL), refer to XSCF documentation:

- http://www.fujitsu.com/global/products/computing/servers/unix/sparc/downloads/manuals/

Maintaining a Secure Environment

Hardware and software provide a number of security features controlling hardware and tracking assets.

Hardware Controls

Some systems can be set up to be turned on and off by software commands. In addition, the power distribution units (PDUs) for some system cabinets can be enabled and disabled remotely by software commands. Authorization for these commands is typically set up during system configuration and is usually limited to system administrators and service personnel. Refer to your system or cabinet documentation for further information.

Asset Tracking

Serial numbers are embedded in firmware located on option cards and system mother boards. These serial numbers can be read through local area network connections for inventory tracking.

Wireless radio frequency identification (RFID) readers can further simplify asset tracking.

Software and Firmware

- Always install the latest released version of the software or firmware on your equipment. Devices such as network switches contain firmware and might require patches and firmware updates.

- Install any necessary security patches for your software.

Local and Remote Access

Follow these guidelines to ensure the security of local and remote access to your systems:

- Create a banner to state that unauthorized access is prohibited.
- Use access control lists where appropriate.
- Set time-outs for extended sessions and set privilege levels.
- Use authentication, authorization, and accounting (AAA) features for local and remote access to a switch.
- If possible, use the RADIUS and TACACS+ security protocols:
  - RADIUS (Remote Authentication Dial In User Service) is a client/server protocol that secures networks against unauthorized access.
  - TACACS+ (Terminal Access Controller Access-Control System) is a protocol that permits a remote access server to communicate with an authentication server to determine if a user has access to the network.
- Use the port mirroring capability of the switch for intrusion detection system (IDS) access.
- Implement port security to limit access based upon a MAC address. Disable auto-trunking on all ports.
- Limit remote configuration to specific IP addresses using SSH instead of Telnet. Telnet passes user names and passwords in clear text, potentially allowing everyone on the LAN segment to see login credentials. Set a strong password for SSH.
- Early versions of SNMP are not secure and transmit authentication data in unencrypted text. Only version 3 of SNMP can provide secure transmissions.
- Some products come out of the box with PUBLIC set as the default SNMP community string. Attackers can query a community to draw a very complete network map and possibly modify management information base (MIB) values. If SNMP is necessary, change the default SNMP community string to a strong community string.
- Enable logging and send logs to a dedicated secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Review logs for possible incidents and archive them in accordance with the security policy.
- If your system controller uses a browser interface, be sure to log out after using it.

Data Security

Follow these guidelines to maximize data security:

- Back up important data using devices such as external hard drives, pen drives, or memory sticks. Store the backed up data in a second, off-site, secure location.
- Use data encryption software to keep confidential information on hard drives secure.
- When disposing of an old hard drive, physically destroy the drive or completely erase all the data on the drive. Deleting all the files or reformatting the drive will remove only the address tables on the drive -information can still be recovered from a drive after deleting files or reformatting the drive. (Use disk wiping software to completely erase all data on a drive.)

Network Security

Follow these guidelines to maximize your network security:

- Most switches allow you to define virtual local area networks (VLANs). If you use your switch to define VLANs, separate sensitive clusters of systems from the rest of the network. This decreases the likelihood that users will gain access to information on these clients and servers.
- Manage switches out-of-band (separated from data traffic). If out-of-band management is not feasible, then dedicate a separate VLAN number for in-band management.
- Keep Infiniband hosts secure. An Infiniband fabric is only as secure as its least secure Infiniband host.
- Note that partitioning does not protect an Infiniband fabric. Partitioning only offers Infiniband traffic isolation between virtual machines on a host.
- Maintain a switch configuration file off-line and limit access only to authorized administrators. The configuration file should contain descriptive comments for each setting.
- Use static VLAN configuration, when possible.
- Disable unused switch ports and assign them an unused VLAN number.
- Assign a unique native VLAN number to trunk ports.
- Limit the VLANs that can be transported over a trunk to only those that are strictly required.
- Disable VLAN Trunking Protocol (VTP), if possible. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.
- Disable unnecessary network services, such as TCP small servers or HTTP. Enable necessary network services and configure these services securely.
- Different switches will offer different levels of port security features. Use these port security features if they are available on your switch:

- MAC Locking: This involves tying a Media Access Control (MAC) address of one or more connected devices to a physical port on a switch. If you lock a switch port to a particular MAC address, superusers cannot create backdoors into your network with rogue access points.
- MAC Lockout: This disables a specified MAC address from connecting to a switch.
- MAC Learning: Use the knowledge about each switch port's direct connections so the switch can set security based on current connections.